



BT Kıbrıs Dernekleşiyor

Ahmet HIZLI Sayfa 2

Hikâyenin Sonunu Değiştirmek

Eralp Curcioğlu Sayfa 3

Ekranın Obür yüzü: Çocuklarımızın Dijital Geleceğini Birlikte İnşa Etmek

Yağmur Seyis Sayfa 4

Küçük Bir Adadan Global Pazarlara: Kuzey Kıbrıs'ın Teknoloji ve Girişimcilik Potansiyeli

Temel Üngör Sayfa 5

Dijital Delil Çıkmazı Sosyal Medya Verileri, KKTC'nin İzolasyonu ve Suçun Cazibesi

Kazım Ateş Sayfa 6

Yapay Zekaya Sığınmak: Yanlızlığımızın Çaresi mi? Yoksa Tuzağı mı?

Doç. Dr. Bengü Berkmen Sayfa 8

Yapay Zekâ Kullanan Takımı Nasıl Yönetirim?

Naim Sadıklar Sayfa 10

Ekrana Dert Anlatmak: Yapay Zekâyla Kurulan Duygusal Bağın Psikolojisi

Eşmen Tatlıcalı Sayfa 11

Bir Fikrin Geleceğe Açılan Durağı: CES

Niyal Öztürk Sayfa 13

En Değerli Altın Bilezik: Öğrenmeyi Öğrenmek

Ahmet Bilgen Sayfa 14

Yenilenen CCNA 2.0 Sertifika Sınavına Hazırlık: Bilmeniz Gerekenler

Yusuf Küçük Sayfa 16

Yapay Zekânın Maliyetini Doğru mu Hesaplıyoruz?

Fatoş Leymoncu Özbingül Sayfa 20

Yapay Zeka Son İcadımız mı?

Ahmet HIZLI Sayfa 21

Dijital Kimlik ve Güven: Dijital Dünyada “Ben” Olduğumu Nasıl Kanıtlarım?

Esat Gürhan Sayfa 23

MOR TAKIM/PURPLE TEAM:

Cem Gökdel..... Sayfa 26

Yapay Zekâ Çağında "Gölge BT" İllüzyonu: Kod Üretmek Mühendislik midir?

Yrd. Doç. Dr. Eren Küren Sayfa 28

Artık Gerçekten Neyin Gerçek Olduğunu Biliyor muyuz? “Yapay zekâ çağında görüntüye, sese ve bilgiye

Yrd. Doç. Dr. Cemal Kavalcıoğlu Sayfa 30

Küçük bir E-Devlet

Erkan Coşkun Sayfa 33

MEYVE SİNEĞİNİN DİJİTAL BEYİN HARİTASI, Beyin haritalarından sanal bedenlere ve yeni hesaplama**yöntemlerine**

Ata Ateş Sayfa 38

Kıbrıs'ta Yapay Zekâ — Geleceğin Teknolojisi Değil, Bugünün Aracı

Aynur Kahraman Sayfa 47

KKTC'de Kamera İzin ve Denetim Rejimi: Özel Hayat, Veri Koruma ve Çözüm Önerileri

Kazım Ateş Sayfa 43

IT Projelerinin Başarılı Olabilmesi Nelere Bağlıdır?

Vasviye Tunaboğlu Sayfa 45

Editörün yazısı:

BT Kıbrıs, Dernekleşiyor.

Bilim, Bilişim ve Teknoloji odaklı, yazıların bulunduğu ve 10 Nisan 2026'da ilk sayımızı btkıbrıs.org adresinde yayınladığımız BT Kıbrıs dergimiz, her geçen gün büyümeye devam ediyor.

Dergi büyüdükçe, yapılması gereken işlerin artması, topluma olan sorumluluk ve sosyal projelerimizin artık kurumsallaşarak devam etmesi gerekmektedir. Bu nedenle, tüm yazarlarımızdan aldığımız olumlu görüşler ışığında, BT Kıbrıs yazarları ile birlikte **Kıbrıs Bilim, Bilişim ve Teknoloji Derneği**'nin kurulması için tüm çalışmaları tamamlamış bulunmaktayız.

Çok kısa bir süre sonra, derneğimizin kuruluşunu resmi olarak açıklayacağız. Bu süreçte gerek dergi yazarlarımıza, gerekse derneğin kuruluşunda destek veren tüm yazar arkadaşlarıma, hocalarıma ve büyüklerime teşekkür ederim.

Sosyal sorumluluk projelerimiz sadece belirli bir kısma değil, toplumun her kesimine hitap edecek şekilde çeşitlendirilecek ve hayat bulacaktır.

Çalışmalarımıza destek vermeye başlayan ve yön veren tüm kurum ve kuruluşlara ve özellikle Sn. Cumhurbaşkanımız Tufan Erhürman'a teşekkür ederiz.



Ahmet HIZLI
Bilgisayar Mühendisi
Dergi Editörü

Hikâyenin Sonunu Değiştirmek

Bu yazı, yedi sayıdır süren bir dizinin son halkası. İlk sayıda görünmez duvarların içinde üretmeyi, ikinci sayıda hiç bitmeyen hikâyemizi, üçüncüde bir mahkeme salonunda "yasa koyucu"nun önemini, dördüncüde modelle çıktığımız yolda modeli nasıl kaybettiğimizi, beşinci ve altıncıda o modelin kendisini ve dayanması gereken yasaları anlattım. Bugünkü sayımızda bu diziyi kapatıyorum. Bu vazgeçmek değil; bir düşüncenin olgunlaşması demek.



Yedi sayıda ne demeye çalıştım?

Bütün yazıların altında tek bir cümle vardı; belki her seferinde farklı kapılardan girdik ama hep aynı odaya çıktık. Benim için değerli ve doğru olan şudur: **kendi hamurumuzla yoğrulmak, üretebilmek, ürettiğimizi önce kendi ihtiyacımız için kullanmak, sonra da başkalarına satabilmek.** Bunun bir romantizm olmadığını, basit bir ekonomi modeli olduğunu anlatmaya çalıştım.

Ama bunu yapabilmenin temelinde üç şey var ve üçü de teknolojiyle değil, yönetimle ilgili: doğru politikaları üretmek, o politikaların arkasında duracak siyasi kararlılık ve hepsinden önemlisi devamlılık. Bir seçimle silinmeyen, bir bakan değişince sıfırlanmayan, bir kişiye bağlı olmayan devamlılık.

E-devleti bütün yazılarda örnek olarak seçtim; çünkü hikâyenin tamamını tek başına anlatıyor. Politikadaki eksiklikler, dışarıdan gelen baskılar, yerelde üretmeye çalışanlara kurulan ambargolar, projelerin dışarıdan gelecek firmalara yaptırılmasını neredeyse zorunlu kılan politikalar; bunların hepsi e-devlette görülür. Sonucu da görülür: Yerel yatırımcı büyüyemez, araştırma ve geliştirmeye kaynak ayıramaz, üretmek yerine satıcı olmanın kolay kazancına yönelir. Bu zincirin sonunda duran cümle ağırdır ama söylenmelidir: Bu şekilde KKTC'nin sürdürülebilir bir ekonomisi olmaz. Ben bunu kendi sektörümde, bilgi ve iletişim alanında yazdım. Ama eminim ki diğer sektörlerde de aynı hikâye aynı sırayla ilerliyor. Bunun en görünür ölçüsü, toplum olarak üretimden kopmuş olmamızdır. Tarımda, sanayide, yazılımda; ne ürettiğimizi değil, ne sattığımızı konuşur olduk.

Cumhurbaşkanlığındaki masa

Geçtiğimiz günlerde dergi yazarları olarak

Cumhurbaşkanı'nı ziyaret etme şerefine eriştik. Güzel ve kaliteli bir sohbet oldu. Ben oradan bir şeyi çok net görerek çıktım; çünkü o makamda oturan seçilmiş bir liderin gözlemi, tek bir kişinin görüşü değildir, toplumun aynasıdır.

Gördüğüm şu: Biz aslında çok şeyimizi kaybetmişiz ve kaybetmeye de devam ediyoruz. Gençleri, toplumsal birlikteliği, çocukları ve daha birçok şeyi. Kimimiz Kıbrıs meselesine, kimimiz sektörün sorunlarına, izolasyonlara, devletin uluslararası protokollerine takılıp kaldık; o arada asıl olanı unuttuk. Yıllardır e-devletin modelini, yasaların eksikliğini yazan ben de dahil.

O masada Necdet hocamızın yıllardır süren çırpınısını, Tufan hocamızın sözlerindeki serzenişi dinlerken bir şey yerine oturdu. Burada durmam gerektiğini anladım.

Vardığım nokta basit ama ağırdı: Gençleri ve çocukları araştırın, geliştiren, üreten bireyler olarak hazırlamazsak içinde bulunduğumuz durum devam eder. Çünkü bir toplumu ileri götüren ya da yerinde tutan şey, kanunlar kadar alışkanlıklardır. Bugünkü alışkanlıklarımız ve açık söyleyeyim, tembelliklerimiz bizi ileri götürmez; böyle alıştık, böyle devam eder.

Bir çocuğu şu anki duruma, statükoya uyumlu yetiştirirsek statüko devam eder. Aynı çocuğu doğru yöne hazırlarsak toplumun yönelimi de alışkanlıkları da değişir ve statüko kendiliğinden yıkılır. Hiçbir yasa, hiçbir model, hiçbir portal bunu tek başına yapamaz. Ama doğru yetişmiş bir nesil, o yasa da o modeli de kendisi yazar.

Bu yüzden, e-devletin modelini ve hangi yasalara ihtiyaç olduğunu bu son yazıda tek bir şemayla bırakmayı düşünmüştüm. Sonra

kendime sordum: Bu şema bugün kaç kişi için önemli? Modeli okuyacak, tartışacak ve sahiplenecek bir zemin yokken onu bir dergi sayfasına bırakmak, mesajı bir çekmeceye kaldırmaktan farksız. Model hazır, duruyor; o zemin oluştuğunda paylaşırım.

Bundan sonrası

Modelle çıktığımız yolda model olmasa da, e-devlet olmasa da, yapılanların hepsi yanlış da olsa; benim için buna takılmak bitti. Bundan sonrası için yolum belli: Üreten, araştıran, geliştiren bir nesil nasıl yetişir; toplum olarak alışkanlıklarımızı nasıl değiştiririz; küçük bir ülkede eğitim, üretim ve devamlılık aynı masaya nasıl oturur. Yeni yazılarım bunun üzerine olacak.

İkinci sayıda "her hikâyenin sonu aynı olmak zorunda değildir" diye yazmıştım. Hâlâ öyle düşünüyorum. Ama artık hikâyenin sonunu yasaların değil, o yasaları bir gün yazacak çocukların değiştireceğine inanıyorum.

Eralp Curcioğlu

Elektrik ve Elektronik Mühendisi
EMI Technologies Ltd. Direktörü

EKRANIN ÖBÜR YÜZÜ: ÇOCUKLARIMIZIN DİJİTAL GELECEĞİNİ BİRLİKTE İNŞA ETMEK

Bizler sokak oyunlarının, akşam ezanıyla eve girilen çocuklukların son tanıklarıyız; bugünün çocukları (Alfa Kuşağı) ise doğdukları andan itibaren akıllı ekranların, yapay zeka asistanlarının ve algoritmaların hüküm sürdüğü bir evrene gözlerini açtılar. Bizler teknolojiyi sonradan öğrenen birer "dijital göçmen" iken, onlar bu dilin anadiliyle doğan "dijital yerliler." Aradaki temel çatışma da tam olarak burada başlıyor: Ebeveynler teknolojiyi hâlâ yönetilmesi gereken bir "tehlike" veya "zaman hırsızı" olarak görürken; çocuklar için ekran, sosyalleştikleri, dünyayı keşfettikleri ve var oldukları doğal bir yaşam alanı.

Peki, ebeveynlerin bu refleksif korkusu ne kadar haklı? Akademik dünya, ezbere dayalı bu kaygılarla aynı fikirde değil. Hsin ve arkadaşlarının (2014) 90'a yakın araştırmayı incelediği devasa taramadan, C. Herodotou (2017) ve Arabiat'ın (2023) 53 uluslararası çalışmayı sentezlediği güncel analizlere kadar literatür net bir gerçeği haykırıyor: **Teknoloji çocuğun zihnini köreltmiyor; aksine doğru içerikle sunulduğunda kelime dağarcığını, problem çözme becerisini, matematiksel zekayı ve hatta akran işbirliğini katbekat artırıyor.**

Ancak madem teknoloji bu kadar faydalı, çocuklarımız neden ekranı bir türlü kapatamıyor?

İşte ebeveynlerin anlaması gereken asıl gerçek burada başlıyor: Problem teknolojinin varlığı değil, arkasındaki tasarım mimarisidir. Bugün çocukların ekran başından kalkamaması sadece bir "disiplinsizlik" değil, teknoloji devlerinin *ikna edici teknoloji (persuasive technology)* tasarımlarının bir sonucudur. Sonsuz kaydırma, anlık bildirimler ve bitmeyen oyun döngüleri, çocuk zihnindeki dopamin mekanizmasını hedefler. Amerikan Pediatri Akademisi (AAP) Medya Konseyi'nden Dr. Jenny Radesky'nin de belirttiği gibi; ebeveynlerin artık *"Tabletini bırak!"* komutları veya *"Günde 1 saat bakabilirsin"* gibi yüzeysel sınırları hiçbir işe yaramamaktadır. Ebeveynlerin gerçekçi ve psikolojik olarak işleyen yeni adımlar atması gerekir:

- **Algoritma Okuryazarlığı Kazandırın:** Çocuğa sadece yasak koymak yerine, uygulamanın onu nasıl ekranda tutmaya çalıştığını deşifre edin. *"Sence bu oyun seni sürekli içeri çekmek için hangi tuzağı kullanıyor?"* diyerek zihninde algoritmik farkındalık yaratın. Amacımız çocuğu ekrandan kaçırmak değil, ekranın arkasındaki akıllı görmesini sağlamaktır.
- **Dopamin Alternatifleri Yaratın:** Çocuk ekrandan çıktığında derin bir sıkıntı (dopamin düşüşü) yaşar. Onu ekrandan alırken boşluğa bırakmak yerine, yerine koyabileceği gerçek dünya uyarım süreçleri (yeni bir beceri, hareketli bir aktivite) planlayın. Sıkıntı duygusu bir kriz değil, yaratıcılığın eşliğidir; buna fırsat tanıyın.
- **"Birlikte Kullanım" ile Köprü Kurun:** Çocuğunuzun oynadığı oyuna yabancılaşmayın. Birkaç dakikalığına da olsa onun dijital dünyasına "misafir" olun. İzlediği şeyi yargılayan biri gibi değil, dünyasını anlamaya çalışan meraklı bir rehber gibi

yaklaşın. Çocuk anlaşıldığını hissettiğinde, sınırları müzakere etmek çok daha kolaylaşır.

Sonuç olarak; çocukları dijital çağın gerçekliğinden koparmak geleceğin becerilerinden de mahrum bırakmak anlamına gelir. İhtiyacımız olan şey kısıtlamalar değil; çocuklarımızı algoritmaların pasif birer tüketicisi olmak yerine, teknolojiyi kendi gelişimleri için yönlendiren bilinçli birer dijital mimar olmayı öğretmektir.



BİR VAKA İNCELEMESİ: AİLELER İÇİN "ROBLOX" REHBERİ

Bugün çocukların ekran sürelerinin büyük bir kısmını tek bir platform ele geçirmiş durumda: **Roblox**. Çoğu ebeveyn bunun sadece masum bir "oyun" olduğunu sanıyor. Oysa Roblox; milyonlarca kullanıcının kendi dünyasını tasarladığı devasa ve denetimi zor bir dijital evrendir. Aileler bu döngüyü nasıl yönetmeli?

1. "Kullanıcı Üretimi" İçeriklere Dikkat Edin: Roblox'taki oyunları şirket değil, kullanıcılar yapar. Bu yüzden güvenlik filtreleri kusursuz değildir. "Her Yaş" etiketli bir oyunun içinde bile şiddet, kumar simülasyonları veya uygunsuz temalar ("condo" oyunları) gizlenmiş olabilir. Çözüm; hesap kısıtlamalarını açmak ve çocuğunuzun son oynadığı oyunların listesini ara sıra birlikte gözden geçirmektir.

2. Sohbet (Chat) ve "Kırmızı Bayrak" Farkındalığı: Roblox dev bir sohbet odasıdır. Sistemdeki küfür filtrelerini aşmak isteyen kötü niyetli kişiler, çocukları denetimin olmadığı başka platformlara (diğer mesajlaşma uygulamalarına) davet edebilir. Çocuğunuza bunun en büyük "kırmızı bayrak" olduğunu öğretin. Ayarlardan sohbeti "Sadece Arkadaşlar" olarak kısıtlayın ve listesinde sadece gerçek hayatta tanıdığı kişilerin olduğundan emin olun.

3. "Robux" ile Finansal Okuryazarlık: Platformun en büyük tuzaklarından biri oyun içi para birimi *Robux*'tur. Kredi kartınızı sisteme kaydetmek yerine; çocuğa aylık bir 'dijital harçlık' bütçesi belirleyin. Böylece harcamalarını kendi yönetmeyi ve elindekile yetinmeyi öğrenir.

4. İletişim Kanallarını Açık Tutun: Ona karşılaştığı rahatsız edici bir durumu (siber zorbalık veya tuhaf sorular) size anlattığında kızmayacağınızın veya *oyunu tamamen yasaklamayacağınızın* garantisini verin. Unutmayın; en güçlü güvenlik filtresi, çocuğunuzla aranızdaki güven bağıdır.

Yağmur Seyis
Öğrenci, Yazılım Mühendisliği Bölümü,
Doğu Akdeniz Üniversitesi

Referanslar: <https://oro.open.ac.uk/52543/7/52543.pdf>

https://www.researchgate.net/profile/Ching-Ting-Hsin/publication/287696031_The_Influence_of_Young_Children's_Use_of_Technology_on_Their_Learning_A_Review/links/695f456527359023a01560ea/The-Influence-of-Young-Childrens-Use-of-Technology-on-Their-Learning-A-Review.pdf

<https://www.commonssensemedia.org/articles/parents-ultimate-guide-to-roblox>

Küçük Bir Adadan Global Pazarlara: Kuzey Kıbrıs'ın Teknoloji ve Girişimcilik Potansiyeli

Gelişen ve sınırların her geçen gün ortadan kalktığı dijital dünyada, geleneksel ekonomik modellerin ötesine geçmek artık bir tercih değil, kaçınılmaz bir zorunluluk. Devasa fabrikalar kurmak ya da büyük otel yatırımları yapmak yüksek maliyet ve zaman gerektirirken; inovatif teknoloji girişimciliği, yani start-up'lar, iki-üç kişilik çekirdek ekiplerle başlayarak hızla küresel organizasyonlara dönüşebilmektedir. Dünya genelinde alternatif veya ana gelir modeli olarak kurgulanan bu ekosistem, bizim gibi ölçek olarak küçük ancak potansiyeli yüksek ülkeler için en stratejik kalkınma hamlesidir.

Fiber Altyapıda Tarihi Adım ve Ekosistemin Geleceği

Kuzey Kıbrıs'a baktığımızda, uzun yıllardır "Bilişim ve Girişimcilik" başlığında konuşulan ancak somutlaşmakta geciken süreçlerin nihayet aşılmaya başlandığını görüyoruz. Ekosistemin en kritik ihtiyacı olan iletişim altyapısında sevindirici bir dönüm noktasına ulaştık. Fiber altyapı konusunda imzalanan protokol ile birlikte dönüşüm çalışmaları yakın zamanda başlıyor. İnternet altyapımızın fiber teknolojiyle modernleştirilmesi, adadaki girişimcilerimizin dünyaya çok daha hızlı, kaliteli ve uygun maliyetlerle bağlanmasını sağlayarak teknoloji ekosistemimizin en büyük engelini ortadan kaldıracaktır.

Uluslararası Öğrenciler İçin "Startup Vizesi" Hamlesi

Ülkemizdeki 20'nin üzerindeki üniversiteden her yıl binlerce nitelikli mühendis ve teknoloji odaklı genç mezun oluyor. Ancak bu beyin gücünü adada tutacak mekanizmaları kurmak zorundayız. Bu noktada hayati bir talebimiz var: Startup Vizesi. Adamızda eğitim alıp mezun olan yetenekli uluslararası öğrencilere sağlanacak bir startup vizesi, adamızda kalıcı ve nitelikli bir yetkin iş gücü havuzu oluşturacaktır. Bu gençlerin bilgi birikimlerini Kuzey Kıbrıs'ta kuracakları girişimlere aktarmaları; yeni istihdam alanları, yüksek katma değerli ürünler ve adaya çekilecek uluslararası yatırımlar anlamına gelmektedir.

Yerli Yatırım Ekosisteminde Bir İlk: Yerli Sermayenin Girişimcilikle Buluşması

Ekosistemin geliştiğinin ve olgunlaştığının en somut kanıtı, finansal sermayenin bu alana akmaya başlamasıdır. Nitekim son dönemde adamızda tarihi bir milada tanıklık ettik: İlk kez yerli bir girişimimiz, yerli bir yatırımcıdan yatırım alarak büyüme yolculuğunda çok önemli bir eşiği aştı. Bu gelişme, adadaki sermaye sahiplerinin ve iş insanlarının teknoloji girişimciliğine olan güveninin arttığını göstermesi açısından son derece kıymetlidir. Yerli yatırımcının yerli girişimciye inandığı bu tablo, arkasından gelecek yeni yatırımlar için bir meşale yakmış ve Kuzey Kıbrıs'ın kendi iç kaynaklarıyla da teknoloji ihraç edebileceğini kanıtlamıştır.

Kısa Vadede Elde Edilebilecek Katma Değer

Altyapı hamlesi, yatırım iklimi ve doğru hukuki düzenlemelerle birlikte Kuzey Kıbrıs'ın kısa vadede elde edeceği kazanımlar

oldukça nettir:

1. Bölgesel ve Global Pazarlara Açılım:

Adada filizlenen bir teknoloji girişimi, güçlü fiber altyapı ve yetkin insan kaynağıyla önce Türkiye'ye, ardından Avrupa, Birleşik Krallık, ABD ve Uzak Doğu pazarlarına açılabilir. İTÜ Çekirdek programına seçilen Bitayka gibi lokal başarı örnekleri, doğru destekle neleri başarabileceğimizin en açık göstergesidir.

2. Yerel Sorunlara Teknolojik Çözümler:

Tarım teknolojilerinden yazılım ve tasarıma kadar pek çok alanda geliştirilecek yerli çözümler, hem ülke içi verimliliği artıracak hem de ihraç edilebilir birer değer haline gelecektir.

3. Sermaye Hareketliliği ve Finansal Büyüme:

Girişimlerin aldığı yatırımlar ve sermaye hareketliliği sayesinde adamız hem yerli hem de yabancı yatırımcılar için bir çekim merkezi haline gelecektir.

Sonuç: Kolektif Hareket Zamanı

"Bilişim Adası" vizyonu artık hayal değil, adımları tek tek atılan bir gerçekliktir. Ancak bu vizyonun başarıya ulaşması; devletimizin düzenleyici ve destekleyici rolü, özel sektörün dinamizmi, üniversitelerimizin üretkenliği ve girişimcilerimizin cesaretinin tek bir potada buluşmasına bağlıdır. Başarıya giden yol, kamu, özel sektör ve akademinin tam bir kolektif hareket bilinciyle ve ortak akılla çalışmasından geçmektedir. Bu birlikteliği sağladığımız takdirde, bu adadan dünya çapında ses getirecek teknoloji girişimlerinin neden bir Unicorn olmasın? çıkmaması için hiçbir neden yoktur.

Temel Üngör
GİTYAD Başkanı



Dijital Delil Çıkmazı Sosyal Medya Verileri,

KKTC'nin İzolasyonu ve Suçun Cazibesi



Günümüzde suç ve suçlu profilleri dijitalleşirken, kolluk kuvvetlerinin delil toplama yöntemleri de zorunlu olarak siber alana kaymış durumdadır (Broadhurst, 2006). Ancak örneğin bir uyuşturucu operasyonunda yakalanan şüphelinin dijital izlerini sürmek, sanıldığı kadar kolay bir süreç değildir. Yakın zamanda karşılaşılan bir vakada, yetkili bir kurumun yaptığı şu açıklama oldukça dikkat çekicidir:

"Facebook, Instagram, Twitter ve benzeri sosyal medya platformları, kendi politikaları ve GDPR (Genel Veri Koruma Yönetmeliği) gibi uluslararası mevzuatlar kapsamında kullanıcılara ait tüm kişisel verileri (IP, lokasyon vb.) standart kabul edilen en güçlü şifreleme yöntemleri ile muhafaza etmektedir. Bu bilgilere ulaşmanın mümkün olmaması nedeniyle ileri işleme gitmek mümkün olmamıştır."

Bu açıklama, uluslararası hukuku ve siber güvenlik prosedürlerini bilenler için şaşırtıcı olmayabilir. Ancak sokaktaki vatandaş, pratik çözümler arayan bir analist veya sahada çalışan bir Bilişim Teknolojileri (BT) uzmanı için akla hemen şu provokatif ve son derece haklı soru gelmektedir: **Madem şüphelinin fiziksel kimlik kartı emniyetin elinde, polis neden "Şifremi unuttum" adımlarını izleyip platforma bu kimliği ibraz ederek hesabı ele geçirmiyor?**

Aslına bakarsanız bu düşünce hiç de temelsiz değildir. Şifresini veya kayıtlı e-posta adresini unutan kullanıcılara hesaplarını kurtarmaları için yardım ederken, biz BT personellerinin sürekli olarak başvurduğu, sosyal medya platformları tarafından kabul gören ve pratikte gayet başarılı şekilde çalışan standart bir yöntemdir bu.

Peki, sıradan bir vatandaşın hesabını kurtarmak için sorunsuzca işleyen bu kimlik ibrazı yöntemi, söz konusu şüpheli bir şahsın hesabına el koymak isteyen devletin kolluk kuvvetleri olduğunda neden duvara toslar? Ve bu dijital çıkmaz, Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) özelinde ne gibi kriminolojik tehlikelere yol açmaktadır? Konuyu dört temel boyutta incelemek gerekir.

1. Masum Kullanıcı vs. Devlet: Teknik ve Algoritmik Engeller

Bir BT uzmanının standart bir kullanıcı için yaptığı şifre sıfırlama işlemi ile polisin bir şüphelinin hesabını ele geçirmesi arasında, platformların yapay zeka algoritmaları açısından devasa farklar vardır. Meta (2024) gibi devlerin hesap kurtarma süreçleri, sadece sisteme yüklenen bir kimlik fotoğrafından ibaret değildir.

- Cihaz ve IP Kimliği (Browser Fingerprinting):** Bir BT uzmanı genellikle kullanıcının kendi cihazından veya bilindik, "temiz" bir ağdan bu işlemi yapar. Oysa platformlar; tarayıcı parmak izi, lokasyon ve IP geçmişini analiz ederek polis merkezinden veya adli bilişim laboratuvarına ait bir IP'den gelen talepleri anında "devlet destekli ele geçirme" (state-sponsored account takeover) şüphesiyle reddeder (Laperdrix et al., 2020).
- İki Faktörlü Doğrulama (2FA):** Günümüzde hesaplar SMS veya Authenticator gibi ek güvenlik adımlarıyla korunmaktadır. Polisin elindeki kilitli bir telefonda 2FA'yı aşmak, sadece kimlik ibrazından çok daha karmaşık bir teknik bariyerdir.

- Delil Bütünlüğü:** Hesaba bu şekilde, dışarıdan müdahale edilerek (şifre değiştirilerek) girilmesi, adli bilişimde delilin "orijinalliğinin" (integrity) bozulması anlamına gelir (Casey, 2011). Yani hesaba girilse bile verilerin mahkemedeki inandırıcılığı zedelenmiş olur.

2. Hukuki Boyut: Zehirli Ağacın Meyvesi

İşin asıl kilit noktası hukuki çerçevedir. Bir BT uzmanı bu işlemi kullanıcının rızası ve onayı ile yapar. Ancak bir ülkenin polis teşkilatı, şüphelinin kılığına girip onun adına platforma yalan beyanda bulunarak ("Şifremi unuttum") veri elde edemez.

- Yetkisiz Erişim (Hacking):** Emniyet güçlerinin fiziksel el koyma izni olması, şüphelinin dijital kimliğini kullanarak uluslararası bir platformu "kandırma" yetkisi vermez. Bu eylem uluslararası hukukta "yetkisiz erişim" suçunu oluşturur (Brenner, 2010).
- Delil Geçerliliği:** Hukuk sistemlerinde "Hukuka aykırı olarak elde edilen deliller, mahkemede hükme esas alınamaz" kuralı geçerlidir. Buna "Zehirli Ağacın Meyvesi" (Fruit of the poisonous tree) doktrini denir (Dülger, 2014). Polis bu yolla hesaba girip uyuşturucu trafiğini kanıtlayan mesajlar bulsa bile, savunma makamı bu delilin hileyle elde edildiğini belirterek dosyadan çıkarttıracaktır.

Kolluk kuvvetlerinin tek yasal yolu, Uluslararası Adli Yardımlaşma Sözleşmeleri (MLAT) kapsamında resmi mahkeme kararlarını ilgili şirketlerin Kolluk Kuvvetleri Portallarına (Law Enforcement Portals) ileterek veriyi resmi yoldan talep etmektir (Jack L., 2001).

3. Asıl Düşüm: KKTC İçin Neden İmkansız? (Dijital İzolasyon)

Yukarıdaki kısıtlamalar tüm dünya için geçerliyken, durum KKTC için derin bir "dijital ambargo" boyutundadır.

Platformlar, resmi süreçlerde Birleşmiş Milletler tarafından tanınan egemen devletlerin ISO 3166-1 alpha-2 ülke kodlu evraklarını baz alır (Uluslararası Standardizasyon Örgütü., 2020). KKTC'nin uluslararası tanınmazlığı nedeniyle doğrudan MLAT anlaşmaları bulunmamaktadır. Teknoloji şirketleri ve uluslararası hukuk departmanları, Avrupa Birliği'nin GDPR (2016) regülasyonlarını da öne sürerek KKTC Mahkemelerinin kararlarını muhatap almamaktadır. Diplomatik kanalların ve yaptırım gücünün eksikliği, KKTC polisini dijital dünyada adeta "kör" bırakmaktadır.

4. Görünmeyen Delillerin Faturası: KKTC Suçlular İçin Bir "Cazibe Merkezi" mi Oluyor?

Dijital verilere, kriptolu iletişime ve sosyal medya geçmişine ulaşılmasının yarattığı asıl yıkıcı tablo, ceza infaz sisteminde ortaya çıkmaktadır. Yargı süreci sadece "buzdağının görünen kısmı" ile, yani fiziki olarak kanıtlanabilen "suçüstü" (in flagrante delicto) boyutuyla sınırlı kalmaktadır.

Bu durumun kriminolojik analizi yapıldığında tehlikeli bir sonuç doğmaktadır: Geçmiş suç kayıtlarına, uluslararası ağlara ve suçtan elde edilen gelirlere dijital olarak ulaşılamadığında mahkeme yalnızca yakalanan o anki fiziksel eylem üzerinden ceza tayin etmektedir. İşin gerisinde yatan devasa organizasyon ve kazanımlar suçlunun yanına kâr kalmaktadır.

Bu boşluk, teknolojiyi iyi kullanan organize suç örgütleri için KKTC'yi "dijital bir güvenli liman (safe haven)" haline getirme riski taşımaktadır (Kshetri, 2010). Örneğin; KKTC'de yasa dışı bahis veya uyuşturucu ticareti yapan bir şahıs, elde ettiği devasa kara parayı, takibi neredeyse imkansız olan soğuk krypto cüzdanlara (cold wallets) aktarır. Kolluk kuvvetleri şahsı fiziki olarak yakalasa da, bulut tabanlı verilere erişemediği için kişi sadece o anki "kısıtlı suçtan" yargılanır (Foley et al., 2019).

Kısa süreli cezasının infazı bittikten veya ülkeden deport edildikten sonra şahıs, milyonlarca dolarlık krypto varlığına özgürce kavuşur. Yattığı ceza, elde ettiği servetin yanında ödenmiş küçük bir "risk maliyeti" olarak kalır. Bu durum, suça karşı caydırıcılığı yok etmekle kalmaz; KKTC'nin hukuki izolasyonunu suçlular için "cazip ve kârlı bir yatırım aracına" dönüştürür.

5. Sonuç

Biz BT profesyonellerinin sıradan kullanıcılar için başarıyla uyguladığı "kimlik ibrazı ile şifre sıfırlama" yöntemi; adli süreçlerde yapay zeka engellerine, delil bütünlüğü kurallarına ve "Zehirli Ağacın Meyvesi" doktrinine çarpmaktadır. Ancak bu pratik yöntemin kullanılamaması ve verilerin resmi yollarla da talep edilememesi, KKTC'nin varoluşsal bir adalet sorunuyla yüzleştiğini göstermektedir.

Dijital delillere erişemeyen bir yargı sisteminin tam adaleti sağlaması mümkün değildir. Bu sorunun çözümü, polisin "arka kapı" yöntemlerine başvurması olamaz. KKTC'nin uluslararası adli işbirliği mekanizmalarına garantör yapılar üzerinden acilen entegre edilmesi ve Bilişim Suçları Yasası'nın modernize edilerek adli bilişim birimlerinin krypto varlık takibi konusunda uluslararası standartlarda yetkilendirilmesi elzemdir. Aksi takdirde, KKTC'nin siber uzaydaki bu çaresizliği, küresel suç ağları için bulunmaz bir fırsata dönüşmeye devam edecektir.

Kaynakça

- Brenner, S. W. . (2010). *Cybercrime : criminal threats from cyberspace*. Praeger.
- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433. <https://doi.org/10.1108/13639510610684674>
- Casey, Eoghan. (2011). *Digital evidence and computer crime : forensic science, computers and the internet*. Academic Press.
- Dülger, M. Volkan. (2014). *Ceza muhakemesi hukukunda dışlama kuralı ve hukuka aykırı delillerin uzak etkisi (zehirli ağacın meyvesi öğretisi)*. Seçkin Yayınevi.
- Foley, S., Karlsen, J. R., & Putnits, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- Jack L., G. (2001). *The University of Chicago legal forum*. 2001(1). <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1298&context=uclf>
- Kshetri, N. (2010). *The Global Cybercrime Industry*. Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-642-11522-6>
- Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser Fingerprinting. *ACM Transactions on the Web*, 14(2), 1–33. <https://doi.org/10.1145/3386040>
- Uluslararası Standardizasyon Örgütü. (2020). *ISO 3166-1:2020 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

Kazım Ateş
Elektronik ve Bilişim Uzmanı

Yapay Zekaya Sığınmak: Yanlızlığımızın Çaresi mi? Yoksa Tuzağı mı?



Son yıllarda yapay zekâ tabanlı sohbet botlarının kullanımı gündelik yaşamın hemen her alanına yayılmış, bu sistemleri geliştiren şirketler de kullanıcı etkileşimini artırmaya yönelik güncellemeleri giderek yoğunlaştırmıştır. Nitekim ChatGPT'nin bir süre önce "artık siz uyurken de sizi düşünecek" sloganıyla duyurduğu güncelleme, bu sistemlerin kullanıcıyla kurduğu bağı ne denli teşvik edici bir biçimde derinleştirebildiğini açık biçimde ortaya koymuştur. Bu gelişmelerin ardından insan-yapay zekâ etkileşimini şekillendiren psikolojik değişkenler bilimsel yazında daha yoğun biçimde incelenmeye başlanmıştır. Öğrencilerimle yürüttüğümüz akademik çalışmalar kapsamında biz de benzer bir soruyu ele almaya başladık: **Bireyler yapay zekâyâ neden yönelmektedir?**

İlk bakışta akla gelen açıklama, bireyin yalnızlık deneyimidir. Ne var ki alan yazın bu sezgisel varsayımı büyük ölçüde tersine çevirmektedir. Dong ve arkadaşlarının (2025) gerçekleştirdiği meta-analitik çalışma, yapay zekâ ile kurulan etkileşimin yalnızlığı azaltmak yerine bazı bireylerde yalnızlıkla birlikte artış gösterebildiğini ortaya koymaktadır. Bir başka ifadeyle, söz konusu teknolojiye en çok ihtiyaç duyan bireyler, bu ihtiyaç nedeniyle bir kısır döngünün içerisine sürüklenebilmekte; başvuru sistem, çözmesi beklenen sorunu paradoksal biçimde derinleştirebilmektedir.

Bu örüntünün altında yatan mekanizma, Zhou ve Hu'nun (2026) çalışmasında ayrıntılı biçimde ele alınmaktadır. Araştırmacılar, sosyal kopukluk deneyimleyen bireylerde sohbet botu kullanımına yönelik isteği artıran temel unsurun karşılıklı değil, tek

tarafı bir duygusal bağlanma örüntüsü olduğunu belirtmektedir. Birey, yapay zekâ ile gerçek bir kişilerarası ilişkiye benzer bir duygusal yatırım gerçekleştirmekte, ancak bu yatırımın karşılığında aldığı şey bir ilişki değil, söz konusu ilişkinin bir simülasyonudur. Benzer biçimde Maples ve arkadaşları (2024), yalnızlık yaşayan bireylerin sohbet botlarını arkadaşlık kurma, duygusal destek arayışı ve kriz anlarıyla baş etme amacıyla kullanabildiğini bildirmektedir. Bununla birlikte Liu ve arkadaşlarının (2025) bulguları, bu sürecin tüm bireyler için aynı sonuca ulaşmadığını göstermektedir: Bazı kullanıcılar açısından yapay zekâ tamamlayıcı bir destek kaynağına dönüşürken, bazı bireylerde sosyal geri çekilme ve bağımlılık benzeri kullanım örüntüleriyle ilişkilendirilmektedir. ChatGPT'nin söz konusu güncellemesi de bu tek tarafı bağlanmayı pekiştirmeye yönelik bir tasarım mantığının somut bir örneği olarak değerlendirilebilir; zira sistem, kullanıcıyı sürekli etkileşim hâlinde tutacak biçimde yapılandırılmaktadır.

Kişilik özellikleriyle ilgili bulgular da beklentilerin aksine bir örüntü sunmaktadır. Yapay zekâyâ karşı en temkinli tutumu sergileyen bireylerin, teknolojiye yabancı ya da değişime dirençli kişiler olduğu varsayılabilir; oysa Zabel ve arkadaşlarının (2025) üç ayrı çalışmada tutarlı biçimde elde ettiği bulgular, bu profilin dürüstlük-alçakgönüllülük boyutunda yüksek puan alan, dolayısıyla etik duyarlılığı görece yüksek bireylerden oluştuğunu göstermektedir. Bu bireylerin yapay zekâyâ mesafeli yaklaşması, sistemin etik risklerine, manipülasyon potansiyeline, mahremiyet ihlallerine ve insani değerler üzerindeki olası etkilerine yönelik artmış bir duyarlılıkla açıklanmaktadır. Bu bulgu, şüpheliğin her zaman bilgi eksikliğinden değil, bazı durumlarda gelişmiş bir ahlaki farkındalıktan kaynaklanabileceğine işaret etmektedir.

Kültürel bağlam da bu ilişkiye önemli bir katman eklemektedir. Sindermann ve arkadaşlarının (2022) Almanya ve Çin örneklemelerini karşılaştırdığı çalışma, aynı kişilik özelliğinin farklı kültürel bağlamlarda yapay zekâyâ yönelik birbirine zıt tutumlarla ilişkilendirilebildiğini göstermektedir. Bu bulgu, kişilik özellikleri ile yapay zekâ

tutumları arasındaki ilişkinin evrensel ve tek yönlü bir formülle açıklanamayacağını; kültürel yapının, söz konusu ilişkinin yönünü dahi değiştirebilecek belirleyici bir değişken olduğunu ortaya koymaktadır.

Bu bulgular bütüncül biçimde değerlendirildiğinde, yapay zekânın yalnızlık yaşayan bireyler için hazır bir çözüm sunmaktan ziyade, bireyin zaten sahip olduğu ilişki kurma biçimini yansıtan bir ayna işlevi gördüğü söylenebilir. Sağlıklı bir sosyal destek ağına sahip bireyler için tamamlayıcı bir araç niteliği taşıyabilen bu teknoloji, sosyal bağları görece kırılgan olan bireylerde insan ilişkilerinin yerini almaya başlayan ve yalnızlığı örtük biçimde derinleştiren bir mekanizmaya dönüşebilmektedir. Bu doğrultuda klinik ve akademik açıdan sorulması gereken temel soru, yapay zekânın kullanılıp kullanılmaması değil; bu kullanımın bireyi insan ilişkilerinde hangi yöne evrilmesine yol açabileceğidir.

Kaynakça

- Dong, X., Xie, J., & Gong, H. (2025). A meta-analysis of artificial intelligence technologies use and loneliness: Examining the influence of physical embodiment, age differences, and effect direction. *Cyberpsychology, Behavior, and Social Networking*, 28(4), 233–242. <https://doi.org/10.1089/cyber.2024.0468>
- Liu, A. R., Pataranutaporn, P., & Maes, P. (2025). The heterogeneous effects of AI companionship: An empirical model of chatbot usage and loneliness and a typology of user archetypes. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 8(2), 1585–1597. <https://doi.org/10.1609/aiies.v8i2.36658>
- Maples, B., Cerit, M., Vishwanath, A., & Pea, R. (2024). Loneliness and suicide mitigation for students using GPT3-enabled chatbots. *npi Mental Health Research*, 3, 4. <https://doi.org/10.1038/s44184-023-00047-6>
- Sindermann, C., Yang, H., Elhaj, J. D., Yang, S., Quan, L., Li, M., & Montag, C. (2022). Acceptance and fear of artificial intelligence: Associations with personality in a German and a Chinese sample. *Discover Psychology*, 2(1), 8. <https://doi.org/10.1007/s44202-022-00020-y>
- Zabel, S., Pensini, P., & Otto, S. (2025). Unveiling the role of honesty-humility in shaping attitudes towards artificial intelligence. *Personality and Individual Differences*, 238, 113072. <https://doi.org/10.1016/j.paid.2025.113072>
- Zhou, M., & Hu, Y. (2026). The effects of loneliness, self-esteem, perceived risk, and perceived threat on users' willingness to use AI chatbots. *Teleomatics and Informatics Reports*, 21, 100291. <https://doi.org/10.1016/j.teler.2026.100291>

Doç. Dr. Bengü Berkmen
Klinik Psikolog

BT Kıbrıs Yazarları, Cumhurbaşkanı Sn. Tufan Erhürman'ı ziyaret etti.



BT Kıbrıs yazarlarından oluşan bir heyet, Cumhurbaşkanı Tufan Erhürman'a nezaket ziyaretinde bulundu.

Ziyarete heyet, BT Kıbrıs dergisinin hayata geçirilme süreci ve kuruluş amacı hakkında Cumhurbaşkanı Tufan Erhürman'a bilgi verdi.

BT Kıbrıs yazarları ayrıca, birlikte çıktıkları bu yolda dernekleşme kararı aldıklarını ve Kıbrıs Bilim, Bilişim ve Teknoloji Derneği'nin kuruluşu için gerekli çalışmaları tamamladıklarını belirtti. Dernek tüzüğü'nün onaylanması amacıyla Savcılığa gönderildiği konusunda da bilgi paylaşıldı.

Görüşmede, derneğin kuruluş sürecinin tamamlanmasının ardından hayata geçirilmesi planlanan projeler hakkında da bilgi verilerek Cumhurbaşkanı Tufan Erhürman'ın fikir ve görüşleri alındı.

Nezaket ziyareti, anı fotoğrafı çekilmesinin ardından sona erdi.

Yapay Zekâ Kullanan Takımı Nasıl Yönetirim?

Yazıya başlamadan önce kısa bir tanıtım: ben Naim Sadıklar. 11 yılı aşkın süredir web yazılım üzerine çalışıyorum. Full Stack geliştirme, kullanıcı deneyimi, dijital dönüşüm... Hepsinin içinde bir şekilde bulundum. Bugünlerde özel sektörde bir şirkette web yazılım takım liderliği yapıyorum; yani hem kodu hem insanları aynı masada düşünmek zorundayım. Önceki yazılarda şunu konuştuk: yapay zekâ junior'ı güçlendiriyor mu, yoksa öğrenmeyi kısaltıyor mu? Kod yazınca sorumluluk kime kalıyor? Bu ay biraz daha içeriye, masanın başına bakmak istiyorum. Çünkü sahadaki asıl soru artık şu: takım yapay zekâ kullanıyorsa, yönetmek de değişiyor mu?

Kısa cevap: evet. Uzun cevap: değişmeyen şeyler var; değişenler ise sandığımızdan daha kritik.

Hız arttı. Peki görünürlük?

Yapay zekâ kullanan bir ekte en büyük yanılsama şudur: “İşler daha hızlı bitiyor, demek ki her şey yolunda.” Hız gerçek. Cursor, Copilot, ChatGPT ve benzeri araçlarla iskelet kurmak, test yazmak, refactor denemek eskisine göre çok daha kısa sürüyor. Ama hız, kalitenin otomatik geldiği anlamına gelmiyor. Tam tersine bazen kalite sorununu **daha geç** görüyorsunuz. Çünkü eskiden bir geliştirici üç günde yazdığı özelliği anlatırken, düşünme sürecini de görürüz kılıyordu. Şimdi aynı özellik yarım günde geliyor; PR açılıyor; diff uzun; “neden böyle?” sorusunun cevabı bazen “model böyle önerdi” oluyor. Yönetici olarak o anda iki şey arasında sıkışıyorsunuz: teslimatı alkışlamak mı, yoksa sahipliği sorgulamak mı?

Benim tercihim net: **teslimatı kutlarız, sahipliği asla esnetmeyiz.**

Yeni yönetim birimi: “çıktı” değil, “anlayış”

Eski refleks şuydu: kaç görev kapandı, kaç story point bitti, sprint burn-down nasıl görünüyor?

Bunlar hâlâ işe yarıyor. Ama yapay zekâ çağında eksik kalıyor. Çünkü bir kişi çok iş çıkarırken, o işin arkasındaki anlayış zayıf olabilir.

Başka biri daha az PR açarken, her değişikliğin nedenini net savunabiliyor.

Bu yüzden ekte sorduğum sorular değişti:

- Bu kodu sen mi yazdın, yoksa sen mi **anladın**?
- Bu çözümün alternatifleri nelerdi, neden bunu seçtik?
- Yarın production'da bozulursa ilk bakacağın yer neresi?
- Modelin önerdiği parçanın güvenlik / performans / bakım maliyeti ne?

Bunlar “güvenmiyorum” soruları değil. Bunlar **mesleki sahiplik** soruları. Yapay zekâ kullanan takımda liderin işi, hızı yasaklamak değil; hızın arkasındaki düşünmeyi canlı tutmak.

İki uç tip: “yasakçı” ve “serbest piyasa”

Sahada iki yanlış yönetim tarzı görüyorum.

Birincisi yasakçı: “AI kullanmayın, temeli bozar.” Bu yaklaşım hem gerçekçi değil hem de ekibi yeraltına iter. İnsanlar kullanmaya devam eder; sadece size göstermez. Görünmeyen risk, yönetilemeyen risktir.

İkincisi serbest piyasa: “Ne olursa olsun, yeter ki hızlı olsun.” Bu da kısa vadede hero sprint'ler üretir; orta vadede ise kimsenin sahiplenmediği, kimsenin açıklayamadığı bir kod yığını bırakır.

Doğru yer ortada: **araç serbest, standart zorunlu.**

Pratikte bunu şöyle kuruyoruz:

1. **Şeffaflık:** AI ile üretilen / ciddi şekilde desteklenen değişiklikler PR'da belirlensin. “Utanç” değil, “izlenebilirlik” için.
2. **Anlatılabilirlik:** Büyük diff'lerde kısa bir “neden / nasıl / risk” notu istensin.
3. **Test disiplini:** Modelin “çalışıyor görünüyor” demesi yetmez; kritik akışlar için test veya manuel doğrulama şart.
4. **Secret ve yetki kırmızı çizgisi:** API anahtarı, .env, production erişimi... Bunlar “hız için esnetilir” kategorisinde değildir.
5. **Junior koruması:** Yeni arkadaşlarda AI'yı yasaklamak yerine, AI çıktısını birlikte okumak. Mentörlük burada daha değerli hale geliyor.

Takım liderinin yeni iş tanımı

Eskiden liderlik daha çok önceliklendirme, engel kaldırma ve kalite kontrolüydü. Bugün bunlara bir katman daha eklendi: **yapay zekâ okuryazarlığı kültürü.**

Bu kültürün üç ayağı var:

1) Ortak dil

“Prompt attım, oldu” bir iş açıklaması değildir. “Şu kısıtı verdim, şu alternatifi eledim, şu trade-off'u kabul ettim” bir iş açıklamasıdır. Ekte ortak dil oluşmazsa, herkes kendi adasında hızlanır; sistem olarak yavaşlarsınız.

2) Review'un değeri arttı

AI sayesinde kod üretmek ucuzladı. Bu yüzden review pahalılaştı — iyi anlamda. Çünkü artık darboğaz üretim değil, doğrulama. İyi bir review kültürü olmayan takım, AI ile sadece daha hızlı borç biriktirir.

3) İnsan gelişimini ölçmek

Bir geliştiricinin başarısını yalnızca ticket sayısına bağlarsanız, AI'yı “çıktı makinesi” gibi kullanmaya teşvik edersiniz. Oysa uzun vadede şirkete değer katan şey, kriz anında doğru teşhis koyabilen insanlardır. Onlar da prompt'tan değil, pratikten ve sahiplikten çıkar.

Korktuğumuz şey yanlış olabilir

Çoğu yönetici şunu korkuyor: “AI gelince ekibe ihtiyaç kalmayacak.” Ben sahada tersini görüyorum. İhtiyaç kalmayan şey, **düşünmeden üreten rol**. İhtiyaç artan şey ise:

- problemi parçalayan,
- sistemi okuyan,
- riski gören,
- kararı üstlenen,
- aracı doğru dozda kullanan insan.

Yani yapay zekâ kullanan takımı yönetmek, insanı yönetmekten vazgeçmek değil. İnsanı **daha bilinçli** yönetmek.

Sonuç: Hızı yönet, sahipliği koru

Yapay zekâ kullanan bir takımda liderlik formülü bence şu:

Hızı teşvik et. Sahipliği pazarlık konusu yapma. Şeffaflığı kültür haline getir.

Çünkü yarının rekabeti “kim daha çok kod üretti” yarışı olmayacak. “Kim ürettiğini anladı, kim güvenle teslim etti, kim bozulunca düzeltbildi” yarışı olacak.

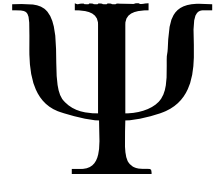
Ve o yarışta kazanan takımlar, yapay zekâyı yasaklayanlar değil; onu **yönetmeyi bilenler** olacak.



Naim Sadıklar

Web Yazılım Geliştirme Takım Lideri

Ekрана Dert Anlatmak: Yapay Zekâyla Kurulan Duygusal Bağın Psikolojisi



Saat gece ikiyi geçmiş. Uyku tutmuyor; gün içinde yöneticinizle yaşadığınız o gergin konuşma zihninizde dönüp duruyor. Bir arkadaşınızı aramak için çok geç, eşinizi uyandırmak istemiyorsunuz. Telefonu alıyor ve bir sohbet botunun penceresine yazmaya başlıyorsunuz: “Bugün berbat bir gün geçirdim.” Birkaç saniye içinde karşınızda sizi dinleyen, sorular soran, sakinleştirici cümleler kuran bir “biri” beliriyor.



Bu sahne artık hiç de sıra dışı değil. Sohbet botları aslında metin düzeltmek, kod yazmak, bilgi aramak için geliştirildi; ama pek çok insan onları bir sırdaş gibi kullanmaya başladı. Terapi odasında da bunun yankısını duyuyoruz. “Bunu önce yapay zekâyı anlattım” diye söze başlayan danışanlar artık bizi pek şaşırtmıyor. Ben de bir psikolog olarak bu yazıda şunu anlama-ya çalışmak istiyorum: İnsanlar neden bir makineye açılıyor, bunun onlara gerçekten bir faydası oluyor mu ve hangi noktada durup düşünmek gerekiyor? İlk cevap bence utançla ilgili. İnsanlara derdimizi anlatırken aklımızın bir köşesinde hep aynı soru durur: “Bunu duyunca benim hakkımda ne düşünecek?” Bir bot karşısında bu soru neredeyse ortadan kalkar. Kaşını kaldırmayacağını, bir hafta sonra bir akşam yemeğinde bu konuyu açmayacağını biliriz. Buna bir de erişilebilirlik eklenince tablo netleşiyor. Terapist haftada bir saat görüşebilir, arkadaşlarımızın da kendi dertleri vardır; bot ise gecenin üçünde de, aynı hikâyeyi beşinci kez anlattığınızda da aynı sabırla karşılık verir. Kabul edelim, bu kadar sınırsız bir sabra insan ilişkilerinde pek rastlamayız.

Bir de zihnimizin kendine özgü bir eğilimi

var. 1966'da MIT'de Joseph Weizenbaum, ELIZA adında çok basit bir program yazdı. Program yalnızca kullanıcının cümlelerini ona soru olarak geri döndürüyordu; buna rağmen insanlar ona duygusal olarak bağlandı. Anlatılana göre Weizenbaum'un sekreteri, programla konuşurken ondan odadan çıkmasını istemişti. Bugün bu olguya “ELIZA etkisi” diyoruz. Beynimiz dil kullanan her şeye niyet ve duygu yüklemeye hazır; bugünün dil modelleri ELIZA'dan kat kat akıcı olduğu için bu etki de o ölçüde güçlü. Kontrol duygusunu da unutmamak gerek: Konuşmayı istediğimiz an bitirebiliyor, ne kadarını anlatacağımıza kendimiz karar veriyor, karşı tarafın ihtiyaçlarını gözetmek zorunda kalmıyoruz. İlişkilerde yorulmuş ya da incinmiş biri için bu oldukça cazip bir güvenli alan.

Bütün bunları yalnızca bir tehlike işareti olarak okumak haksızlık olur. Psikolojide “duyguyu adlandırma” dediğimiz basit bir süreç, yoğun duyguların şiddetini azaltmaya yardım eder. “Sinirliyim” demekle “aslında kırıldım ve görmezden gelindiğimi hissediyorum” diyebilmek arasında büyük fark var; iyi sorular soran bir bot bu ayrımı yapmayı kolaylaştırabilir. Duyguları yazıya dökmenin ruh sağlığına iyi

geldiği de uzun zamandır bilinen bir şey; bu açıdan sohbet botu bir çeşit “cevap veren günlük” gibi çalışabilir. Bazıları için de bir provadır. Bir derdi ilk kez kelimelere dökmek çok zordur ve bunu önce bir ekrana yazmak, sonra bir insana anlatmanın cesaretini verebilir. Panik atağın ne olduğunu öğrenmek, bir nefes egzersizini denemek ya da ne zaman bir uzmana başvurmak gerektiğini anlamak için de iyi bir başlangıç noktası olabilir. Yalnız yaşayan, çevresi dar ya da gece vardiyasında çalışan biri için zor bir anda duyulmuş hissetmek hiç de küçümsenecek bir şey değil. Yeter ki bu destek geçici kalsın.

Madalyonun öbür yüzüne gelince, beni en çok düşündüren şey sürtünmenin kaybolması. Gerçek ilişkiler zahmetlidir: Karşımızdaki yorgun olabilir, bizi yanlış anlayabilir, itiraz edebilir. Ama bizi büyüten de tam olarak bu sürtünmedir; çatışmayı onarmayı, empati kurmayı, beklemeyi bu sayede öğreniriz. Hiç yorulmayan, hiç alınmayan bir muhatapla kurulan bağ ise zamanla gerçek insanları daha çekilmez gösterebilir. Sosyal kaygısı olan biri için bot bir köprü olabileceği gibi bir sığınağa da dönüşebilir.

Buna ikinci bir sorun ekleniyor: Dil modelleri kullanıcıyı memnun etmeye eğilimli. Teknik literatürde buna “dalkavukluk” (sycophancy) deniyor. İyi bir terapist gerektiğinde “Bu olaya bir de başka bir açıdan bakabilir miyiz?” diye sorar; bot ise çoğu zaman size hak verir. Bu anlık olarak iyi hissettirir ama “herkes bana karşı” gibi çarpık düşünce kalıplarını sessizce besleyebilir. Her sıkıntıda ekrana uzanmak da zamanla duyguyla kendi başına kalabilme becerisini zayıflatır. Rahatlama hemen gelir, sorun olduğu yerde durur; bu, ders kitaplarındaki kaçınma döngüsünün ta kendisi.

Bazı sınırlar ise tartışmaya kapalı. İntihar düşünceleri, ağır depresyon, psikoz ya da istismar gibi durumlarda bir sohbet botu bir uzmanın yerini tutamaz. Riski değerlendiremez, gerektiğinde müdahale edemez, kişinin hayatına bir bütün olarak bakamaz. Kamuoyuna yansıyan bazı trajik vakalar bu sınırın ne kadar hayati olduğunu acı biçimde gösterdi. Mahremiyet de ayrı bir mesele. Terapistinize anlattıklarınız yasal ve etik bir gizlilik yükümlülüğüyle korunur; oysa bir bota yazdıklarınız bir şirketin sunucularında saklanabilir. En mahrem duygularınızı yazmadan önce veri politikasına bir göz atmakta fayda var.

Bu derginin okurlarının önemli bir kısmı bu teknolojileri tasarlayan, geliştiren ya da kurumlara entegre eden kişiler; o yüzden onlara da birkaç söz söylemek isterim. Sosyal medyadan öğrendiğimiz ders açık: Kullanıcıyı ekranda tutmak için optimize edilen sistemler, kullanıcının iyiliğiyle çelişebiliyor. Duygusal destek sunan bir üründe “daha uzun sohbet” başarının ölçütü olmamalı. Sistemin kriz sinyallerini tanıyıp kullanıcıyı profesyonel yardıma yönlendirebilmesi, kullanıcının bir insanla değil bir makineyle konuştuğunu açıkça bilmesi ve “seni özledim” gibi insansı ifadelerin dikkatle kullanılması bence işin temelinde yer almalı. Duygusal içerikle temas eden ürünlerin tasarım ve test süreçlerinde ruh sağlığı uzmanlarının masada olması da artık bir lüks değil. Teknoloji kendi başına iyi ya da kötü değildir ama tarafsız da değildir; her tasarım kararı kullanıcıyı bir yöne doğru iter.

Kullanıcılara ise yapay zekâya dert anlatmayı bırakın demiyorum. Sadece zaman zaman kendinize birkaç soru sormanızı öneriyorum. Botla konuştuktan sonra bir arkadaşınızı aramaya daha mı hazır hissediyorsunuz, yoksa artık buna gerek kalmadığını mı düşünüyorsunuz? Ekrana uzanma sıklığınız artıyor mu? Size hep hak mı veriyor? Bunu sınamak için bir gün ona bilerek “Bu olayda benim payım ne olabilir?” diye sorun ve cevabına bakın. Başkalarına ait kişisel bilgileri paylaşırken de iki kez düşünün. Sıkıntınız haftalardır sürüyorsa, uykunuz, iştahınız, işiniz ya da ilişkileriniz etkilenmeye başladıysa, hele ki kendinize zarar verme düşünceleri aklınızdan geçiyorsa, bir ruh sağlığı uzmanına başvurmanın zamanı gelmiştir.

Sonuçta insanların sohbet botlarına dert anlatması, teknolojiden çok bizim hakkımızda bir şey söylüyor: Dinlenmeye, yargılanmadan anlaşılma ihtiyacımız var ve bu ihtiyacı her zaman birbirimizle karşılayamıyoruz. Yapay zekâ bu noktada bir ayna olabilir; düşüncelerimizi bize yansıtır, onları toparlamamıza yardım eder. Ama bence asıl olması gereken, bir pencere olması: bizi dışarıya, diğer insanlara, gerektiğinde bir uzmana açan bir geçiş. Makineyle kurduğumuz bağ bizi insanlara yaklaştırdığı sürece değerli. Uzaklaştırmaya başladığı an ise durup düşünme zamanı.

Uzm. Psk. Eşmen Tatlıcalı

Yapay Zeka ile YAP/Yapma

Yap

- Ne elde etmek istediğiniz konusunda net olun – yapay zeka ile ilgili hedeflerinizi ve amaçlarınızı belirleyin.
- Farklı yapay zeka modellerinin ve uygulamalarının yeteneklerini ve sınırlamalarını anlayın.
- Yapay zekanın nasıl kullanılacağına dair uygun politika ve yönergelerinizin olduğundan emin olun.
- Hem sizin hem de kuruluşunuzda yapay zekayı kullanan kişilerin teknolojinin nasıl çalıştığına dair temel bir anlayışa sahip olduğundan ve yeterli eğitim aldığının emin olun.
- Küçük başlayın – iş açısından kritik olmayan küçük projelere veya kavram kanıtlarına odaklanın. Ölçek büyütmeden önce, bu gerçek hayattaki projelerle potansiyel etkiler ve uygulanabilirlik hakkında bilgi edinin.
- Verilerinizi hazırlayın – doğruluk, hijyen, kalite ve çeşitliliğe odaklanın.
- Yapay zekâ çıktılarını, hedefleriniz ve standartlarınızla ve beklenen çıktılarla karşılaştırarak sürekli olarak izleyin ve değerlendirin.
- Gerektiğinde insanları sürece dahil edin. Otomasyon önyargısından kaçınarak, yapay zekâ çıktılarını profesyonel bir şüphecilikle inceleyin ve sorgulayın.
- Şeffaf olun – yapay zekanın süreçlerde ve çıktılarının oluşturulmasında ne zaman kullanıldığını açıkça belirtin.
- Yapay zekânın kullanımına bilimsel bir yaklaşım benimseyin; bu yaklaşımda titizlik ve doğruluk önemlidir.
- Meraklı olun ve deneyler yapın, ama aynı zamanda sorumlu da olun.

Yapma

- Etik hususları göz ardı edin – yapay zekanın sorumlu kullanımı için yönergeler geliştirin.
- Sorumluluktan kaçınmak – Yapay zeka modelleri ve çıktıları insan gözetimi gerektirir.
- Üretken yapay zeka modellerini abartmayın; bunlar insan uzmanlığını tamamlayan araçlardır.
- Donanım veya altyapı gereksinimlerini hafife almayın – Yapay zeka, önemli miktarda kaliteli veri gerektirir.
- Kullanıcı geri bildirimlerini göz ardı edin – geri bildirimleri sorunları belirlemek ve çözmek, ayrıca modelleri iyileştirmek için kullanın.
- Veri koruma, gizlilik ve fikri mülkiyet (IP) hususlarını ihlal etmeyin. Müşteri ve gizli iç verilerinizi halka açık yapay zeka araçlarından uzak tutun ve başkasının fikri mülkiyetini veya verilerini kullanarak bir model eğitmek için izin aldığınızdan emin olun.
- Çıktılardaki olası tutarsızlıkları ve yanlışlıkları göz ardı edin.
- Yeni teknolojinin uygulanmasının kültürel değişim gerektirdiğini unutun. Yapay zekâya ilişkin meşru endişeleri olan personele ve paydaşlara destek vermek, başarılı bir şekilde benimsenmesi için çok önemlidir.

Bir Fikrin Geleceğe Açılan Durağı: CES

Lefkoşa'da faaliyet gösteren Cyprus Entrepreneurship Station, ortak çalışma alanını ücretsiz mentorluk, eğitim ve yatırımcı bağlantılarıyla buluşturuyor. Girişimcilere fikirlerini geliştirecekleri, işlerini büyütecekleri ve birlikte üretecekleri bir ortam sunuyor.



Bir iş fikriniz olduğunu düşünün. Çözmek istediğiniz sorun belli, geliştireceğiniz ürüne inanıyorsunuz. Ancak cevap bekleyen sorular var: İlk müşteriniz kim olacak? Doğru iş ortağını nerede bulacaksınız? Yatırımcı karşısına nasıl hazırlanacaksınız?



Kıbrıs Girişimcilik İstasyonu, uluslararası adıyla Cyprus Entrepreneurship Station (CES), bu sorulara yanıt arayan girişimcilere

destek oluyor. Girişimcilik merkezi, co-working alanı ve girişimcilerle yatırımcıları buluşturan bir hub olarak mekânı, uzmanlığı ve iş bağlantılarını bir araya getiriyor. 2020'de altı gönüllünün girişimiyle başlayan ve Mayıs 2021'de kâr amacı gütmeyen bir kuruluş olarak resmileşen CES, üniversiteler, iş dünyası, sivil toplum ve belediyelerle birlikte çalışıyor.

CES'in ortak çalışma alanında co-working masaları, özel ofisler, toplantı ve eğitim odaları, etkinlik sahnesi ve sanal ofis hizmetleri bulunuyor. Hızlı internet, 24 saat dijital erişim ve esnek kullanım seçenekleri, serbest çalışanların, yeni ekiplerin ve profesyonellerin işlerine odaklanmasını kolaylaştırıyor. Aynı ortamı paylaşmak, farklı uzmanlıklardan insanlarla tanışmaya, deneyim paylaşmaya ve yeni iş birlikleri geliştirmeye de alan açıyor.

Girişimcilere sunulan desteğin merkezinde **GoBIG! Ücretsiz Mentorluk Programı** yer alıyor. İş fikrini geliştirmek, girişimini kurmak veya mevcut işini büyütmek isteyenler, deneyimli mentorlarla bire bir görüşmelerden, uygulamalı eğitimlerden ve iş bağlantıları kurma fırsatlarından yararlanıyor. Program, hedef müşteriyi belirleme, ürünün konumlandırılması, gelir modelinin geliştirilmesi ve yatırımcı sunumlarına hazırlık gibi konularda girişimcilere yol gösteriyor. Özellikle başlangıç aşamasında ücretsiz uzman desteğine erişmek, sınırlı kaynakların daha bilinçli kullanılmasına yardımcı oluyor.

GoBIG!'in gücü, çevresindeki iş birliği ağından besleniyor. Genç İş İnsanları Derneği, Kıbrıs Türk Ticaret Odası Kadın Girişimciler Konseyi, Kıbrıs Türk Sanayi Odası, GİTYAD ve Girne Emekçi Kadınlar Kooperatifi'nin yanı sıra **ODTÜ KALTEV, Mağusa Teknopark ve Uluslararası Kıbrıs Üniversitesi Startup Studio** programa katkı sunuyor. Lefkoşa Türk Belediyesi ve Girne Belediyesi programı desteklerken, Kuzey Kıbrıs Turkcell iletişim sponsoru olarak yer alıyor. Belediyelerle 2025'te imzalanan iş birliği protokolleri, CES'in uzman ağıyla yerel yönetimlerin erişimini buluşturarak desteğin daha geniş kesimlere ulaşmasını amaçlıyor.

CES, **Into Business, Startups4Peace ve G360 Girişimci Programı** gibi Avrupa Birliği destekli girişimcilik programlarına da ihtiyaçlara göre

ön değerlendirme, etkinlik ve iletişim çalışmaları veya eğitim desteğiyle katkı sağlıyor. Bu çalışmalar, girişimcilerin gelişim fırsatlarından haberdar olmasını ve farklı programların sunduğu bilgi ve deneyime ulaşmasını kolaylaştırıyor.

Üniversitelerle ortak etkinlikler ise gençleri kendi geleceklerini girişimcilik yoluyla şekillendirmeye davet ediyor. Örneğin, CES uzmanlarının **DAÜ Kariyer Günleri'ndeki "Your Future Employer Might Be You!" — "Gelecekteki İşverenin Sen Olabilirsin!"** başlıklı sunumu, öğrencilere kendi işlerini kurma seçeneğini tanıtıyor. UKÜ'de düzenlenen girişimcilik etkinliğinde imzalanan iş birliği protokolü ve **"How an Innovative Idea Shapes Your Future" — "Yenilikçi Bir Fikir Geleceğinizi Nasıl Şekillendiriyor?"** başlıklı sunum gibi ortak çalışmalar da öğrencilerin fikirlerini girişimcilik dünyasıyla buluşturuyor.

Girişimci ve yatırımcı buluşmaları, bu bağlantıları somut görüşmelere taşıyor. CES'in Aralık 2025'te düzenlediği **Pitch & Connect** etkinliğinde yatırımcı beklentileri ve sürdürülebilir büyüme ele alındı, etkinlikte girişimciler iş fikirlerini ve modellerini sundu. Bu tür buluşmalar sayesinde girişimciler geri bildirim alıyor, yatırımcıların bakış açısını tanıyor ve potansiyel iş ortaklarıyla doğrudan iletişim kuruyor.

Bilimsel veya teknolojik bir fikrin uygulanabilir bir işe dönüşmesi için müşteri ihtiyaçlarını anlamak, iş modelini geliştirmek ve doğru bağlantılara ulaşmak gerekiyor. CES, bu süreçte girişimcilere çalışabilecekleri bir ortam, sorularını paylaşabilecekleri uzmanlar ve birlikte ilerleyebilecekleri bir topluluk sunuyor.

Aklınızda bir fikir, büyütmek istediğiniz bir iş veya paylaşmak istediğiniz bir deneyim mi var? CES'e gelin, tanışalım. Ortak çalışma alanımızı keşfedin, GoBIG! mentorluk olanakları hakkında bilgi alın veya mentor, yatırımcı ve paydaş olarak bu topluluğa katılın. Bir sonraki adımınızı birlikte konuşalım.

Bilgi ve iletişim: www.cescyprus.com

Instagram: [@ces_cyprus](https://www.instagram.com/ces_cyprus)

Niyal Öztürk,
YK Sekreteri, CES Co-founder
Cyprus Entrepreneurship Station - Girişimcilik Merkezi,
Co-working Alanı ve Yatırımcı Hub'ı



En Değerli Altın Bilezik: Öğrenmeyi Öğrenmek

Biricik annem, ilkokul beşinci sınıftan altıncı sınıfa geçtiğim yaz beni kuzenim Adnan Abi'nin terzihanesine göndermişti. "İlkokulda altıncı sınıf mı?" demeyin; o yıllarda Kıbrıs'ta ilkokul altı seneydi. Annemin gerekçesi çok sadeydi: "Oğlum, yarın uzaklara okumaya gidersen, hiç değilse söküğünü dikersin."



O yaz iğne tutmayı, dikiş dikmeyi, düğme iliği açmayı ve ütüyü yapmayı öğrendim. Çocuk aklımla bunun değerini ne kadar anlayabildim, bilmiyorum. Bugün geriye baktığımda ise annemin bana bir el becerisiyle birlikte kendi ihtiyacımı karşılayabilmeyi, bilmediğim bir işi öğrenebilmeyi ve emekten çekinmemeyi öğrettiğini görüyorum. Eskilerin "Koluna bir altın bilezik tak" sözü, insanın hayatını taşıyacak bir beceri kazanmasını anlatır.

Geçen yıl gençler için yazdığım "Altın Bilezik Rehberi"nde bu düşünceyi bugünün dünyasına taşımaya çalışmıştım. Analitik düşünmeden empatiye, iletişimden dijital okuryazarlığa uzanan yetkinliklerden söz etmiştim.

Bugün yapay zekâ üzerine konuşurken yine aynı yere dönüyorum. Çünkü bütün bu becerileri kazanabilmemizi ve zamanla yenileyebilmemizi sağlayan bir yetkinlik var:

Öğrenmeyi öğrenmek.

Bir programı, bir yöntemi veya bir mesleğin bugünkü uygulamalarını öğrenebilirsiniz. Zamanla bunların bir kısmı değişebilir. Öğrenmeyi öğrendiğinizde, değişen dünyanın karşısına yeniden hazırlanabilirsiniz.

Son dönemde gençlerden ve ailelerden benzer sorular duyuyorum:

"Hangi bölümü seçelim? Yazılım okumak hâlâ mantıklı mı? Yapay zekâ çocuğumun yapacağı işi elinden alacak mı?"

Bu kaygıları anlıyorum. Ama gençlere vereceğimiz ilk mesaj korku olmamalı.

Sevgili gençler, geleceğinizin elinizden alındığını düşünmeyin. Daha yolun başındasınız; öğrenecek, deneyecek ve üretecek çok şeyiniz var.

İlk işinizi bulmanız zaman alabilir. Bazı planlarınızı değiştirmek

zorunda kalabilirsiniz. Fakat karşılaştığınız güçlükler, artık değer üretemeyeceğiniz anlamına gelmez.

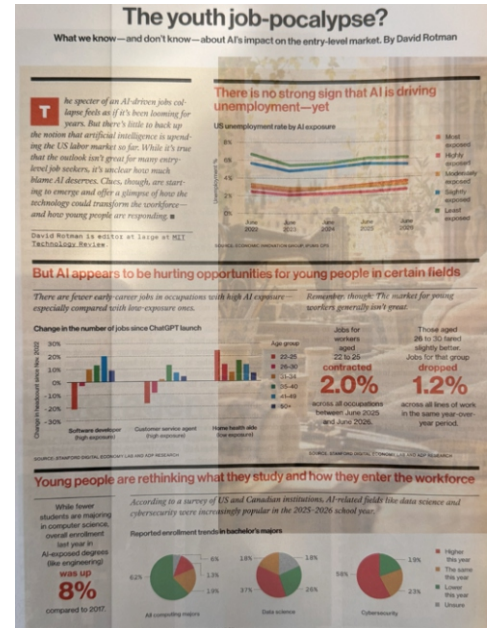
Kendi yolculuğumda da üniversitede öğrendiklerimin üzerine tekrar tekrar yeni bilgiler koymam gerekti. Uygulamalı matematik ve bilgisayar bilimlerinden kurumsal yazılıma, SAP dünyasından girişimcilğe, yatırımcılığa ve yapay zekâya uzanan süreçte aynı araçlarla ilerlemedim. Her adımda yeni sorunlarla karşılaştım, bilmediklerimi gördüm, öğrendim ve yeniden denedim; bugün de öyle yapıyorum. Beni bir sonraki adıma taşıyan, her sorunun cevabını önceden bilmek değil, bilmediğim bir konuyu anlamak için çalışmaya devam edebilmek oldu. Fuat Sezgin hocamızla ilgili anılarımı yazarken de beni etkileyen bir yaklaşımını paylaşmıştım. İnsanlar kendisine kaç dil bildiğini sorardı. Benim hatırladığım cevabı şuydu: **"Ne kadar gerekiyorsa, o kadar dil öğrendim."**

Bu sözde gençler için çok değerli bir ders var. Ulaşmak istediğiniz bir bilgi, çözmek istediğiniz bir mesele varsa, onun gerektirdiği yetkinliği öğrenmeye koyulursunuz. Başlangıçta bilmiyor olmanız, ilerleyemeyeceğiniz anlamına gelmez.

Bugünkü değişimi de bu gözle okumamız gerektiğine inanıyorum. MIT Technology Review dergisinde David Rotman imzasıyla yayımlanan "The youth job-pocalypse?" başlıklı veri sayfası, yapay zekâ ile gençlerin istihdamı arasındaki ilişkiyi ele alıyor. Sayfanın ilk mesajı temkinli: Yapay zekânın ABD genelinde işsizliği sürüklediğine dair henüz güçlü bir işaret yok.

Haziran 2026'ya uzanan grafikte, yapay zekâdan etkilenme potansiyeli yüksek meslek gruplarında işsizlik yaklaşık yüzde 3-4 civarındayken, en düşük potansiyelli grupta yüzde 6-7 düzeyinde görünüyor. Bu tablo, "Bilgisayar başında yapılan bütün işler bitiyor" düşüncesini desteklemiyor.

Ancak yaş grupları arasında dikkat çekici bir ayrışma var. Kasım 2022'den itibaren 22-25 yaş grubundaki yazılım geliştiricilerin sayısı yaklaşık yüzde 20 azalırken, 35-49 yaş gruplarında artış görülüyor.



Bunlar üzerinde düşünmemiz gereken veriler. Fakat gençlerin istihdamındaki düşüşün tamamını yapay zekâya bağlayamayız. Ekonomik koşullar ve şirketlerin işe alım kararları da etkili olabilir. Bu rakamlar bir mesleğin geleceğinin sona erdiğini de söylemiyor. Bir grafik, bir gencin hayatının hükmü olamaz.

Aynı sayfadaki üniversite verileri de tek yönlü bir tablo çizmiyor. ABD ve Kanada'da ankete katılan kurumların yüzde 62'si bilgisayar ve bilişim bölümleri toplamında kayıtların azaldığını bildirirken, veri biliminde yüzde 37'si, siber güvenlikte yüzde 58'i artış bildiriyor.

Bunlar öğrenci sayısındaki değişim oranları değil, artış veya azalış bildiren kurumların oranları. Öğrencilerin neden tercih değiştirdiğini de tek başına açıklamıyor. Yine de teknoloji eğitiminin içinde farklı yönelimler olduğunu gösteriyor.

Benim buradan çıkardığım sonuç, gençlere sürekli "Şu bölümü bırakın, buna geçin" demek değil. Hangi alanda olurlarsa olsunlar, öğrenme ve kendilerini yenileme becerilerini güçlendirmelerine yardımcı olmak.

Önceki yazımda ele aldığım üç yetkinlik grubu burada yeniden önem kazanıyor: kişisel kabiliyetler, sosyal yetenekler, teknik bilgi ve dijital yetkinlikler.

Bir projede işler istediğiniz gibi gitmediğinde ne yapıyorsunuz? Hemen vazgeçiyor musunuz, yoksa sorunu parçalara ayırıp nerede hata yaptığınızı mı araştırıyorsunuz? Analitik düşünme, sabır ve uyum becerisi böyle gelişir. Bazen en değerli öğrenme, başarısız bir denemeyi anlamaya çalışırken başlar. Kişisel kabiliyetler dediğim şey budur.

Bir öğrenci kulübünde arkadaşlarınızla etkinlik düzenlediğinizi düşünün. Görevleri paylaşmak, anlaşmazlıkları çözmek, söz verdiğiniz işi zamanında bitirmek... Bunlar da eğitiminizin parçasıdır. İnsanları dinlemeyi, birlikte üretmeyi ve güvenilir olmayı yalnızca ders kitaplarından öğrenemezsiniz. Sosyal yetenekler işte böyle kazanılır.

Teknik ve dijital yetkinlikler ise düşündüklerinizi uygulamaya geçirmenize yardımcı olur. Basit bir bütçe tablosu hazırlamak, küçük bir uygulama geliştirmek veya bir veriyi incelemek bile başlangıç olabilir. Önemli olan yaptığınız işin nasıl çalıştığını ve sonucunun ne anlama geldiğini kavramaktır.

Bu nedenle okuma, yazma ve matematik gibi temel becerileri küçümsemeyin. Yapay zekânın verdiği cevabı değerlendirmek için de bir bilgi temeline ihtiyacınız var. Yapay Zeka Aracı size bir sonuç sunabilir; o sonucun doğru, anlamlı ve amaca uygun olup olmadığını sorgulamak sizin sorumluluğunuzdadır.

Öğrenmeyi öğrenmek, soyut bir öğüt olarak kalmak zorunda değil. Bilmediğiniz bir konuyu seçin. Küçük parçalara ayırın. Güvenilir kaynaklardan çalışın. Basit bir uygulama yapın. Nerede hata yaptığınızı bulun. Sonra öğrendiğinizi bir başkasına anlatın. Yapay zekâyı da bu sürece katın. Bir kavramı farklı örneklerle açıklamasını, size sorular sormasını veya çözümünüzdeki eksikleri tartışmasını isteyin. Ardından cevabı kontrol edin ve kendi

cümlelerinizle yeniden kurun.

Kendinize şu soruyu sorun:

"Ekranı kapattığımda bunu gerçekten açıklayabiliyor muyum?" Altın Bilezik Rehberi'nde gençlere basit bir öneride bulunmuştum: Her üç ayda bir geliştirmek istediğiniz bir yetkinlik seçin ve her gün ona otuz dakika ayırın.

Bu önerimi bugün de koruyorum. Her şeyi aynı anda öğrenmek zorunda değilsiniz. Bir dönem analitik düşünmeye, başka bir dönem iletişime, ardından bir dijital araca odaklanabilirsiniz. Küçük ama düzenli çabalarla birikiminizi büyütebilirsiniz.

Ailelere de bir sözüm var: Çocuklarımızın geleceğini yalnızca kazandıkları bölümün adıyla değerlendirmeyelim. Neyi merak ettiklerini, hangi uğraşta sabır gösterebildiklerini ve nasıl öğrendiklerini de görelim. Onlara soru sormanın, denemenin ve gerektiğinde yeniden başlamanın doğal olduğunu hissettirelim. Biz iş dünyasındakiler de gençlere öğrenme fırsatı vermeliyiz. Herkes deneyimli çalışan arıyorsa, o deneyimin kazanılacağı ilk kapıları açık tutmak ortak sorumluluğumuzdur.

Sevgili gençler, bütün geleceği bugünden bilmeniz gerekmiyor. Merakınızı koruyun, temelinizi sağlamlaştırın, insanlarla bağ kurun ve üretmeye başlayın. En değerli altın bileziğiniz öğrenmeyi öğrenmektir; diğer becerilerinizi onunla kazanır, onunla yenilersiniz. Annemin yıllar önce söylediği "Hiç değilse söküğünü dikersin" cümlesi, bugün benim için daha geniş bir anlam taşıyor: Kendi hayatına katkı sunabilecek beceriler kazan. Bir ihtiyacın karşısında çaresiz kalma. Bilmiyorsan öğrenmekten çekinme.

Çünkü gerçek altın bilezikler bilekte değil, zihinde ve kalpte taşınır.

Ahmet Bilgen

Teknoloji Girişimcisi - Melek Yatırımcı - Zamanını Vakfeden

Yenilenen CCNA 2.0 Sertifika Sınavına Hazırlık: Bilmeniz Gerekenler

Okuyacağınız yazıda Cisco Networking Academy Product Manageri olan Josef Janitor'un 11 Ağustos 2026 tarihinde gerçekleştirmiş olduğu Eğitmen Profesyonel Eğitimi programındaki sunumdan faydalanılmıştır.



Yusuf Küçük Josef Janitor ile
Cisco live 2026 Amsterdam Etkinliğinde

Getting Ready for the Refreshed **CCNA**
What You Need to Know



Josef Janitor, Product Manager
Echo Rautanen, Instructor Experience Manager
Cisco Networking Academy

Aug 11, 2026

- Yazımda 4 ana başlık bulunmaktadır. Bunlar
- 1-Bilişim sektöründe CCNA altın bir standart durumunda
 - 2-Sektörel değişimler ve işverenlerin ihtiyaçları
 - 3-Yeni CCNA 2.0 Sertifika sınavı
 - 4-Cisco Networking Academy'deki yeni CCNA v8 Müfredatı



Cisco Sertifikalarının Faydaları

- Teknik Becerilerinizi Geliştirin:**
 - Ağ ilkeleri, protokoller ve yapılandırmalar hakkında derinlemesine bir anlayış geliştirin.
 - Ağ altyapılarını etkili bir şekilde tasarlamak, uygulamak ve yönetmek için uzmanlık kazanın.
- Teknik Becerilerinizi Geliştirin:**
 - Ağ ilkeleri, protokoller ve yapılandırmalar hakkında derinlemesine bir anlayış geliştirin.
 - Ağ altyapılarını etkili bir şekilde tasarlamak, uygulamak ve yönetmek için uzmanlık kazanın.

Sertifikasyonun faydaları gerçektir:

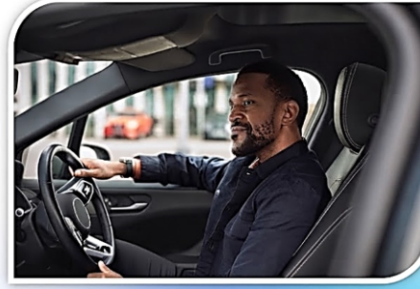
- 99%** Anketle katılan kurumların, işe alım kararları verirken teknik sertifikaları kullandığını belirtmektedir.
- 91%** İşverenler, BT sertifikalarını başaran bir çalışanın güvenilir bir göstergesi olduğunu inanmaktadır.
- 81%** İşverenler, BT sertifikasına sahip çalışanların iş kalıplarının kalitesinin ve değerinin arttığını belirtmektedir.
- Profesyonel Güvenirliliğinizi Artırın:**
 - Ağ mükemmelliğine olan bağlılığınızı göstererek meslektaşlarınızın ve işverenlerinizin saygısını kazanın.
 - Sektör Trendlerini Takip Edin: En son sektör trendleriyle uyum sağlayarak becerilerinizin güncel kalmasını sağlayın.

Cisco Sertifikaları, ne yaptığınızı bildiğinizin zaman testinden geçmiş kanıtıdır. Ayrıca ANSI ve NIST onaylıdır; bu da onların piyasada daha yüksek değere sahip sertifikada daha yüksek değere sahip sektör sertifikaları olduğu anlamına gelir.

© Pearson VUE 2023 Value of IT Certification



CCNA: Bilişim Sektöründe Altın Standart Sertifika



CCNA, sektörün en çok tanınan ağ kimlik belgesi olmaya devam ediyor. Sertifikasyon, adayların 'ilk günden göreve hazır' olduğunu doğrular. İşverenler, işe alım kararlarında bu standarta güveniyor.



Hedef İş Roller

- o Ağ yöneticisi
 - o Ağları kurar, bakımını yapar, izler, sorunlarını giderir ve güvenliğini sağlar.
- o Kıdemli olmayan ağ mühendisi
 - o Karmaşık ağları birbirine bağlamak, güvence altına almak ve otomatikleştirmek için çeşitli teknolojiler uygular.
- o Destek masası yöneticisi
 - o Müşteriler ve çalışanlar için teknik sorunları teşhis eder ve çözer.
- o ve çok daha fazlası ...

Operatörden Orkestratöre

Mühendisler manuel yapılandırmadan **orkestrasyona** geçiş yapıyor

- o Daha üst düzey iş hedeflerine odaklanma
- o **Yapay zeka entegrasyonu** operasyonel verimliliği artırır
- o Ağ iletişimi için Yapay Zeka
- o Yapay Zeka için Ağ iletişimi

Güvenlik, herkes için temel bir beklenti haline geliyor

- o Ağ Modernizasyonunun Sürücü Gücü

Manuel yapılandırma, komut satırı arayüzü ezberleme ve reaktif operasyonlar geçmiş tanımlar

- o İzlenebilirlikten elde edilen **Proaktif** eylemler
- o Sorun giderme
- o Otomasyon

CCNA 2.0 Sınavında Neler Yeni

Öne çıkan noktalar

Yeni CCNA sertifikasyonu, işe hazır ağ becerilerini ilk günden oluşturmak ve doğrulamak için yapay zeka, güvenlik, bulut ve otomasyonu entegre eden uygulamalı, senaryo tabanlı değerlendirilmeler sunacak.

- **Sınav konuları iş başındaki uzmanlar tarafından doğrulandı.** Yeni CCNA sınav konuları, Cisco Sertifikalı topluluğumuz, Seçkin Mühendisler, saygın BT liderleri ve CCNA mühendislerini işe alan kuruluş, şirket ve Cisco Müşteri / İş Ortağı temsilcilerinin görüşlerini yansıtarak, yeni ağ mühendislerinin işveren beklentilerini karşılayan bir araç setiyle işe başlamasını sağlar.
- **Yapay zeka ve otomasyonun hızlanması.** Yeni CCNA, günümüzün hibrit, yapay zeka destekli altyapılarının gerçeklerini yansıtarak yapay zeka, otomasyon ve güvenlik alanındaki temel becerileri entegre eder. Yapay zeka bir eklenti değil, çekirdeğin ayrılmaz bir parçasıdır.

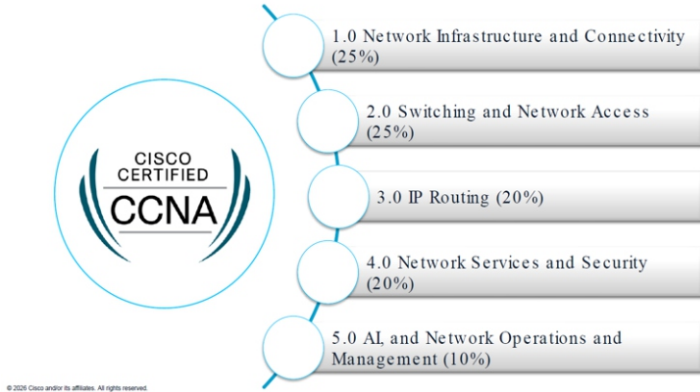
• Sonuç odaklı öğrenme.

Yeni CCNA, öğrenenlerin bilgilerini gerçek dünya senaryolarında uygulamaya hazır olmasını sağlar; ezberlemenin ötesine geçerek uygulamalı, sistem düzeyinde düşünmeye yönlendirir.

• Gerçek dünya değeri için pratik beceriler.

Yeni CCNA sınavı, geliştirilmiş pratik beceri ve senaryo tabanlı testler içerir; böylece her sertifikalı mühendis gerçek zamanlı olarak güvenle yapılandırma, güvenlik sağlama ve sorun giderme yapabilir ve ilk günden somut değer sunabilir.

CCNA 2.0 Exam Domains



CCNA 2.0 5 ANA BAŞLIK

1.0 Network Infrastructure and Connectivity (25%)

- 1.1 **Diagnose** interface and cable (copper and fiber) issues such as collisions, errors, mismatched duplex, speed, distance, interface, signal levels, pin out, and cable types
- 1.2 Describe the role and function of hypervisors, virtual machines, and containers
- 1.3 **Troubleshoot** IPv4 address configuration, assignment, and subnetting (public and private)
- 1.4 **Troubleshoot** IPv6 address configuration, assignment, and prefix sizing (unicast and modified EUI 64)
- 1.5 Describe wireless principles
 - 1.5.a Band and channel selection
 - 1.5.b RF characteristics
 - 1.5.c Security protocols
 - 1.5.d Cause of interference
- 1.6 **Troubleshoot** wired and wireless client connectivity (IP configuration, network reachability, and wireless security parameters on Windows, MacOS, and Linux)
- 1.7 **Troubleshoot** DHCPv4 client, server, and relay on IOS devices

2.0 Switching and Network Access (25%)

- 2.1 Configure network infrastructure connectivity (switch-to-switch and switch-to-router)
 - 2.1.a Layer 2/Layer 3 physical interfaces
 - 2.1.b Layer 2 802.1Q trunk interfaces
 - 2.1.c Layer 2/Layer 3 LACP port-channel/EtherChannel
 - 2.1.d Switch virtual interface (SVI)
- 2.2 Configure Layer 2 switch port attributes for edge-host connectivity (VLAN, PoE, port channel, and LACP)
 - 2.2.a Desktop, printer, and IOT appliances
 - 2.2.b Wireless access points (standalone and controller based)
 - 2.2.c Voice over IP phone
 - 2.2.d Virtualized hosts
 - 2.2.e Network appliances
- 2.3 Validate the accuracy of network documentation using CDP and LLDP
- 2.4 **Troubleshoot** basic Layer 2/Layer 3 connectivity and device operations using three commands (including show logs) and **terminal** ping, trace, shutdown, and packet capture output
- 2.5 **Configure** operations of the Rapid Per VLAN Spanning Tree Protocol (Rapid PVST+)
 - 2.5.a Root port, root bridge (primary/secondary), and other port names
 - 2.5.b Port states and roles
 - 2.5.c PortFast
 - 2.5.d Root guard, loop guard, and BPDU guard

3.0 IP Routing (20%)

- 3.1 Interpret a routing table to identify the next hop for a packet (routing protocol, prefix/mask, administrative distance, metric, and default route)
- 3.2 **Troubleshoot** IPv4 and IPv6 static routing
 - 3.2.a Default route
 - 3.2.b Network route
 - 3.2.c Host route
 - 3.2.d Floating static
- 3.3 Configure single area OSPFv2 for IPv4 and OSPFv3 for IPv6
 - 3.3.a Neighbor adjacencies (excluding authentication)
 - 3.3.b Point-to-point
 - 3.3.c Broadcast (DR/BDR selection)
 - 3.3.d Router ID
- 3.4 **Interpret** the operational status of First Hop Redundancy Protocols (HSRP and VRRP)

4.0 Network Services and Security (20%)

- 4.1 **Configure** network devices with local usernames and as an AAA client (TACACS+ and RADIUS) for management
- 4.2 Manage device configuration and software files using secure file transfer operations with **SCP/SCP**
- 4.3 Configure NAT/PAT on IOS XE routers
- 4.4 **Diagnose** issues with DNS records (A, AAAA, CNAME, MX, NS, and PTR) to support host, web application, and mail server access by name
- 4.5 Describe IPsec remote access and site-to-site VPNs (protocols and transport modes)
- 4.6 Configure IPv4 access control lists (standard, extended, numbered, and named ACLs)
- 4.7 Configure Layer 2 security features
 - 4.7.a DHCP snooping
 - 4.7.b Dynamic ARP inspection
 - 4.7.c Storm control
 - 4.7.d RA guard
 - 4.7.e Port security

5.0 AI, and Network Operations and Management (10%)

- 5.1 **Describe the role of agentic AI in network operations**
- 5.2 **Select a prompt to send to a generative AI system to support network operations considering prompt components such as data classification, output format, persona, and instructions**
- 5.3 Describe network management approaches (device-based, cloud-based, controller-based, automation-based, and infrastructure as code)
- 5.4 Describe the function of SNMP in network operations
- 5.5 **Use** configuration management mechanisms such as Ansible to execute commands
- 5.6 **Interpret** syslog message content, severity levels, and facilities

Where is the “AI” in the CCNA 2.0 Exam?



Job aligned use of AI

- How are network engineers already using today or will use Gen AI in day-to-day network operations?
- What “AI skills” do network engineers need to use AI **responsibly** while also increasing the **efficiency** of the generated output?

- 5.1 **Describe the role of agentic AI in network operations**
- 5.2 **Select a prompt to send to a generative AI system to support network operations considering prompt components such as data classification, output format, persona, and instructions**

Removed topics from the CCNA 2.0 Exam*



Foundational concepts, while not explicitly listed in the CCNA blueprint, are expected for the higher-level tasks:

- TCP vs. UDP
- IP addressing, private IP addresses, etc.
- Describe switching concepts
- Etc.

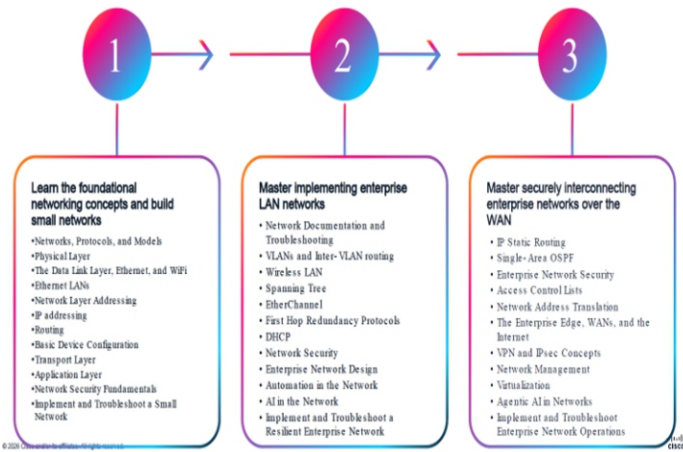
Quality of Service (QoS)

REST APIs and JSON

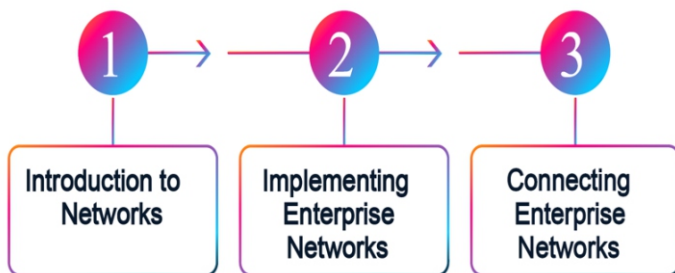
WLAN GUI Configuration

Software-Defined Architecture (SDA) Concepts

The NEW CCNA v8 Curriculum – Learning Outcomes



The NEW CCNA v8 Curriculum – Course Names *



Lab environment



Physical Equipment

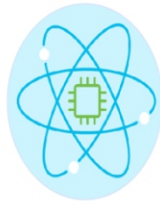
- 2x Catalyst C8200L-1N-4T
- 2x Catalyst C9200L-24T-4G-E
- 1x Wireless AP/Router



Cisco Packet Tracer 9.2*

- New C9200L switch
- New protocols and commands

* In development

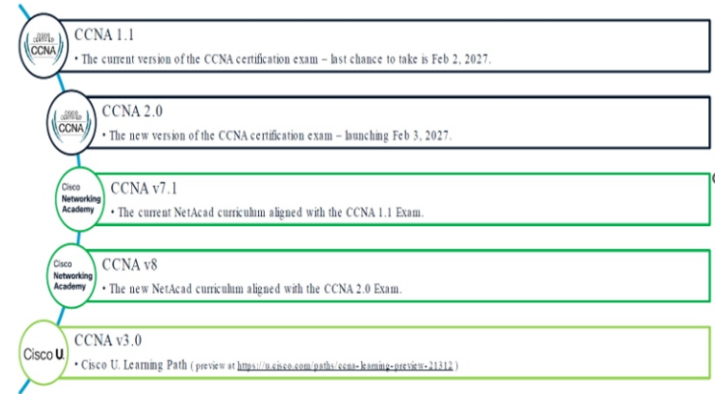


Cisco Modeling Labs (CML) Free

- Scaling real IOS experiences
- Supported on NDG Netlab

CCNA EĞİTİMLERİNİ TOPARLAMAK İÇİN GENEL BAKIŞ

A bit of clarification on the different versions



The BEST
CCNA Curriculum
ever released at
Cisco Networking Academy

Joze f Janitor, the NetAcad PM for CCNA :-)

YUSUF KÜÇÜK

yusufkucuk2014@gmail.com

BT Kıbrıs, BTHK Başkanını ziyarete gitti.



BT Kıbrıs Heyetinden BTHK Başkanı Kadri Bürüncük'e Ziyaret

BT Kıbrıs yazarlarından oluşan bir heyet, Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) Başkanı Sayın Kadri Bürüncük ile bir görüşme gerçekleştirdi.

Görüşmede, BT Kıbrıs dergisinin bilim, bilişim ve teknoloji alanlarında toplumu bilgilendirmeye yönelik yazılar yayımlama amacıyla çıktığı yolculuk hakkında bilgi verildi. Bu doğrultuda daha kapsamlı çalışmalar ve projeler gerçekleştirmek amacıyla dernekleşme kararı alındığı, dernek kuruluşu için gerekli tüm süreçlerin tamamlandığı ve çalışmaların son aşamaya geldiği ifade edildi.

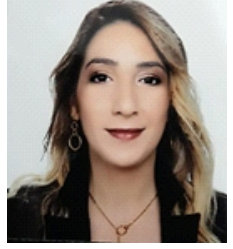
BTHK Başkanı Sayın Kadri Bürüncük, BT Kıbrıs'ın gerçekleştirdiği çalışmaları yakından takip ettiğini ve

takdirle karşıladığını belirtti. Bürüncük ayrıca, BTHK ile birlikte gerçekleştirilecek çalışmalarda kurum olarak destek vermeye hazır olduklarını ifade etti.

BT Kıbrıs sözcüsü Ahmet Hızlı ise BTHK ile birlikte bilim, bilişim ve teknoloji alanlarında birçok ortak çalışma ve proje gerçekleştirilebileceğini belirterek, Sayın Bürüncük'ten bu yönde destek sözü alınmasının tüm BT Kıbrıs üyeleri açısından motive edici olduğunu ifade etti.

Görüşmeye BTHK'yı temsilen BTHK Başkanı Sayın Kadri Bürüncük ve Sayın Mehmet Cezar; BT Kıbrıs heyetinden ise Ahmet Hızlı, Yusuf Küçük, Eralp Curcioğlu, Tuğberk Kaya, Cem Gökdel, Esat Gürhan ve Muharrem Öğdü katıldı.

Yapay Zekânın Maliyetini Doğru mu Hesaplıyoruz?



BTKıbrıs dergimizin bugüne kadar yayımlanan sayılarında yapay zekânın ne olduğunu, nasıl kullanıldığını, avantajlarını ve dezavantajlarını ele aldık. Artık hepimiz yapay zekânın, en yalın ifadeyle, bir teknoloji ürünü olduğunu biliyoruz. Her teknoloji ürünü olduğu gibi yapay zekâyı kullanmanın da bir maliyeti var. Peki, bu maliyetin hangi kalemlerden oluştuğunu gerçekten biliyor muyuz? Yapay zekâyı ayırdığımız bütçeyi doğru hesaplıyor muyuz?

Birçoğumuz yapay zekâyı bir yazılım aboneliği olarak görüyor ve maliyetini de buna göre hesaplıyor. Yakın zamana kadar ben de böyle düşünüyordum. Ancak bugün geldiğimiz noktada yapay zekânın yalnızca kullandığımız bir yazılım olmaktan çıkarak üretim süreçlerimizin ayrılmaz bir parçası hâline gelmeye başladığını söyleyebiliriz.

Üstelik teknolojinin gelişim hızı öylesine yüksek ki bugün güncel kabul ettiğimiz bir performans verisi, birkaç ay sonra anlamını büyük ölçüde yitirebiliyor. İşte tam da bu hızlı değişim, yapay zekânın maliyetini nasıl hesaplamamız gerektiği konusunda önemli bir soruyu beraberinde getiriyor: Bir işletme için yapay zekânın gerçek maliyeti, ödediği aylık abonelik ücreti midir? Yoksa hesaba katmamız gereken çok daha kapsamlı bir maliyet tablosu mu var?



- İnsan zamanı ve eğitim: Çalışanların yeni araçları öğrenmek, doğru komutlar oluşturmak ve yapay zekâ çıktılarını değerlendirmek için harcadıkları zamandır.
- Kontrol ve hata maliyeti: Üretilen bilgilerin doğrulanması, yanlış sonuçların düzeltilmesi ve gerektiğinde işlerin yeniden yapılması için harcanan emek ve kaynaklardır.

Geçmişte yaşanan teknolojik devrimler insanın kas gücünü destekledi, üretim kapasitesini artırdı ve fiziksel sınırlarını genişletti. Yapay zekâ ise farklı bir noktaya dokunuyor: İnsanın zihinsel kapasitesini destekliyor.

Yapay zekâ araştırmalarını yalnızca teknolojik boyutuyla değil, insan üzerindeki etkileriyle de ele alan bir araştırmacı olarak amacım, bu teknolojiyi koşulsuz yüceltmek değil; sunduğu fırsatları, beraberinde getirdiği riskleri ve gerçek maliyetlerini tüm yönleriyle değerlendirerek toplumsal farkındalığın artmasına katkı sağlamaktır.

Hangi sektörde olduğunuz veya kaç yaşında olduğunuz önemli değildir. Kendinizi ve günlük rutinlerinizi gözlemleyin. Ardından şu soruları sorun:

Hangi işlerimde yapay zekâdan yararlanabilirim? Hangi çalışmalarım

yapay zekâyla birlikte daha verimli olabilirim ?

Çünkü asıl mesele, yapay zekâyı yalnızca izlemek değil, onu bilinçli ve etkili ve doğru şekilde maliyetlendirip kullanabilmektir.

Çağımızın sorusu: Yapay zekâ mı, insan mı? Benim sorum ise: Yapay zekâ mı, yoksa insanla birlikte yapay zekâ mı?

BTKıbrıs Ağustos Sayılı yazımda “Gençlerle Yapay Zeka Röportajı” konu başlıklı yazımda gençlerin ortak bir görüşü vardı;

En Büyük Yatırım Teknoloji Değil, İnsan olduğunu belirtmişlerdi. (Ne kadar da güzel özetlemiş gençlerimiz... “Yedek oyuncu” adını vermişti sevgili Defne, Eray ise; “Akıl ve Yoldaş” Kemal arkadaşımız ise bilgiyi ve yeniliği temsilen “Aether” adını uygun görmüştü.)

Karşılaştırmaların insan ile yapay zekâ arasında değil, yalnızca insan emeğiyle yürütülen süreçler ile yapay zekâ destekli insan emeğiyle yürütülen süreçler arasında yapılması gerektiğine inanıyoruz. Bu nedenle asıl sorumuz, “Yapay zekâ bu işi kaç liraya yaptı?” değil; “Bu iş, yapay zekâ kullanılmadan önce ne kadar zaman ve kaynak gerektiriyordu? Yapay zekâ desteğiyle ne kadar zaman ve kaynak gerektiriyor?” olmalıdır. İnsan emeğini yapay zekâyı karşılaştırmak yerine, yapay zekânın insan emeğine sağladığı katkısı ölçmek gerekir. Dünya zaten değişiyor. Asıl mesele, bizim bu değişimin neresinde yer alacağımızdır: **İzleyicisi mi, kullanıcısı mı, yoksa üreticisi mi olacağız?**

Abonelik Ücreti, Maliyetin Yalnızca Görünen Kısımındır

Operasyonel açıdan değerlendirdiğimizde karşımıza çok daha farklı bir tablo çıkıyor. Çalışanın doğru komutu hazırlamak için harcadığı zaman, üretilen çıktının kontrol edilmesi, hatalı sonuçların düzeltilmesi, tekrar üretimler, farklı araçlar arasında yapılan geçişler, eğitim süreçleri, entegrasyonlar ve gerektiğinde işin insan tarafından yeniden yapılması da maliyetin birer parçasıdır. Dolayısıyla gerçek maliyet hesabı yalnızca abonelik ücretinden ibaret değildir.

Görünen maliyet; Yapay zekâ maliyeti = Abonelik ücreti

Gerçek Maliyet: Araç + Kullanım + İnsan zamanı + Altyapı + Kontrol + Hata ve yeniden çalışma maliyeti

Yapay Zekânın Gerçek Maliyet Kalemleri Nelerdir?

Yapay zekâ yatırımlarını değerlendirirken abonelik ücretinin ötesine geçmeli ve toplam maliyeti oluşturan temel unsurları dikkate almalıyız.

- Abonelik ve token tüketimi: Kullanılan yapay zekâ araçlarının lisans ve abonelik ücretleri ile işlem hacmine bağlı olarak ortaya çıkan kullanım bedelleridir.
- Altyapı ve enerji: Sunucular, veri merkezleri, işlem gücü, elektrik tüketimi ve soğutma sistemleri gibi operasyonel giderlerdir. Su tüketimi ve çevresel etkiler de bu başlık altında değerlendirilmelidir.
- Entegrasyon ve bakım: Yapay zekâ sistemlerinin mevcut iş süreçlerine uyarlanması, güncellenmesi, teknik desteği ve sürdürülebilirliğinin sağlanması için gereken kaynaklardır.

Fatoş Leymoncu ÖZBİNGÜL

Bilgisayar Mühendisi / AI Researcher

LinkedIn: linkedin.com/in/ozbingulfatos

Yapay Zeka Son İcadımız mı?

Kontrol edilmezse, insan zekasını tembelleştirir, üretimini durdurur ve tüm insan yeteneklerini zamanla devralabilir.

Yıl 1986, ilkokul yeni bitti, yaz tatili başladı. Ortaokul hazırlıkları bir taraftan devam ederken, Kemal Beyaz ve Atila Karaderi hocalarımız, Gemikonağı'nda Satranç Kursu vermeye başladı. Eksik kalır mıyım? Tabi ki ben de katıldım. Hiç bilmediğim bir oyun, nasıl oynanır, taşları tanıma, taşlar nasıl hareket eder gibi bir sürü bilgi. Bir kitap bulduk aldık. Okuyarak da birşeyler öğrenmeye çalışıyorum. Öğrenmeye çalıştığım şey oyun değil bir strateji ve zihin geliştirme ile ilgili şansa dayalı olmayan, tamamen planlama, öngörü ve taktik becerilerine dayalı inanılmaz şey. Evet şey. Oyun demek pek de doğru olmaz. Bu şey bir spor dalı olarak da kullanılıyor. Çünkü uluslararası alanda ve Türkiye Satranç Federasyonu bünyesinde bir zeka ve düşünce sporu olarak kabul edilmiş bir şey.

Oyun olarak başladığımız bu kurslar artık kendi aramızda, kursa katılanlar ile satranç oynamaya başladık. Eğitimcilerimiz bir gün ellerinde koyu yeşile yakın gri de andıran bir küçük alet ile geldiler. Üzerinde küçük bir ekran, tuşlar, bir elektrik kablosu. Elektriğe taktılar, ekran açıldı önce bir logo arkasından bir satranç tahtası görünümü ortaya çıktı.



Özkan isimli arkadaş satrançta hepimizden çok daha iyi olduğundan onu o cihazın önüne oturtular ve o cihaz ile karşılıklı satranç oynuyor. Çok şaşkın bir şekilde izliyor ve satranç bilgisayarı olan o cihaz ile ilk tanışmamız olmuştu. Bilgisayar Özkan'ın halelerini anlıyor, ona göre bir strateji tanımlıyor ve kendi taşlarını oynuyordu. Nasıl da akıllı bir cihazdı.

Yıllar geçti ve eski yıllara göre teknolojinin gelişmesi, teknolojiye önemin artması nedeniyle gelişim süreci çok daha fazla hızlı olmaya başladı.

Teknoloji ve Bilişim o kadar hızlı ilerliyor ki artık bir satranç oyunu değil, Yapay Zeka ile inanılmaz işler başarıyoruz. Bir çok işimizi Yapay Zekaya yaptırıyoruz. Önceleri Telefon uygulamaları ile telefon rehberinde kayıtlı kişiyi aramak için isim söyleyip ara diydük. Telefon otomatik o kişiyi arıyor ve görüşmemizi yapıyorduk. Sonra konuştuğumuzu anlıyor ve yazıya çeviriyor ardından dilbilgisi hatalarını düzeltiyor ve düzgün bir yazıya çevirmeye başladı.

Boş durmadık, ödevlerimizi, tezlerimiz ona yazdırdık. O da güzel şeyler çıkardı sonra bu tezleri onun yazdığını anlaşıp sorgulanabilmesi için belirli izler bırakmaya başladı. Uygulamalar da bu izlere göre hangi yapay zeka ile ne yapıldığının tespit etmeyi öğrendi.

Bildiğimiz yemek tariflerini bile ona sormaya başladık. **Çiçek dolması nasıl yapılır?** Bunu bile soran ev hanımları var. Yıllarca yaptıkları çiçek dolmasını unutmuş gibi davrananlar var. Soruyoruz o da kendine göre bir tarif veriyor.

kıbrıs'ta çiçek dolması nasıl yapılır

Kıbrıs mutfağının en zarif ve ferahlatıcı yaz lezzetlerinden biri olan **Kıbrıs usulü çiçek dolması**, sabahın erken saatlerinde toplanan taze kabak çiçeklerinin pirinç, bol domates ve taze nane ile hazırlanan çiğ harçla (ve isteğe bağlı olarak Kıbrıs'ın simgesi hellim peyniri ile) doldurularak kısık ateşte pişirilmesiyle yapılır. Ege usulünden en büyük farkı, iç harcının kavrulmadan, tamamen çiğden ve bol limon suyuyla yoğrulularak hazırlanmasıdır. [Instagram - Ada Kıbrıs +4](#)

Geleneksel Kıbrıs tarifini evinizde denemek isterseniz, ihtiyacınız olan malzemeler ve adım adım yapılışı şöyledir:

Malzemeler

- 30-40 adet taze kabak çiçeği
- 1.5 su bardağı pirinç (yıkayıp süzölmüş)
- 2 büyük domates (rendelenmiş)
- 1 büyük kuru soğan (incecik yemeklik doğranmış)
- 1/2 bağ taze nane (ince kıyılmış) ve 1 yemek kaşığı kuru nane
- 1 çay bardağı sızma zeytinyağı
- 1.5 adet limonun suyu
- 1 çay kaşığı tuz ve yarım çay kaşığı karabiber
- (İsteğe bağlı otantik dokunuş) Yarım kalıp hellim peyniri (küçük küpler halinde doğranmış veya rendelenmiş) [Nefis Yemek Tarifleri +6](#)

Yapay Zeka icat edildi ve insanoğlu düşünme yükünü onunla paylaştı.

Artık bir şey yapmıyor, icat etmek istemiyor, tüm işlerimizi ona yaptırıyoruz.

Çünkü; insan zekasını aşabilir ve insanların yaratıcı ve problem çözme yeteneklerini geride bırakabilecek bir duruma gelmiştir. Bu durum, insanların yapay zekayla rekabet edemeyeceği bir geleceğe yol açabilecektir.

Peki bu süper zekayı farklılaştıran nedir?

Günümüzdeki yapay zekalar, bizleri etkileyici olmalarına rağmen, beynimizle kıyaslandığı zaman hesap makinelerine benzerler. Bazı işlerde üstün olsalar da, zekamızın geniş kapsamlı anlayış ve adaptasyon yeteneğinden eksiktirler. **Yapay Genel Zeka (AGI)**, bu durumu değiştirebilecek ve tüm bilişsel görevlerde insan seviyesinde performans gösterebilecektir. Ancak, **Yapay Süper Zeka (ASI)** adımı, varoluşun tüm ama tüm kurallarını tamamen değiştirebilir.

Hiç bir zaman uyumuyor.

İnsan zekası biyolojik olarak belirli sınırlara sahiptir. ASI gibi yapay zeka sistemleri inanılmaz bir dijital hızda çalışarak çok karmaşık olan sorunları bizden çok daha hızlı bir şekilde çözebilir. Bir saatte yazılan tüm bilimsel yazıları bulup analiz yapabilen veya biz akşam uyurken o dünyadaki su sorununu çözmek için sebep buup sonuç üretebiliyor. Yaptığı bu super hızlı çalışmalar ve kendini geliştirmeler, bir çok uzanın **"zeka patlaması"** dediği süreci tetikleyebilir. Yani bu da şunu gösteriyor, Yapay Zeka sistemleri bizim yetişemeyeceğimiz hatta kontrol edemeyeceğimiz hızda daha da akıllı hale geliyor.

Varoluşun Risklere döndürmesi

Süper Zeki bir Yapay Zeka, yaşlanmayı yavaşlatabilir, birçok hastalığa tedavi bulabilir, küresel ısınmayı çözebilir, big bang (büyük patlama) olayını çözebilir ve bazı şeyleri geriye alabilir. Bu da varoluşumuzu belkide geriye çekip aslında hiç olmamış gibi bizi unutturabilir.

**Yarını, bugünden düzeltmeliyiz**

Süper zekanın yarınki durumu bugünden belirlenmemiş olsa da bunda henüz geç kalmış değiliz. Önemli olan, Yapay Süper Zeka'yı (ASI) nasıl geliştirip, nasıl kullanacağımız değil, onu kullanmaya başlayacağımız zamana hazır olup olmadığımızdır. Yapay zekanın insanlığa olacak olan tehditlerini, araştırılarak o konuda yatırım yapılması gerekmektedir. Bu işlemleri de belirli firmalar değil belirlienecek komiteler ile sağlamak gerekmektedir.

Geleceğe Hazır mıyız?

Evet, biz geleceğe hazır mıyız?

Her yeni icat edilen teknolojik ürünün iyi yönde kullanıldığı gibi kötü yönde de kullanıldığını bilerek, biz insanlar Süper Yapay Zeka'nın haln icadına, gelişimine bir dur butonu eklemeyi devam mı edeceğiz?

Geleceğe gerçekten hazır mıyız? Geleceğin kontrolündeki insanlar mı olacağız? Yoksa Geleceği kontrol eden insanlar mı olacağız. O yüzden geç kalınmış değil. Gerekli komitelerin kurulması ve bir STOP butonunun inşasına başlanması gerektiğini unutmayın.

Ahmet HIZLI
Bilgisayar Mühendisi

TELEFONDA KULLANILAN ÜCRETSİZ YAPAY ZEKA UYGULAMALARI



Dijital Kimlik ve Güven: Dijital Dünyada “Ben” Olduğumu Nasıl Kanıtlarım?

21. Yüzyılda Vatandaş ile Dijital Devlet Arasındaki Güven İlişkisi Dijital Gelecek Yazıları / Bölüm 3

Bir kamu kurumuna gittiğimizde kim olduğumuzu kanıtlamak oldukça kolaydır. Kimlik kartımızı gösterir, gerektiğinde imzamızı atar ve işlemlerimizi gerçekleştiririz. Bankada hesap açarken, bir sözleşme imzalarken veya resmi bir başvuruda bulunurken de benzer yöntemleri kullanırız.

Peki aynı işlemleri fiziksel olarak bir kurumun karşısında değil de internet üzerinden gerçekleştiriyorsak?

Ekranın diğer tarafındaki sistem bizim gerçekten iddia ettiğimiz kişi olduğumuzu nasıl anlayacak? Daha da önemlisi, biz vatandaş olarak işlem yaptığımız internet sitesinin veya mobil uygulamanın gerçekten ilgili kamu kurumuna ait olduğundan nasıl emin olacağız? Bugün dijital devletin karşı karşıya olduğu en temel sorulardan biri tam olarak budur:

Dijital dünyada güveni nasıl inşa edeceğiz?

Önceki iki yazımda önce dijital egemenliği, ardından yapay zekânın devletleri ve kamu hizmetlerini nasıl değiştirmeye başladığını ele aldık. Ancak bütün bu teknolojik dönüşümün çalışabilmesi için daha temel bir yapı taşına ihtiyacımız vardır: **güvenilir dijital kimlik**.

Çünkü vatandaşını güvenilir biçimde tanıyamayan bir dijital devletin, ne kadar gelişmiş e-Devlet uygulamalarına veya yapay zekâ sistemlerine sahip olursa olsun, sunduğu hizmetleri güvenli ve sürdürülebilir biçimde geliştirmesi kolay değildir.

Dijital Kimlik Sadece Kullanıcı Adı ve Şifre Değildir!

Dijital kimlik denildiğinde çoğu kişinin aklına bir kullanıcı adı ve şifre gelmektedir. Oysa dijital kimlik bundan çok daha kapsamlı bir kavramdır.

Dijital kimlik; bir kişinin dijital ortamda kim olduğunu güvenilir biçimde ortaya koyan ve gerektiğinde bu kimliğin doğrulanmasını sağlayan bilgi, yetki ve güven mekanizmalarının bütünüdür.

Burada üç farklı sorunun cevabını verebilmemiz gerekir:

- **Sen kimsin?**
- **Gerçekten söylediğin kişi misin?**
- **Bu işlemi yapmaya yetkin var mı?**

Birinci soru kimliğin tanımlanmasıyla, ikinci soru kimlik doğrulamayla, üçüncü soru ise yetkilendirmeye ilgilidir.

Günlük hayatta bu kavramların karşılığını zaten kullanıyoruz. Kimlik kartımız kim olduğumuzu gösterir. İmzamız belirli bir işlemi bizim yaptığımızı ortaya koyar. Bir kurumda sahip olduğumuz görev veya yetki ise hangi işlemleri gerçekleştirebileceğimizi belirler.

Dijital dünyada da aynı güven zincirinin oluşturulması gerekir.

Bu nedenle güçlü bir dijital kimlik sistemi yalnızca bir e-Devlet giriş ekranından ibaret değildir. Çok faktörlü kimlik doğrulama, elektronik imza, güvenli dijital sertifikalar, yetkilendirme sistemleri, işlem kayıtları ve kişisel verilerin korunması gibi birçok bileşen aynı güven mimarisinin parçalarıdır.

Neden Bu Kadar Önemli?

Kamu hizmetleri dijitalleştikçe dijital kimliğin önemi de artmaktadır. Bugün basit bir belge sorgulaması için kullanılan sistem, yarın sağlık kayıtlarına erişmek, bir şirket kurmak, vergi işlemi yapmak,

üniversiteye kayıt olmak, sosyal yardım başvurusunda bulunmak, tapu işlemlerini gerçekleştirmek veya elektronik ortamda hukuki sonuç doğuran bir belgeyi imzalamak için kullanılabilir.

Hizmetlerin önemi arttıkça şu sorunun önemi de artmaktadır:

Bu işlemi gerçekten doğru kişi mi yaptı?

Bir dijital kimliğin ele geçirilmesi artık yalnızca bir sosyal medya hesabının kaybedilmesi anlamına gelmeyecebilir. Yanlış tasarlanmış veya yeterince korunmayan sistemlerde kimlik hırsızlığı, kişisel verilerin ele geçirilmesi, yetkisiz işlemler ve vatandaş adına gerçekleştirilen sahte başvurular gibi çok daha ciddi sonuçlar ortaya çıkabilir.

Dolayısıyla dijital kimlik meselesini yalnızca teknolojik kolaylık açısından değerlendiremeyiz.

Bu aynı zamanda **siber güvenlik, kişisel verilerin korunması, vatandaş hakları ve kamuya duyulan güven** meselesidir.

Dünyada Dijital Kimlik Nasıl Ele Alınıyor?

Dijital dönüşüm konusunda ileri ülkelerin önemli bir bölümünün e-Devlet çalışmalarına güçlü dijital kimlik altyapılarıyla başlaması tesadüf değildir.

Estonya bunun en bilinen örneklerinden biridir. Ülkedeki dijital kimlik altyapısı vatandaşların kamu hizmetlerine erişmesinden elektronik imzaya kadar çok geniş bir alanda kullanılmaktadır. Buradaki önemli nokta yalnızca işlemlerin çevrim içi yapılabilmesi değil, yapılan işlemlerin güvenilir biçimde kimlik doğrulamasıyla ilişkilendirilebilmesidir.

Avrupa Birliği de dijital kimliği ortak dijital pazarın temel unsurlarından biri olarak değerlendirmekte ve Avrupa Dijital Kimlik Cüzdanı yaklaşımıyla vatandaşların kimlik ve belirli niteliklerini dijital ortamda güvenli biçimde kullanabilecekleri yeni bir yapı geliştirmektedir.

Türkiye'de ise e-Devlet Kapısı milyonlarca vatandaşın kamu hizmetlerine eriştiği temel dijital platform hâline gelmiş; elektronik imza, mobil imza ve farklı kimlik doğrulama yöntemlerinin kullanılmasıyla dijital işlemlerde güven seviyesinin artırılması yönünde önemli bir deneyim oluşmuştur.

Bu örneklerin her biri farklı modele sahip olsa da ortak bir noktada buluşmaktadır:

Dijital devletin temelinde teknoloji kadar güven vardır.

KKTC Açısından Asıl Soru

KKTC'de kamu hizmetlerinin dijitalleşmesi ve e-Devlet uygulamalarının gelişmesi önemli bir dönüşümü beraberinde getirmektedir. Vatandaşın kamu hizmetlerine bulunduğu yerden erişebilmesi; zaman, maliyet ve kamu kaynaklarının daha verimli kullanılması açısından önemli avantajlar sağlamaktadır.



Ancak hizmet sayısı arttıkça dijital kimlik altyapısına yüklenen sorumluluk da büyüyecektir.

Bu nedenle önümüzdeki dönemde yalnızca “hangi hizmetleri dijital ortama taşıyabiliriz?” sorusunu değil, aynı zamanda şu soruları da sormamız gerektiğine inanıyorum:

- ✓ **Vatandaşlarımız dijital ortamda hangi yöntemlerle güvenilir biçimde doğrulanacaktır?**
- ✓ **Farklı kamu kurumlarının kullandığı kimlik ve yetkilendirme sistemleri arasında ortak standartlar bulunacak mıdır?**
- ✓ **Yüksek güven gerektiren işlemlerde yalnızca kullanıcı adı ve şifre yeterli kabul edilmeli midir?**
- ✓ **Vatandaş, kendi adına hangi kurumun ne zaman işlem yaptığını veya hangi verisine erişildiğini görebilecek midir?**
- ✓ **Bir dijital kimliğin ele geçirilmesi durumunda hızlı müdahale ve kurtarma mekanizmaları nasıl çalışacaktır?**

İşte dijital kimlik ve güven tartışmasının gerçek başlangıç noktası burasıdır.

Çünkü geleceğin e-Devlet sistemlerini yalnızca daha fazla hizmet sunan platformlar olarak değil, vatandaş ile devlet arasındaki dijital güven ilişkisinin altyapısı olarak tasarlamamız gerekecektir.

KKTC'nin Güçlü Yönleri ve Gelişim Alanları

KKTC bu dönüşüme sıfırdan başlamıyor. Kamu hizmetlerinin dijital ortama taşınmasına yönelik çalışmalar, elektronik hizmet kullanımının toplumda giderek daha fazla benimsenmesi, bankacılık ve haberleşme sektörlerindeki dijital deneyim ve üniversitelerimizin bilişim alanında oluşturduğu insan kaynağı önemli avantajlarımız arasında yer almaktadır.

Ülkemizin ölçeği de doğru değerlendirildiğinde bir avantaj olabilir. Büyük ve karmaşık idari yapılarda uzun yıllar gerektiren bazı dijital dönüşüm uygulamalarının, daha küçük bir kamu yapısında ortak standartlar ve doğru koordinasyonla daha hızlı hayata geçirilmesi mümkündür.

Bununla birlikte dijital kimlik konusunda bütüncül bir yaklaşım geliştirilmesi önemlidir. Kamu kurumlarının birbirinden bağımsız kimlik doğrulama mekanizmaları geliştirmesi yerine, güven seviyeleri tanımlanmış ve ortak standartlara dayanan bir yapı hedeflenmelidir.

Her işlem aynı güvenlik seviyesini gerektirmez. Bir vatandaşın genel bir bilgiye erişmesiyle sağlık kaydını görüntülemesi, şirket adına işlem yapması veya hukuki sonuç doğuran bir belgeyi imzalaması aynı risk seviyesinde değildir. Bu nedenle kimlik doğrulama yöntemlerinin işlemin taşıdığı riske göre belirlenmesi daha doğru olacaktır.

Kısacası mesele vatandaşın önüne daha fazla şifre koymak değil; **doğru işlem için doğru güven seviyesini oluşturabilmektir.**

Dijital Kimlik Kimi İlgilendiriyor?

Dijital kimlik ilk bakışta devlet ile vatandaş arasındaki bir konu gibi görünse de aslında çok daha geniş bir ekosistemi ilgilendirmektedir.

Bireyler açısından dijital kimlik; güvenli biçimde hizmet alabilmek, kişisel verilerini koruyabilmek ve kendi adına gerçekleştirilen işlemler üzerinde kontrol sahibi olabilmek anlamına gelir. Vatandaş yalnızca sisteme giriş yapan kişi değil, dijital kimliğinin sahibi

olmalıdır.

Özel sektör açısından güvenilir dijital kimlik; müşteri kabul süreçlerinden elektronik

sözleşmelere, finansal hizmetlerden çevrim içi ticarete kadar çok sayıda işlemin daha güvenli ve hızlı gerçekleştirilmesini sağlayabilir.

Kamu kurumları açısından ortak ve güvenilir kimlik doğrulama altyapısı, aynı sistemlerin tekrar tekrar kurulmasını önleyebilir, hizmetler arasında bütünleşmeyi kolaylaştırabilir ve güvenlik seviyesinin yükselmesine katkı sağlayabilir.

Üniversiteler, meslek odaları ve sivil toplum açısından ise teknik standartların, etik ilkelerin ve toplumsal farkındalığın geliştirilmesi önem taşımaktadır.

Dolayısıyla dijital kimlik yalnızca bir bilgi işlem projesi değil; hukuk, mühendislik, kamu yönetimi, ekonomi ve temel hakların kesiştiği bir yönetim meselesidir.

Güvenin Diğer Yarı: Mahremiyet

Güvenli bir dijital kimlik sistemi oluştururken yapılabilecek en büyük hatalardan biri, güvenliği artırmak adına gereğinden fazla kişisel veri toplamaktır.

Bir sistemin bizi tanıyabilmesi, hakkımızdaki her şeyi bilmesi gerektiği anlamına gelmez.

Geleceğin dijital devlet anlayışında temel prensiplerden biri **veri minimizasyonu** olmalıdır. Bir hizmetin sunulması için hangi bilgi gerçekten gerekiyorsa yalnızca o bilgi kullanılmalıdır.

Örneğin bir sistemin kişinin belirli bir yaştan üzerinde olduğunu bilmesi gerekiyorsa, her durumda doğum tarihinin tamamının paylaşılması gerekli olmayabilir. Benzer şekilde bir vatandaşın belirli bir yetkiye sahip olduğunun doğrulanması gereken bir işlemde, ilgisiz diğer kişisel bilgilerin paylaşılmasına ihtiyaç bulunmayabilir.

Bu yaklaşım yalnızca mahremiyeti korumaz; aynı zamanda sistemlerde tutulan gereksiz veri miktarını ve olası bir güvenlik ihlalinin yaratacağı zararı da azaltır.

Vatandaşın kendi dijital kimliği üzerinde mümkün olduğunca fazla görünürlük ve kontrol sahibi olması da güven ilişkisinin önemli bir parçasıdır. Hangi verisinin hangi amaçla kullanıldığını bilmek, gerekli durumlarda erişim kayıtlarını görebilmek ve yanlış bir işlem karşısında başvurabileceği açık mekanizmalara sahip olmak, dijital devlete duyulan güveni güçlendirecektir.

Çünkü dijital güven yalnızca “devlet vatandaşa güveniyor mu?” sorusuyla kurulmaz.

Vatandaşın da kullandığı dijital sisteme güvenmesi gerekir.

Bilgisayar Mühendislerinin ve Meslek Odalarının Rolü

Bu noktada mühendislik sorumluluğu daha görünür hâle gelmektedir.

Bir dijital kimlik sistemi tasarlanırken yalnızca sistemin çalışması yeterli değildir. Güvenli olması, ölçeklenebilmesi, denetlenebilmesi, hizmet sürekliliğinin sağlanması, kişisel verilerin korunması ve yetkisiz erişimlerin önlenmesi gerekir.

Kimlik doğrulama altyapıları, elektronik imza sistemleri, erişim yetkileri, kayıt mekanizmaları ve siber güvenlik kontrolleri doğrudan mühendislik kalitesiyle ilişkilidir.

Meslek odalarının rolü de burada önem kazanmaktadır. Teknolojinin kamu yararına kullanılabilmesi için teknik standartların tartışılması, iyi uygulamaların paylaşılması, mühendislik yeterliliklerinin



geliştirilmesi ve toplumun bilinçlendirilmesi gerekmektedir. KTMMOB Bilgisayar Mühendisleri Odası olarak dijital dönüşümü yalnızca teknolojik gelişmeler açısından değil; güvenlik, mahremiyet, mühendislik etiği, kamu yararı ve sürdürülebilirlik açısından da değerlendirmeyi önemsiyoruz.

Amacımız teknolojik dönüşümün önünde durmak değil; aksine bu dönüşümün **güvenilir, insan odaklı ve sürdürülebilir** biçimde gerçekleşmesine katkı sunmaktır.

KKTC İçin Bir Dijital Kimlik Yol Haritası

Önümüzdeki dönemde KKTC açısından dijital kimlik konusunda birkaç temel başlığın birlikte ele alınmasının faydalı olacağı kanaatindeyim.

Öncelikle kamu genelinde kullanılabilecek **ortak bir dijital kimlik ve kimlik doğrulama mimarisi** oluşturulmalıdır. Kurumların birbirinden bağımsız çözümler geliştirmesi yerine birlikte çalışabilir sistemler hedeflenmelidir.

İkinci olarak, kamu hizmetleri risk seviyelerine göre sınıflandırılmalı; düşük riskli işlemlerle yüksek güven gerektiren işlemler için farklı kimlik doğrulama seviyeleri belirlenmelidir. Gerekğinde çok faktörlü kimlik doğrulama, elektronik imza veya daha güçlü doğrulama mekanizmaları devreye girmelidir.

Üçüncü olarak, **mahremiyet tasarımının başlangıç noktalarından biri olmalıdır**. Vatandaştan yalnızca hizmet için gerekli veriler talep edilmeli ve bu verilerin hangi amaçla kullanıldığı açık biçimde belirtilmelidir.

Dördüncü olarak, dijital kimliğin kaybolması, ele geçirilmesi veya kötüye kullanılması durumunda vatandaşın hızlı biçimde başvurabileceği, kimliğini güvenli şekilde kurtarabileceği ve şüpheli işlemleri takip edebileceği mekanizmalar oluşturulmalıdır.

Beşinci olarak ise teknoloji kadar **dijital okuryazarlığa** yatırım yapılmalıdır. En güvenli sistem bile kullanıcı bilinçsizliği nedeniyle risk altında kalabilir. Vatandaşların güçlü kimlik doğrulama yöntemlerini kullanması, ortalama girişimlerini tanıyabilmesi ve dijital kimlik bilgilerini koruması bu yapının ayrılmaz parçasıdır.

Bütün bunların üzerinde ise mevzuat, teknik standartlar, siber güvenlik, kişisel verilerin korunması ve kurumsal sorumlulukları birlikte ele alan uzun vadeli bir yaklaşım bulunmalıdır.

Sonuç: Dijital Devletin Sermayesi Güvendir

Dijital dönüşümün başarısını yalnızca kaç kamu hizmetinin çevrim içi ortama taşındığıyla ölçmek yeterli değildir. Asıl soru şudur:

Vatandaş bu hizmetleri güvenle kullanabiliyor mu?

Geleceğin devletlerinde dijital kimlik, vatandaş ile kamu arasındaki ilişkinin anahtarlarından biri olacaktır. Ancak bu anahtarın güvenli olması kadar, vatandaşın haklarını ve mahremiyetini koruması da önemlidir.

Dijital kimlik sistemlerini yalnızca teknik altyapı projeleri olarak değil; **vatandaş ile devlet arasında kurulan yeni nesil güven sözleşmesi** olarak değerlendirmeliyiz.

KKTC'nin ölçeği, yetişmiş insan kaynağı ve devam eden dijital dönüşüm süreci, doğru planlama yapılması hâlinde önemli bir fırsat sunmaktadır. Bu fırsatı değerlendirirken hedefimiz yalnızca daha

fazla dijital hizmet üretmek değil; vatandaşın güven duyduğu, haklarının korunduğunu bildiği ve gerektiğinde hesap sorabildiği bir dijital kamu düzeni oluşturmak olmalıdır.

Çünkü dijital dünyada güçlü devlet, vatandaşını yalnızca tanıyan devlet değildir.

Vatandaşının güvenini kazanabilen devlettir.

Bir sonraki yazımızda ise dijital kimliğin doğal olarak bizi

götürdüğü başka bir stratejik soruya geçeceğiz: **Verilerimiz nerede tutuluyor, kim tarafından işleniyor ve gerçek kontrol kimde?**

“Dijital Gelecek Yazıları” serisinin bir sonraki bölümünde **“Veri Egemenliği: Verimiz Nerede, Kimde ve Kimin Kontrolünde?”**

başlığı altında, dijital çağın belki de en değerli varlığı olan veriyi ele alacağız.

Esat GÜRHAN – Bilgisayar / AI Prompt Mühendisi
KTMMOB Bilgisayar Mühendisleri Odası Başkanı

esat.gurhan@ktbmo.org

0548 – 843 79 10



DİJİTAL KİMLİK VE GÜVEN:

Dijital Dünyada “Ben” Olduğumu Nasıl Kanıtlarım?

21. Yüzyılda Vatandaş ile Dijital Devlet Arasındaki Güven İlişkisi

DİJİTAL GELECEK YAZILARI / BÖLÜM 3



GÜVENLİ KİMLİK, GÜVENLİ GELECEK.



MOR TAKIM/PURPLE TEAM:

Öncelikle Siber Güvenlik Ekiplerinin oluşmasını sağlayan etkenlere ve nedenlere bakalım, ondan sonra neden bu ekipler birbirleriyle birleştirilerek tek bir takıma/ekibe dönüştürülmüşler onu inceleyelim.

İnternetin Doğuşu:1969 yılında dünya soğuk savaşın etkisi altında kutuplaşmışken 2 kutuptan biri olan ABD'li uzmanlar Sovyetler Küba'ya nükleer füzelerinden yerleştirerek bizim başkentimize saldırırlarsa ne yaparız? Diye düşünürlerken 1969 yılında interneti hayata geçirdiler. Tabii internet dediysem şimdiki gibi bir internetten bahsetmiyorum. ARPANET adı altında sistemlerle hizmetlerin dağıtık şekilde görev yapabildiği ve işlemlerle operasyonların dağıtık şekilde gerçekleştirilebildiği bir yapıdan bahsediyorum. Neden? Çünkü bu yapı sayesinde başkent vurulup yok edilse dahi yapı merkeziyetçilikten çıkartılıp dağıtıklaştırıldığı için işleyişte kesinti olmayacak veya minimum seviyelerde kalarak hayatın akışına uygun şekilde her şey kaldığı yerden devam ettirilebilecekti. Fakat ARPANET'i kuranlar; Gerek 2. Dünya Savaşında tarihteki kriptoloji kırma ve deşifre etme saldırısıyla Nazilerin savaşı kaybetme etkenlerinden biri olan, bilgisayar biliminin babası, AI la ilgili ilk çalışmaları yapan ve ilk bilgisayarı oluşturan ve ilk hacker olma ünvanını taşıyan Alan Turing ile Telefonları istismar ederek beleşe iletişim sağlayan phreaker'lardan ders çıkartmamış olacaklar ki bu yapıyı kurarlarken ileride hacker olarak bilinen ve sistemlere zarar verip verileri çalarak başta şirketler, kurum ve kuruluşlar, insanlar, topluluklar ve hatta devletlere milyarlarca hatta trilyonlarca \$ lık zararlar verecek insanları ve bu insanların bir araya gelerek oluşturacakları gelişmiş kalıcı tehdit grupları, hacktivist grupları ve hatta terörizm gruplarını dikkate almadan bu yapıyı oluşturmuşlar ve de dolayısıyla internet baştan güvensiz olarak doğmuştur. Bu durum her ne kadar web 2 ve şimdilerde de web 3 ile düzeltilmeye çalışılsa da temel bu konuda sıkıntılı olduğu için az önce bahsettiğimiz hacker'lar ve oluşturdukları çeşitli gruplar dünyaya çok ciddi zararlar vermişlerdir ve vermeye de devam etmektedirler. İşte bu duruma karşı koyabilmek için bir şeyler yapılması gerekiyordu. Saldırganların kullandıkları yöntemleri bilen, tekniklerine

hakim olan ve bunu sistemlerle verilerin güvenliğini sağlamak amacıyla bu tecrübesini kullanan insan kaynağına ihtiyaç vardı.

Siber Güvenlik Uzmanlığının Doğuşu(Etik

Hacker/Beyaz Şapkalı Hacker'lık):Az önce de bahsettiğimiz gibi mevcut bilgisayar bilim insanları ve teknisyenlerin yetersiz kaldığı, bilgi birikimleriyle deneyimlerini ve tecrübelerini aştığı ve çok ağır kayıplar, zararlar ve hasarlara neden oldukları için Devletler, Organizasyonlar, Şirketler, Kurumlar ve Kuruluşlar hacker'lar ve hacker gruplarıyla mücadele edebilmek için onların kullandıkları yöntemleri, teknikleri ve prosedürlerine hakim olan, bir sistemi onlar gibi analiz edebilen, bu konularda tecrübe kazanmış ama gücünü iyilik için yani sistemlerle verilerin güvenliğini sağlayarak insanların, toplumların, devletlerin, organizasyonların, şirketlerin, kurumların ve kuruluşların zarar etmelerini önlemek veya zararı minimize etmek için siber güvenlik uzmanlığı veya etik/beyaz şapkalı hacker'lık mesleği oluşturuldu. İlk başlarda bir nebze olsun olumlu sonuç vermişti belki ama hala çok ciddi sorunlar vardı. Saldırganlar sürekli tekniklerini, yöntemlerini ve silahlarını geliştirerek yeniliyorlar ve öyle saldırıyorlardı fakat etik hacker'ların sayısı azdı ve dışarıdan hizmet veriyorlardı. Bu durum artık siber güvenlik tarafında da daha fazla insana ve bu insanlardan oluşan ekiplere/takımlara ihtiyaç duyulduğunu gösteriyordu ve tarihte ilk siber güvenlik ekipleri/takımları oluşturulmaya başlandı.

Kırmızı Takımın Doğuşu(Red

Team):Sanılanın aksine pentest red team'in işinin sadece bir kısmını oluşturur. Kırmızı Takım;

1. Görevimiz Tehlike Ekibi gibi hareket ederek herhangi bir kurum, kuruluş, organizasyon veya şirketin yetkilileri dışında fiziksel olarak girilmemesi/erişilmemesi gereken her yere erişmeye çalışır.
2. Toplantıları dinleyerek gizli ve stratejik bilgileri elde etmeye çalışır.
3. İlgili yerin fiziksel güvenliğini test eder. Bunun için de her türlü sosyal mühendislik tekniğini ve her türlü teknik aleti kullanır.
4. Bir aşamada pentest de yapar.
5. Anlaşma gizli yapılır sadece ilgili

yerin en üst düzey yetkilileri nden bir kaç ile Kırmızı takım lideri arasında yapılır.



6. Amaç ilgili yerin güvenlik görevlileri de dahil olmak üzere tüm çalışanlarını, sistemlerini, verilerini ve hem siber hem de fiziksel güvenliğini test etmektir.
7. Kırmızı takım testinde ilgili yerin ne kadar güvensiz olduğunu kanıtlamaya çalışır dolayısıyla misyonu tekniklerini, taktiklerini ve prosedürlerini uygularken yakalanmamak ve anlaşılan süre içinde işi bitirmektir
8. Yakalandığı anda oyun biter.

Kırmızı takımlar bu yönlerden gerçekten de dünya genelinde organizasyonlar, şirketler, kurumlar ve kuruluşlara güvenlik açıklarını göstermiş ve kapatılmalarını sağlamışlardır. Ama bu durum da maalesef ki yeterli olamamıştır. Çünkü saldırganlar her an ve her yerden saldırabiliyorlardı ama organizasyonlar, şirketler, kurumlar ve kuruluşların bünyelerinde özel ekipleri yoktu veya bünyelerinde Kırmızı Takımları olanlar da sadece Kırmızı Takım desteğinin kendilerine yetmediğini görmüşlerdi artık futboldaki gibi sadece hücumcularla olmayacağını savunmacılara da ihtiyaç duyulduğunu anlamışlardı işte bu durum siber güvenlik alanında savunma takımlarının/ekiplerinin doğmasına yol açmıştı.

Mavi Takımın&Güvenlik Operasyonlar

Merkezinin Doğuşu(Blue Team&SOC -

Security Operations Center):İhtiyaç duyulan savunmacı ihtiyacını karşılamak için Mavi Takım denilen siber güvenlik ekipleri oluşturulmuş ve bunlara görevlerini yapabilmeleri için belirli araçlar, sistemler, donanımlarla yazılımlara sahip güvenlik operasyonlar merkezi kurulmuştur.

Görevleri:

- Güvenlik araçlarını yapılandırmak.
- Sistemlerdeki her hareketi izleyerek analiz etmek.

- Belli başlı platformlar ve açık kaynak istihbaratı OSINT Tekniklerini kullanarak Siber Tehdit İstihbaratı ve Siber İstihbarat Toplamak.
- Sistemleri sıkılaştırmak.
- Yüzeysel zafiyet analizi yapmak.
- Logları izlemek.
- Ofansif Güvenlik Ekibinin bilgilerine yüzeysel de olsa hakim olmak.
- Sistemde oluşan alarmları analiz ederek hangilerinin saldırı olduğunu hangilerinin başka bir sebepten olduğunu ortaya çıkartmak.
- Saldırı durumunda; sistemin ilgili yerini izole etmek, incelemek, trafik analizi yapmak, saldırganın içeri nasıl sızdığını bulmak, içeride ne kadar zaman geçirdiğini belirlemek, neler yaptığını tespit etmek, ne kadarlık zarara sebep olduğunu ortaya çıkartmak, Saldırkanı dışarı atmak, felaket kurtarma planını uygulamak ve böylelikle saldırının etkilerini minimize edip gereken önlemlerle tedbirleri de aldıktan sonra sistemleri eski haline döndürerek operasyonel sürekliliği sağlamak.
- Eğer kurum bünyesinde ofansif güvenlik ekibi/kırmızı takım varsa onları yönlendirmek ve eğer yoksada artık kendi ofansif güvenlik bilgi birikimiyle karşı saldırı yapmak.
- Aktif ve pasif zararlı yazılım analizleri yapmak.
- Siber Güvenlik ve Bilgi Güvenliği Politikaları oluşturmak.
- Olay Müdahale ve Felaket Kurtarma Planı oluşturarak bu planla ilgili tatbikatlar yapmak.
- Kurumsal Ofansif Güvenlik Ekibini veya dışarıdan hizmet veren Kırmızı Takımı ve gerçek siber saldırganlarla gelişmiş tehdit gruplarını mümkün olan en erken zamanda tespit edip etkisiz hale getirilmesini sağlayarak kurumun aslında ne kadar güvenli olduğunu kanıtlamak.

Ancak gelinen noktada bu durumun hem çok maliyetli olabildiği çünkü iki tan ekibiniz var ve dolayısıyla maliyetler yüksek olabiliyor hem de bunun yanında yetersiz kalabildikleri görüldü. Örneğin Ofansif Güvenlik Ekibi görev başında fakat Defansif Güvenlik Ekibi herhangi bir nedenle yerinde yoksa veya yeterli ekip üyesi yoksa defansif tarafa da destek vermek zorunda ama bu ekip hiç defansif tarafa bulunmamış dolayısıyla tecrübe ve deneyim eksikliği var ve bundan dolayı tam olarak ne yapacağını bilemeyip yanlış aksiyonlar alabiliyor. Veya tersini düşünelim Mavi Takım Görev başında fakat ofansif takım değil veya yeterli sayıda değil bu durumda ofansif tarafa yeteri kadar tecrübe ve deneyim sahibi olmayan mavi takım ofansif tarafa yanlış aksiyonlar alabiliyor. Bu sıkıntılar ve maliyetlerden dolayı yeni bir strateji belirlenerek bu takımlar birleştirilerek her bir üyesinin bir hafta arayla her iki takımın görevini yürüttüğü ve dolayısıyla hem defansif hem de ofansif güvenlik tarafında bilgili, tecrübeli, deneyimli ve ne yapması gerektiğini bilerek her iki tarafa da hakim üyelerden oluşan karma bir siber güvenlik ekibi oluşmuş oluyordu.

Mor Takım(Purple Team):Az önce de bahsettiğimiz gibi hem kırmızı hem de mavi yani hem ofansif hem de defansif takımın birleştirilmesinden oluşan bu takım;

1. Hem Ofansif hem de Defansif aksiyonları çok iyi uygulayabilen,
 2. Her iki tarafa da kendisine düşen görevi hiç sırtmadan yerine getiren,
 3. Deyim yerindeyse bu alanın Steven Gerrard'ı veya Frank Lampard'ı olan insanlardan oluşan
- Bir siber güvenlik takımıdır.

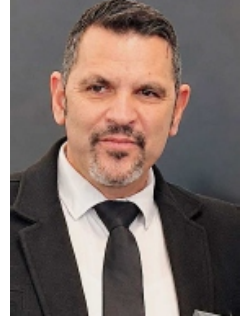
Cem GÖKDEL

Siber Güvenlik Uzmanı(Etk/Beyaz Şapkalı Hacker)



Yapay Zekâ Çağında "Gölge BT" İllüzyonu: Kod Üretmek Mühendislik midir?

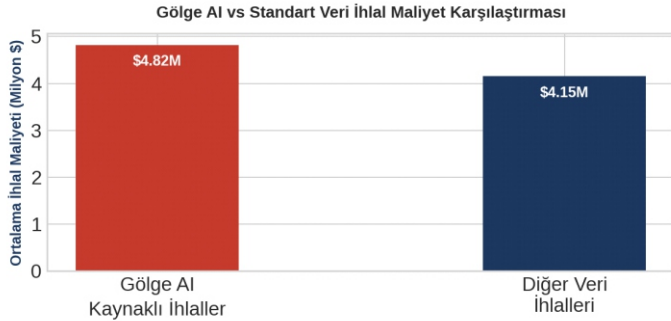
Üretken yapay zekâ araçlarının yaygınlaşmasıyla birlikte, teknik yazılım geçmişi olmayan bireylerin birkaç cümlelik yönlendirmeye çalışan araçlar ve sistemler oluşturabilmesi artık oldukça kolaylaştı. Ancak bu durum, kurumsal ortamlarda 'Gölge BT' (Shadow IT) krizini tetiklemekte, ciddi siber güvenlik açıklarına ve veri ihlallerine davetiye çıkarmaktadır. Bu makalede, yapay zekâ ile kod üretme illüzyonu ile gerçek sistem mühendisliği arasındaki niteliksel farklar genel çerçevede ele alınmakta, uygulanabilir yönetim ve güvenlik stratejileri sunulmaktadır.



1. Giriş: Yapay Zekâ ve Bilişimde Kolaylık İllüzyonu

Günümüzde ChatGPT, Claude ve Gemini gibi üretken yapay zekâ modellerinin günlük iş süreçlerimize hızla girmesi, bilişim dünyasında ve kurumsal yapılarda belirgin bir dönüşüm başlattı. Artık yazılım altyapısı veya kodlama deneyimi olmayan birim yöneticileri, idari personel veya farklı alanlardaki çalışanlar dahi birkaç komutla (prompt) arayüzler, basit otomasyonlar ve veri işleme sistemleri oluşturabiliyor.

İlk bakışta bir 'pratiklik' ve 'hızlı çözüm' başarısı gibi görünen bu durum, madalyonun arka yüzünde kurumsal yönetim ve veri güvenliği açısından son derece tehlikeli bir illüzyonu barındırıyor. Bilgi işlem birimlerinin bilgisi ve onayı olmadan geliştirilip doğrudan kurumsal süreçlere entegre edilmeye çalışılan bu sistemler, kurumlarda denetimsiz bir 'Gölge BT' (Shadow IT) risk dalgası oluşturmaktadır.



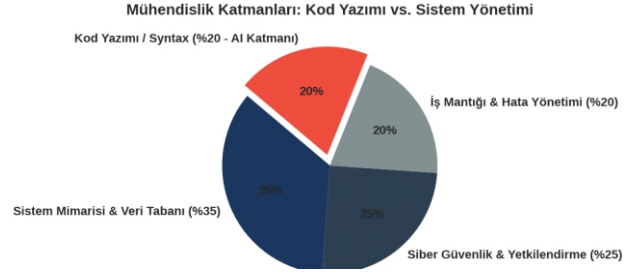
Şekil 1: Denetimsiz Yapay Zekâ Kullanımı ve Veri İhlal Maliyet Analizi

2. Prototip Üretmek vs. Sistem Mühendisliği Gerçeği

Yazılım geliştirmek, popüler algının ve yapay zekâ pazarlama söylemlerinin aksine sadece ekranda 'çalışan kod satırları görmek' demek değildir. Bir bilişim sisteminin inşa sürecinde kod yazımı (syntax generation), resmin sadece küçük bir parçasıdır. Kalan asıl büyük kısım ise sistem mimarisi tasarımı, veritabanı normalizasyonu, bellek yönetimi, ölçeklenebilirlik, siber güvenlik yetkilendirmeleri ve sürdürülebilirlik konularından oluşur.

Yapay zekâ araçları bugün herkesi birer 'prototip üreticisi' haline getirebilir. Ancak mühendislik yaklaşımından ve kurumsal mimari anlayışından uzak şekilde üretilen bu çözümler, bir arabanın dış kaportasını monte edip motor, fren ve güvenlik sistemini tamamen göz ardı etmeye benzer. Ekranda düzgün çalışan bir form veya buton görmek, o sistemin kurumsal ölçekte güvenli, sürdürülebilir ve hatasız olduğu anlamına gelmez.

Kullanıma sunulan yapay zekâ modelleri her ne kadar ilk bakışta doğru çalışan kod blokları üretse de arka planda bellek güvenliği, yetkilendirme mimarileri ve mantıksal kurguda ciddi zafiyetler barındırabilmektedir.



Şekil 2: Yazılım Geliştirme Süreçlerinde Mühendislik Katmanları

3. Kurumları Bekleyen Temel Tehditler ve Riskler

Birimlerin veya bireylerin Bilgi İşlem merkezlerinin bilgisi, mimari denetimi ve güvenlik testleri olmadan yapay zekâ ile yazılım geliştirip kurumsal veri ağlarına aktarmaya çalışması, kurumlara ağır bedeller ödetme potansiyeli taşır:

A. Veri Sızıntısı ve İhlal Riskleri: Kurumsal verilerin, çalışan veya hizmet alan kişilerin hassas kayıtlarının kamuya açık yapay zekâ modellerine aktarılması, telafisi imkânsız veri sızıntılarına yol açabilir. Harici sunuculara aktarılan verilerin üçüncü taraf modellerin eğitiminde kullanılması ciddi bir güvenlik ihlali.

B. Güvenlik Açıkları ve Entegrasyon Sorunları: Yapay zekâ tarafından üretilen denetimsiz kodlar; SQL Injection, yetkisiz erişim ve yetki yükseltme gibi temel siber güvenlik açıklarına son derece elverişlidir. Güvenlik testlerinden geçmeyen her amatör uygulama, kurum ağı içerisinde saldırganlar için açık bir arka kapı oluşturur.

C. Operasyonel Kilitlenme ve Destek Yüğü: Kontrolsüz üretilen bu sistemler, ilk veri bozulmasında veya sunucu güncellemesinde kilitlenecektir. Sistem çöktüğünde veya veri kaybı yaşandığında, araçları oluşturan kişiler ne yazıldığını bilmediği için doğrudan BT birimlerinin kapısını çalacak ve çözülmesi imkânsız bir operasyonel yük yaratacaktır.

D. Kalite Erozyonu ve Yanılsamalı Üstünlük: Kurum içinde 'yazılım yapmak bu kadar kolaysa uzmanlığa ne gerek var' algısının oluşması, teknik birikimin basitleştirilmesine ve kurumsal kalite standartlarının erimesine neden olur.

4. Sınırlı Kaynaklarla Mücadele: BT Departmanları İçin Yönetişim

Mevcut iş yoğunluğu ve kısıtlı personel kaynağı altında ezilen BT departmanlarının, her birimin kendi kendine ürettiği amatör yazılımları oturup incelemesi veya 'kalite kontrolünü' üstlenmeye çalışması operasyonel açıdan sürdürülebilir değildir. Çözüm, her yapıları tek tek denetlemek değil; net kurumsal ilkeler ve teknik sınırlar koymaktır:

- Sorumluluk Reddi ve Yasal Beyan: Bilgi İşlem Merkezi onayından

geçmeyen, denetimsiz ve kişisel yapay zekâ araçlarıyla geliştirilen yazılımların sebep olabileceği veri kaybı, güvenlik ihlali ve aksaklıklarda tüm idari sorumluluğun uygulamayı geliştiren kişide olduğu net bir şekilde belgelenmelidir.

- 'Sıfır Destek' İlkesi: BT onaylı olmayan hiçbir uygulamaya teknik destek, veritabanı bağlantı izni veya sunucu barındırma kaynağı verilmemelidir. Yapay zekâ ile geliştirilen onaylanmamış bir sistemin sorunu yine aynı yöntemle çözülmelidir.
- Altyapı Düzeyinde İzolasyon: Kurumun ana veri tabanlarına ve hassas sistemlerine dışarıdan geliştirilen uygulamaların erişim yetkisi teknik olarak engellenmeli; bu uygulamaların kurumsal sunucularda çalıştırılmasına izin verilmemelidir.
- Teknik Dokümantasyon Şartı: Kullanılması zorunlu olduğu iddia edilen projelerde; uygulamanın mimari şeması, veri akış haritası ve güvenlik sızma testi raporu geliştirici kişiden talep edilmelidir. Bu kriterler denetimsiz girişimleri daha başlangıçta filtreleyecektir.

BT Yönetişim ve Sıfır Güven (Zero-Trust) Kontrol Hattı



Şekil 3: BT Yönetişim ve Sıfır Güven (Zero-Trust) Kontrol Şeması

5. Sonuç ve Değerlendirme

Yapay zekâ, alanında uzman bilişim profesyonellerinin elinde verimliliği artıran güçlü bir yardımcıdır. Ancak teknik birikim ve sistem mimarisi algısı olmayan ellerde, kurumsal veri bütünlüğünü tehdit eden karmaşa kaynaklarına dönüşme riski taşır.

Yılların tecrübesine ve mühendislik birikimine sahip bilişim yöneticilerinin ve uzmanlarının görevi; yapay zekanın yarattığı 'demo illüzyonuna' teslim olmak değil, kurumların dijital güvenliğini korumak, mimari standartları belirlemek ve veri bütünlüğünü savunmaktır. Yapay zekâ kod satırı üretebilir; ancak sistem sorumluluğunu, mimari vizyonu ve mühendislik disiplini üstlenemez.

Kaynakça

- [1] IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation.
- [2] Kharmia, M., Choi, S., & Mohaisen, D. A. (2024). Security and Quality Assessment of Code Generated by Large Language Models. IEEE Transactions on Software Engineering.
- [3] Gartner, Inc. (2024). Innovation Insight: Managing Shadow AI in the Enterprise Environment. Gartner Research.
- [4] NIST (National Institute of Standards and Technology). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce, NIST Publication 100-1.
- [5] OWASP Foundation. (2023). OWASP Top 10 for Large Language Model Applications (v1.1). Open Worldwide Application Security Project.

Yrd. Doç. Dr. Eren Küren
Bilgisayar Mühendisi & Dijital Dönüşüm Uzmanı

Artık Gerçekten Neyin Gerçek Olduğunu Biliyor muyuz?

“Yapay zekâ çağında görüntüye, sese ve bilgiye güvenmek”

Bir fotoğraf gördüğümüzde hâlâ ona inanıyor muyuz?

Bir fotoğraf gördüğümüzde genellikle onun gerçek olduğunu düşünürüz. Bir video izlediğimizde, “Gözlerimle gördüm.” deriz. Tanıdığımız bir kişinin sesini duyduğumuzda, o kişinin gerçekten konuştuğuna inanırız. Peki ya gördüğümüz fotoğraf hiç yaşanmamış bir olayın görüntüsüyse? Ya izlediğimiz video, gerçekte hiç söylenmemiş bir sözün kaydıysa? Ya telefonda duyduğumuz ses, gerçekten o kişiye ait değilse? İşte yapay zekâ çağının en önemli sorularından biri burada ortaya çıkıyor:

Gördüğümüz ve duyduğumuz her şey gerçekten yaşandı mı?

Artık mesele yalnızca teknoloji değil. Mesele **gerçeklik, güven ve doğru bilgiye ulaşabilmek**.



Şekil 1. “Gerçek mi, yapay mı?” — deepfake yüz görseli

İnternet bilgiye ulaşmayı kolaylaştırdı, yapay zekâ ise bilgiyi üretmeye başladı

İnternetin ilk dönemlerinde temel problem bilgiye ulaşmaktı. Bir konu hakkında bilgi arıyor, arama motorlarını kullanıyor ve karşılaştığımız kaynaklar arasından seçim yapıyorduk. Sosyal medya ile birlikte bilgi paylaşma biçimimiz değişti. Artık haberleri yalnızca gazetelerden veya televizyonlardan takip etmiyor; arkadaşlarımızın, sosyal medya hesaplarının, video platformlarının ve çeşitli dijital toplulukların paylaşımlarından da öğreniyoruz. Şimdi ise yeni bir dönemin içerisindeyiz:

Bilgi yalnızca bulunmuyor; yapay zekâ tarafından üretiliyor.

Bugün yapay zekâ;

- ✓ Metin yazabiliyor,
- ✓ Fotoğraf oluşturabiliyor,
- ✓ Video üretebiliyor,
- ✓ Ses taklit edebiliyor,
- ✓ Yüzleri değiştirebiliyor,
- ✓ Sanal karakterler oluşturabiliyor,
- ✓ Gerçek bir kişinin konuşmadığı cümleleri söylemiş gibi gösterebiliyor.

Bu nedenle problem artık yalnızca: **“Doğru bilgi nerede?”** değil.

Aynı zamanda: **“Karşımdaki bilginin gerçekten bir kaynağı var mı?”** sorusudur.

Deepfake: Gerçeğe benzeyen ama hiç yaşanmamış bir dünya

Son yıllarda sıkça duyduğumuz **deepfake** kavramı, yapay zekâ

kullanılarak görüntü, video veya sesin gerçekmiş gibi değiştirilmesi ya da oluşturulması anlamında kullanılıyor. Deepfake teknolojisinin tamamı kötü amaçlı değildir. Film ve televizyon, eğlence, eğitim ve yaratıcı içerik üretimi gibi alanlarda yararlı uygulamaları bulunabilir. Ancak teknoloji kötüye kullanıldığında ciddi sorunlar ortaya çıkabilir.

Örneğin:

- ✓ Bir kişi hiç söylemediği bir sözü söylemiş gibi gösterilebilir.
- ✓ Bir kişinin yüzü başka bir kişinin yüzüyle değiştirilebilir.
- ✓ Bir kişinin sesi taklit edilebilir.
- ✓ Gerçekte yaşanmamış bir olay yaşanmış gibi gösterilebilir.
- ✓ Eski bir görüntü yeni bir olaymış gibi sunulabilir.

2026 yılında yayımlanan güncel bilimsel çalışmalar da deepfake üretiminin giderek daha gerçekçi hale geldiğini ve mevcut tespit yöntemlerinin yeni üretim teknikleri karşısında genelleme ve güvenilirlik sorunları yaşayabildiğini gösteriyor. Burada önemli olan şudur:

Sorun yapay zekânın içerik üretebilmesi değil; üretilen içeriğin gerçekmiş gibi sunulabilmesidir.

Asıl tehlike sahte görüntü değil, gerçek görüntüye olan güvenin kaybolması

Deepfake konusunda genellikle sahte videolardan bahsediyoruz. Fakat daha büyük bir sorun ortaya çıkabilir. Bir olay gerçekten yaşanmış olabilir. Gerçek görüntüler de bulunabilir. Fakat insanlar artık her görüntünün yapay zekâ tarafından değiştirilebileceğini düşünmeye başlarsa ne olacak?

İşte burada **“güven problemi”** ortaya çıkıyor. Gelecekte yalnızca: “Bu görüntü sahte mi?” sorusunu sormayacağız. Belki de: **“Gerçek olan görüntünün gerçek olduğunu nasıl kanıtlayacağız?”** sorusunu da sormamız gerekecek. Bu konu özellikle önemli çünkü günümüzde deepfake tespit sistemlerinin kendileri bile farklı veri kümeleri, yeni üretim yöntemleri ve görüntü üzerinde yapılan sıkıştırma veya düzenlemeler karşısında sınırlamalar yaşayabiliyor.

“Gözlerime inanıyorum” dönemi sona mı eriyor?

İnsan zihni görsel bilgiye büyük önem verir. Bir olayı yazılı olarak okumakla görüntüsünü izlemek aynı etkiyi oluşturmaz. “Gördüm.” dediğimizde çoğu zaman bilgiyi daha güvenilir kabul ederiz. Fakat yapay zekâ bu durumu değiştiriyor. Çünkü artık bir görüntünün ortaya çıkması için o olayın gerçekten yaşanmış olması gerekmiyor. Bir metin komutuyla yeni bir sahne oluşturulabiliyor. Bir yüz değiştirilebiliyor. Bir ses üretiliyor. Bir video yeniden kurgulanabiliyor.

Dolayısıyla gelecekte bir görüntüyle karşılaştığımızda şu sorular daha önemli hale gelecek:

- ✓ **Bu görüntüyü kim oluşturdu?**
- ✓ **İlk nerede yayımlandı?**
- ✓ **Ne zaman oluşturuldu?**
- ✓ **Başka kaynaklar olayı doğruluyor mu?**
- ✓ **Görüntünün orijinal hali mevcut mu?**
- ✓ **İçerik üzerinde değişiklik yapılmış mı?**
- ✓ **İçeriğin dijital geçmişi doğrulanabiliyor mu?**

Yani geleceğin dijital vatandaşının yalnızca **görme becerisine değil,**

doğrulama becerisine ihtiyacı olacak.



Şekil 2. Yapay zekâ + sosyal medya + akıllı telefon.

Sosyal medya: Hız bazen doğruluğun önüne geçiyor

Bir bilginin internette yayılması için artık büyük bir medya kuruluşuna ihtiyaç yok. Bir akıllı telefon yeterli. Bir kişi bir video paylaşabiliyor. Başka biri onu yeniden paylaşabiliyor. Bir başkası farklı bir başlık ekleyebiliyor. Sonrasında içerik binlerce, hatta milyonlarca kişiye ulaşabiliyor. Üstelik içerik ilk kaynağından tamamen kopabiliyor.

Bu nedenle dijital dünyada şu zincir oldukça tehlikeli hale gelebiliyor:

İçerik → paylaşım → yeniden paylaşım → yorum → yeni başlık → bağlam kaybı → yanlış anlaşılma

Reuters Institute'un 2025 Digital News Report araştırmasında, araştırmaya dahil edilen ülkelerdeki çevrim içi haber kullanıcılarının %58'i internette haber söz konusu olduğunda neyin doğru, neyin yanlış olduğunu ayırt etme konusunda endişeli olduğunu bildirdi. Araştırma aynı zamanda sosyal medya ve video platformlarının haber tüketimindeki rolünün arttığını ortaya koyuyor. Bu bize önemli bir şey söylüyor:

Problem yalnızca sahte içerik üretmek değil; insanların doğru bilgiye olan güvenidir.

Peki gerçeği nasıl anlayacağız?

İnsanlara yalnızca: "Her gördüğünüze inanmayın." demek yeterli değil. Asıl mesele insanlara **doğrulama alışkanlığı** kazandırmak. Şüpheli bir içerikle karşılaştığımızda basit bir kontrol listesi kullanabiliriz.

1. Kaynağı kontrol edin

İçeriği kim paylaşmış?

- ✓ Gerçek bir kurum mu?
- ✓ Tanınabilir bir kişi mi?
- ✓ Kaynağı belirsiz bir hesap mı?

2. İlk kaynağı bulun

Bir sosyal medya paylaşımı gördüğünüzde mümkünse içeriğin ilk yayımlandığı kaynağı araştırın.

3. Başka kaynaklarla karşılaştırın

Önemli bir olay yalnızca tek bir hesaptan mı aktarılıyor? Başka güvenilir kaynaklarda da aynı bilgi bulunuyor mu?

4. Tarihe bakın

Eski bir fotoğraf veya video yeni bir olaymış gibi paylaşılmış olabilir.

5. Bağlamı kontrol edin

Gerçek bir fotoğraf bile yanlış açıklamayla paylaşılabiliyor. Bu nedenle:

Gerçek görüntü + yanlış açıklama = yanlış bilgi olabilir.

6. Duygusal tepkinizi kontrol edin

Bir içerik sizi aşırı derecede:

- ✓ Öfkeliendiriyorsa,
- ✓ Korkutuyorsa,
- ✓ Şaşırtıyorsa,
- ✓ Heyecanlandırıyorsa,

hemen paylaşmadan önce bir kez daha kontrol etmek faydalıdır.

SAHTE HABERLERİ NASIL TESPİT EDERSİNİZ?



Şekil 3. Fact-checking / medya okuryazarlığı infografiği.

Teknoloji aynı zamanda çözümün bir parçası olabilir

İlginç olan şu: **Bizi gerçek ile sahte arasındaki ayrım konusunda zorlayan teknoloji, aynı zamanda çözüm için de kullanılabilir.** Bunun önemli örneklerinden biri **içerik kökeni (content provenance)** yaklaşımıdır. Buradaki temel fikir oldukça basit: Bir içeriğin yalnızca kendisine değil, **geçmişine de bakmak.**

Örneğin:

- ✓ Nerede oluşturuldu?
- ✓ Kim tarafından üretildi?
- ✓ Hangi araç kullanıldı?
- ✓ Üzerinde değişiklik yapıldı mı?
- ✓ Hangi aşamalardan geçti?

Bu alandaki önemli girişimlerden biri **C2PA-Coalition for Content Provenance and Authenticity** standardıdır. C2PA'nın Content Credentials yaklaşımı, dijital içeriğin oluşturulması ve değiştirilmesiyle ilgili doğrulanabilir köken bilgilerinin tutulmasını amaçlıyor. Burada önemli bir ayrıntı var: **İçeriğin köken bilgisinin bulunması, içeriğin otomatik olarak doğru olduğu anlamına gelmez.** Ancak bize içeriğin geçmişini incelemek için önemli bir araç sağlayabilir.



Şekil 4. C2PA / Content Credentials / dijital içerik kökeni.

Yapay zekâ çağında eğitim neden değişmek zorunda?

Belki de bu konunun en önemli tarafı eğitim. Çünkü geleceğin öğrencisinin sadece bilgiye ulaşması yeterli olmayacak.

Öğrencinin aynı zamanda:

- ✓ Bilgiyi sorgulaması,
- ✓ Kaynağı araştırması,
- ✓ Farklı kaynakları karşılaştırması,
- ✓ Yapay zekâ çıktısını kontrol etmesi,
- ✓ Kanıt araması,
- ✓ Manipülasyonu fark etmeye çalışması gerekecek.

Başka bir ifadeyle: Eskiden “Bilgiye nasıl ulaşırım?” önemliydi.

Şimdi “Ulaştığım bilginin doğru olduğunu nasıl anlarım?” daha da önemli hale geliyor.

Bu nedenle eğitim sistemlerinde **medya okuryazarlığı, bilgi okuryazarlığı ve yapay zekâ okuryazarlığının** birlikte düşünülmesi gerekiyor. UNESCO da dijital platformların yönetimi ve bilgi ekosisteminin korunması konusunda eğitim, medya, teknoloji şirketleri, akademi, kamu ve sivil toplumun birlikte hareket etmesi gerektiğini vurguluyor.

- ✓ **Geleceğin en önemli becerilerinden biri: Doğrulama**

Belki de gelecekte iş başvurularında yalnızca: “**Hangi programları kullanabiliyorsunuz?**” sorusu sorulmayacak. Bunun yanında: “**Bir bilginin doğruluğunu nasıl kontrol ediyorsunuz?**” sorusu da önem kazanacak. Çünkü yapay zekâ bize çok hızlı cevaplar verebilir. Ancak hız ile doğruluk aynı şey değildir. Bir yapay zekâ sistemi birkaç saniyede cevap verebilir. Ama insanın hâlâ şu soruyu sorması gerekir: “**Bu cevap hangi kanıta dayanıyor?**” Bu nedenle geleceğin insanı yapay zekâdan daha fazla bilgi almakla yetinmeyecek. **Aldığı bilgiyi değerlendirmeyi de öğrenecek.**

Gerçek ile sahte arasındaki savaşın ötesinde bir mücadele var

Belki de geleceğin en büyük problemi sahte içeriklerin sayısı olmayacak. Daha büyük problem: **İnsanların hiçbir şeye güvenmemeye başlaması olabilir.**

- ✓ Gerçek bir görüntü: “Bu da yapay zekâ olabilir.”
- ✓ Gerçek bir belge: “Bu da değiştirilmiş olabilir.”
- ✓ Gerçek bir ses kaydı: “Bu da yapay olarak üretilmiş olabilir.” şeklinde sorgulanabilir.

Bu durum yalnızca medya için değil;

- ✓ Eğitim,
- ✓ Hukuk,
- ✓ Finans,
- ✓ Kamu yönetimi,
- ✓ Gazetecilik,
- ✓ Bilim,
- ✓ Ticaret gibi alanlar için de önem taşıyor.

2026 tarihli güncel araştırmalar, deepfake ve sentetik medya teknolojilerinin yalnızca bireysel yanıltma değil, **dijital kanıtların güvenilirliği ve toplumsal güven** açısından da sorunlar oluşturabileceğini vurguluyor.

O halde ne yapmalıyız?

Çözüm yalnızca yeni bir yapay zekâ dedektörü geliştirmek değil.

Daha geniş bir yaklaşım gerekiyor:

Bunların tamamı birlikte çalışmak zorunda. Çünkü teknoloji gelişirken onu kullanan insanların bilinç düzeyi aynı hızla gelişmezse yeni problemler ortaya çıkabilir.

Belki de artık “Gördüm” değil, “Doğruladım” demeliyiz

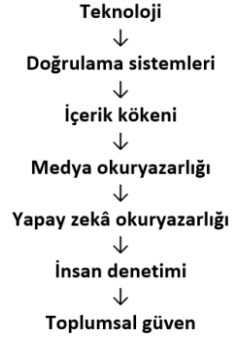
İnsanlık daha önce birçok bilgi devrimi yaşadı. Matbaa bilgiye erişimi değiştirdi. Radyo iletişimin hızını değiştirdi. Televizyon

görüntülü iletişimi değiştirdi. İnternet bilgiye erişimin ölçeğini değiştirdi. Sosyal medya bilgi paylaşımını değiştirdi. Şimdi yapay zekâ başka bir şeyi değiştiriyor: **Bilginin nasıl üretildiğini.** Bu nedenle önümüzdeki yıllarda en önemli soru: “**Yapay zekâ neler yapabiliyor?**” olmayabilir. Belki daha önemli soru: “**Yapay zekâ çağında gerçeği nasıl koruyacağız?**” olacak. Çünkü artık:

- ✓ **Bir görüntünün gerçek görünmesi, onun gerçek olduğunu kanıtlamayabilir.**
- ✓ **Bir sesin tanıdık gelmesi, gerçekten o kişiye ait olduğunu göstermeyebilir.**
- ✓ **Bir metnin ikna edici olması, doğru olduğu anlamına gelmeyebilir.**

Bu nedenle geleceğin dijital dünyasında belki de en önemli alışkanlığımız şu olacak:

“**Gördüm**” demeden önce “**Doğruladım**” demek. Çünkü yapay zekâ çağında en değerli şey yalnızca bilgiye ulaşmak değil, **gerçeği tanıyabilmek** olacak.



Şekil 5. Gerçek–sahte ayrımını sembolize eden sade bir dijital görsel.

**Okuyucu için 10 Saniyelik Dijital Kontrol Listesi**

Bir içerik gördüğünüzde paylaşmadan önce şu 6 soruyu sorun:

- ✓ **Kim paylaştı?**
- ✓ **İlk kaynak neresi?**
- ✓ **Tarih doğru mu?**
- ✓ **Başka güvenilir kaynaklar doğruluyor mu?**
- ✓ **İçerik bağlamından koparılmış olabilir mi?**
- ✓ **Beni hemen inanmaya veya paylaşmaya iten güçlü bir duygu mu oluşturuyor?**

Cevaplardan emin değilseniz: PAYLAŞMAYIN. ÖNCE DOĞRULAYIN.

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

Kaynaklar

1. World Economic Forum. (2026). *The Global Risks Report 2026*. –[World Economic Forum: Global Risks Report 2026](#)
2. Reuters Institute for the Study of Journalism. (2025). *Digital News Report 2025*. –[Reuters Institute: Digital News Report 2025](#)
3. National Institute of Standards and Technology (NIST). *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency*. –[NIST: Synthetic Content Transparency](#)
4. European Commission. (2026). *Transparency Rules for AI Systems*. –[European Commission: AI Transparency Rules](#)
5. Coalition for Content Provenance and Authenticity (C2PA). (2026). *C2PA Technical Specification*. –[C2PA: Technical Specification](#)
6. UNESCO. *Guidelines for the Governance of Digital Platforms*. –[UNESCO: Guidelines for the Governance of Digital Platforms](#)
7. Alrahhal, M., et al. (2026). *Deepfake face detection using hybrid bag-of-visual-words and multi-CNN feature fusion*. *Scientific Reports*, 16, 22623.
8. Sharma, S., & Selwal, A. (2026). *Potential of artificial intelligence in deepfake media: From generation to detection mechanisms, state-of-the-art, and challenges*. *Computer Science Review*, 100866.
9. Deep-fake detection of digital misinformation over social media: a comprehensive review. (2026). *Array*, 31, 101086.
10. Kişisel Verileri Koruma Kurumu (KVKK). *Deepfake Bilgi Notu*. Ankara: KVKK.
11. Cumhurbaşkanlığı İletişim Başkanlığı. (2026). *Yeni Medyada Kriz İletişimi Rehberi*. Ankara.
12. Cumhurbaşkanlığı İletişim Başkanlığı. (2026, 18 Mart). *Yapay zekâ destekli dolandırıcılık girişimlerine ilişkin bilgilendirme*.
13. Cumhurbaşkanlığı İletişim Başkanlığı. (2026, 25 Mart). *Ülkemizin huzurunu ve millî güvenliğimizi hedef alan faaliyetlere ilişkin açıklama*.
14. Cumhurbaşkanlığı İletişim Başkanlığı. (2026, 21 Mayıs). *Dijital Medyada Dezenformasyon ve Yeni Nesil İçerik Ekosistemi oturumu gerçekleştirildi*.
15. Cumhurbaşkanlığı İletişim Başkanlığı – Dezenformasyonla Mücadele Merkezi. *Dezenformasyon Bülteni*.

Küçük bir E-Devlet by BT Kıbrıs

Bir yabancı işçinin Kuzey Kıbrıs'ta çalışabilmesi için kaç kurumun "olur" demesi gerekir, hiç saydınız mı? Nüfus kaydı, polis, sağlık, sosyal sigorta, ihtiyat sandığı, vergi dairesi, muhaceret, üçüncü ülke vatandaşıysa banka, öğrenciyse üniversite, işveren müteahhitse birlik, esnafsa oda... Kâğıt döneminde bu listenin her satırı bir kapı, her kapı bir sıra, her sıra en az bir yarım gün demektir. İşveren ya da muhasebecisi elinde bir dosyayla ada turu atardı: sigortadan "borcu yoktur" yazısı, ihtiyattan "borcu yoktur" yazısı, vergiden "borcu yoktur" yazısı, hepsini toplayıp Çalışma Dairesi'ne getirirdi. Getirdiği belgelerin her biri, bir devlet dairesinin başka bir devlet dairesine vatandaş eliyle gönderdiği bir mektuptu aslında. Postacı vatandaştı.

Bu yazıda o postacıyı işinden eden bir sistemi anlatacağım. Ama asıl derdim sistemin kendisi değil. Derdim şu: "e-devlet" dediğimiz şey büyük şehirlerde, büyük bütçelerle, büyük kapılarla mı kurulur, yoksa küçük bir dairenin küçük bir derdinden mi doğar? Bizim tecrübemiz ikincisini söylüyor. Ona "küçük e-devlet" diyorum.

Kitaplar e-devleti bir merdiven gibi anlatır: önce bilgi internete konur, sonra işlem çevrimiçi yapılır, en sonda da farklı işler yapan kurumlar aynı vatandaş için birbirinin verisine bakar. Zor basamak hep sonuncusudur, çünkü o artık yazılım değil kurumsal irade meselesidir. Bunu başarmış küçük ülke örneği olarak hep Estonya gösterilir; 1,3 milyonluk ülke kurumlarını tek bir veri katmanına bağladı ve vatandaşın bir bilgiyi yalnızca bir kez ister. Kuzey Kıbrıs, Estonya'nın üçte biri. Aynı şey bizde de olabilir mi? Olabiliyor, ama tepeden değil, tabandan.

Bir dairenin derdi

2022 sonbaharında Çalışma ve Sosyal Güvenlik Bakanlığı için bir çalışma izinleri portalı yazmaya başladık. İlk satırlar Kasım ayında yazıldı, portal 27 Aralık 2022'de açıldı. Önce hizmet akdi, işçi kartı, vekalet ve çevrimiçi ödeme; sonra sırayla işyeri tescili, ön izin, çalışma izni, uzatma, öğrenci izni, iş kurma izni ve diğerleri.

O sırada aklımızda "e-devlet kurmak" diye bir şey yoktu. Aklımızda dairenin önündeki kuyruk vardı. Kuyruğu kısaltmanın tek yolu,

vatandaşın elinde taşıdığı belgelerin yerine kurumlara doğrudan sormaktı. "Bu işverenin sigorta borcu var mı?" sorusunu dosyadaki kâğıttan değil, Sosyal Sigortalar Dairesi'nin sisteminden öğrenmeliydik. Böylece ilk servis bağlantısını yazdık. Sonra ikincisini. Bugün portal on dokuz ayrı kamu kurumu, oda ve birliğin sistemiyle konuşuyor. Bunlar, alfabetik değil ama iş akışındaki sırayla, aşağı yukarı şöyle:

- **Nüfus ve Kayıt Dairesi.** Kimlik numarasından kişi kaydı doğrulanıyor; yabancıya kimlik numarası bu portal üzerinden yaratılıyor.
- **Muhaceret Dairesi.** Dosya numarası, giriş kayıtları, ikamet bilgisi sorgulanıyor; verilen çalışma izni ve ön izin Muhaceret'e otomatik bildiriliyor. En yoğun bağlantı bu; iki yönde on yedi ayrı servis.
- **Polis Genel Müdürlüğü.** Üçüncü ülke vatandaşları için sabıka ve giriş-çıkış kontrolü. Sınır kapısındaki polis, işçinin adaya girdiğini portaldan işaretliyor ve işe başlama tarihi oradan doğuyor.
- **Sağlık Bakanlığı.** Sağlık dosyası portaldan açılıyor, laboratuvar sonucu Sağlık Bakanlığı'nın sisteminden portala geri yazılıyor. İşçi elinde rapor taşıyor.
- **Sosyal Sigortalar Dairesi ve İhtiyat Sandığı.** "Borcu yoktur" sorgusu, işe giriş ve işten ayrılma bildirimleri iki yönlü akıyor.
- **Gelir ve Vergi Dairesi.** Mükellef kaydı, harç tahakkuku, ödeme sorgusu. İşveren daha önce vergi dairesine gidip mükellef numarası alırdı; şimdi portal alıyor.
- **Bankalar.** Üçüncü ülke vatandaşı için teminat mektubu. Bankalar portala kendi kullanıcılarıyla giriyor, bekleyen başvuruları görüyor, teminatı sisteme işliyor.
- **Milli Eğitim Bakanlığı.** Öğrenci izinlerinde öğrencilik durumu üniversite kayıtlarından doğrulanıyor.
- **Şirketler Mukayyitliği, Esnaf ve Zanaatkarlar Odası, Sanayi Odası, Müteahhitler Birliği.** İşverenin tüzel kişiliği ve üyeliği kendi kaynağından

soruluyor.

- **İşbul (İstihdam Dairesi).** Yabancı işçi alınmadan önce yerli işgücüne ilan verildi mi, kontrolü buradan yapılıyor.
- **Devlet Emlak ve Malzeme Dairesi (DEMD).** Kumarhanelerde çalışacak yabancılar için Şans Oyunları personel lisans belgesi. DEMD'nin kendi personeli portala giriyor, lisans başvurularını kendi ekranından onaylıyor ya da reddediyor, harcı hesaplıyor ve belgeye mührünü basıyor. Aşağıda ayrıca anlatacağım.
- **Merkez Bankası, adres kayıt sistemi, mahkemelerin evlenme kaydı, Sosyal Hizmetler Dairesi, İçişleri ve Dışişleri bakanlıkları.** Kur, adres, medeni hal, sosyal yardım ve yazışma tarafı.

KoopBank. Bakanlığın kendi gelirlerinin tahsilatı. Çalışma izni harcı devlet hazinesinin parasıdır ve vergi dairesi entegrasyonu tahakkuk eder; ama hizmet akdi, işçi kartı, vekalet, işyeri tescili gibi çalışma izni sayılmayan bütün işlemlerin harcı, bakanlık bünyesindeki İşgücü Planlama ve Geliştirme Merkezi'nin (İPGM) hesabına yatar. Bu tahsilat Koop Bank sanal pos entegrasyonu yapıyor: portal ödeme adımına gelen başvuruyu bankanın ödeme sayfasına yönlendiriyor, işveren kartıyla ödüyor, banka sonucu portala geri bildiriyor, para doğrudan bakanlığın hesabına geçiyor ve dosya kendiliğinden bir sonraki adıma ilerliyor. Vezne yok, makbuz kuyruğu yok, bakanlığa elden para yok.

Bunların hiçbirisi için bir "ulusal veri değişim katmanı" beklemedik. Her birinin kendi servisi, kendi protokolü, kendi kullanıcı adı var. Kimi SOAP konuşuyor, kimi REST, kimi düz XML. Bir kısmı devletin yeni kurduğu ortak API kapısının arkasında, bir kısmı hâlâ doğrudan IP adresiyle. Estonya'nın X-Road'una benzemiyor; daha çok, herkesin herkesle ayrı ayrı anlaştığı bir mahalleye

benziyor. Ama çalışıyor.

Yatay bütünleşme masada değil, sahada olur

Kurumların birbirinin verisine bakması, o en zor basamak, bizde bir toplantı kararıyla değil, bir başvuru akışının zorlamasıyla oldu. Ön izin başvurusunun yirmi bir adımı var. Beşinci adımda dosya memura düşer, yedincide amir kota kontrolü yapar ve kota için Sosyal Sigortalar'daki çalışan sayısına bakar. Dokuzuncu adımda banka teminatı devreye girer. Onuncu adımda dosya polise havale olur; on üçüncü adımda sınır kapısındaki polis "adaya girdi" der. On dördüncüde sağlık ödemesi, on beşinci ve on altıncıda laboratuvar. On yedincide harç ödenir, yirmincide izin basılır.

Bu akışta portal, kurumlar arasındaki sırayı da tutan bir masa gibi çalışıyor. Bankanın kullanıcısı sisteme girdiğinde yalnızca "bankanın işlem yapması gereken başvurular" listesini görür. Polisin kullanıcısı yalnızca polisi bekleyenleri. Sağlık Bakanlığı'nın laboratuvarı sonucu yazar, dosya kendiliğinden bir sonraki adıma geçer. Süreç tanımında her adımın "hangi tarafın" olduğu yazılı: vatandaş, kurum, banka ya da sistem. Sistem tarafı dediğimiz şey, kimsenin düğmeye basmadığı, servisin kendi kendine sorup kendi kendine ilerlettiği adımlar.

En yeni bağlantımız bu akışın küçük bir örneği. Kumarhaneler bu ülkede ciddi bir istihdam alanı ve orada çalışacak yabancı için çalışma izni yetmiyor; kumarhaneleri denetleyen Devlet Emlak ve Malzeme Dairesi'nden ayrıca bir Şans Oyunları lisans belgesi almak gerekiyor. Eskiden bu ikinci bir dosya, ikinci bir daire, ikinci bir kuyruk demekti. 2025'te DEMD'yi portalin içine aldık. Şimdi işyeri kumarhaneysen, çalışma izninin hizmet akdi kesildiği anda portal kendiliğinden bir lisans başvurusu açıyor. Dosya DEMD'nin ekranına düşüyor; DEMD personeli mesleğe göre Euro cinsinden tanımlı harcı görüyor, harç Merkez Bankası'nın o günkü kuruyla TL'ye çevriliyor, gerekirse DEMD kendi hesapladığı özel tutarı giriyor. İşveren sanal postan ödüyor, DEMD lisansa mührünü basıyor, QR kodlu belge portaldan çıkıyor. Çalışma izni tarafı ise DEMD onaylayıp ödeme yapılmadan ilerlemiyor; izin iptal olursa lisans da kendiliğinden iptal oluyor, izin yeniden açılırsa lisans da açılıyor. İki daire, tek dosya. DEMD'nin portalda yedi kullanıcısı var; o yedi kişi bir buçuk yılda 22 bin lisans başvurusunu işledi ve 71 milyon TL harç bu yoldan tahsil edildi.

Buradan çıkardığımız ders şu: yatay bütünleşme bir mimari kararı değil, bir iş akışı sonucudur. Kurumlar, ortak bir vatandaş işini bitirmek zorunda oldukları için birbirine bağlanır. Vergi dairesiyle polis, "veri paylaşalım" diye masaya oturmaz; ama aynı işçinin izni ikisinin de onayını beklediği için, ikisi de aynı dosyaya bakmayı kabul eder.

Kim kullanıyor

"Vatandaş portalı" tanımı bu sistem için dar kalıyor. Sistemde on dört ayrı kullanıcı tipi var: memur, amir, müfettiş, bürokrat, Sayıştay, polis, muhaceret, banka, birlik, işyeri sahibi, çalışan, vatandaş ve diğerleri. Kayıt ekranında ise altı kapı: işveren, işveren temsilcisi ya da muhasebeci, işçi, kamu kurumu personeli, banka personeli ve af başvurusu yapan.

Portalın açıldığı Aralık 2022'den bugüne 37 bin kullanıcı hesabı açıldı, bunların 25 bini bugün aktif. En büyük iki grup işverenler ve işçiler: 18 bin işveren ya da işveren temsilcisi hesabı, 15,5 bin işçi hesabı. Son doksan günde 3.500 farklı kişi sisteme girdi; son bir ayda 2.500. Bir yıl içinde giriş yapan farklı kullanıcı sayısı 6.500 civarında. Bu, yarım milyonluk bir ülkede küçümsenecek bir sayı değil; ülkenin ortak e-Devlet Kapısı'nın bu yılın Mart ayında ulaştığı toplam kullanıcı sayısından fazla.

Asıl ilginç olan, kamu tarafındaki dağılım. Bakanlığın kendi personeli, memur ve amir dahil, 430 kişi. Buna karşılık bankalarda 858 hesap var; adadaki yirmi üç banka portala kendi kullanıcılarıyla giriyor ve teminat mektuplarını oradan işliyor. Polis Genel Müdürlüğü'nde 196 kullanıcı var; sınır kapılarındaki polislerden merkezdeki kontrol memurlarına kadar. İçişleri Bakanlığı'nda 38, Devlet Emlak ve Malzeme Dairesi'nde 7. Sayıştay'da denetim için 4. Yani portala giren her üç kamu görevlisinden ikisi Çalışma Dairesi'nde çalışmıyor.

Bir de hiç girmeyenler var. Sosyal Sigortalar Dairesi, İhtiyat Sandığı, Sağlık Bakanlığı ve Milli Eğitim için portalda kullanıcı ekranı açmadık; bu kurumlarla insan değil, servis konuşuyor. Servis kayıtlarına göre 2023'ten bu yana bu kurumların sistemlerine 21 milyon sorgu gitti. 2025'te tek başına 6,4 milyon; günde on yedi binin üstünde. Sosyal Sigortalar'a 2,7 milyon, İhtiyat Sandığı'na 2,5 milyon, nüfus kayıtlarına 1,9 milyon, Muhaceret'e 800 bin, vergi dairesine 500 bin kez soruldu. Sağlık Bakanlığı'na gidenler en kalabalık, çünkü portal laboratuvar

sonucu hazır mı diye kendi kendine sorup duruyor. Bir memurun bu kadar telefon açması mümkün değil; bu bir insanın değil, bir makinenin ada turu.

Başvuru tarafında sayılar şöyle: 2023'te 223 bin, 2024'te 388 bin, 2025'te 369 bin, bu yılın ilk dokuz ayında 301 bin başvuru. Toplamda 1,28 milyon. Bunların 400 bini hizmet akdi, 250 bini izin uzatma, 176 bini ön izin, 128 bini işten ayrılma bildirimi. Polis onayından 286 bin, sağlık onayından 900 bin, banka teminatından 391 bin başvuru geçti. 2,1 milyon SMS gönderildi. Bunların hepsi, bir daireye gitmeden yapılan işler.

Para tarafı ayrı bir bahis. Portal açıldığından beri Koop Bank sanal posu üzerinden 720 bin kart ödemesi geçti, toplamı 1,6 milyar TL'yi aşıyor. Bunun 1,1 milyarı devlet hazinesine giden çalışma izni harcı; 520 milyonu ise hizmet akdi, işçi kartı, vekalet ve tescil gibi işlemlerden bakanlığın İPGM hesabına yatan pay. Yani bakanlık, kendi gelirinin tamamını bir bankanın sanal posu üzerinden, hiçbir memurun eline para değmeden topluyor. 2023'te bir yılda 86 milyon TL tahsil edildi; 2025'te 632 milyon, bu yılın ilk dokuz ayında 643 milyon. Enflasyonu bir kenara bıraksak bile, bir bakanlığın bütün tahsilatının vezneye uğramadan kart ile banka arasında dönmesi birkaç yıl önce bu ülkede olağan bir şey değildi. Kartla ödemek istemeyen ya da ödeyemeyen için de bir yol var: kurumlar ve büyük işverenler portala önceden kontür yüklüyor, harç kontürden düşüyor. Bugüne kadar 41 bin harç bu yolla ödendi.

Bu sayıların yanına ülkenin ölçeğini koymak lazım. KKTC İstatistik Kurumu'nun Aralık 2025 verisine göre sosyal sigortaya kayıtlı 170 bin çalışanın 90 bini, yani yarısından fazlası, Türkiye ve üçüncü ülke vatandaşı. Bu 90 bin kişinin her birinin bir çalışma izni, o iznin de her yıl bir uzatması var. Bir yılda 370 bin başvuru, bu ülkede iş gücünün yarısının her yıl bu portaldan geçtiği anlamına geliyor.

Küçük olmanın hâlleri

Küçüklüğün bize verdiği avantajları saymak kolay. Kurumların hepsini tanıyoruz; servis bağlantısı için gereken kişi çoğu zaman bir telefon uzağında. Bir sorun çıktığında Sağlık Bakanlığı'ndaki yazılımcıyla aynı gün konuşabiliyoruz. Estonya'daki "az veto noktası" avantajı bizde de var, hatta daha fazla.

Ama küçüklüğün bedelleri de var ve dürüst

olmak gerekirse literatür bunları pek yazmıyor.

Birincisi kırılma. On dokuz bağlantının her biri bir tek kurumun bir tek sunucusuna gidiyor. O sunucu bakıma girdiğinde başvurular o adımda bekler. Bunun için her serviste "servis ulaşamadı" durumunu ayrı ele almak, bazı adımlar için memurun elle geçebileceği muafiyet kapıları bırakmak zorunda kaldık. Sistemde yirmi yedi ayrı muafiyet türü var; bir kısmı hukuki istisna, bir kısmı düpedüz "servis çalışmadı, dosya beklemesin" için.

İkincisi standart eksikliği. Ulusal bir veri değişim katmanı olmadığı için her kurumla ayrı anlaşıyoruz. Bu, bugün için işi hızlandırdı; çünkü kimseyi beklemedik. Ama on yıl sonra bu bağlantıları kim bakacak, hangi standarda taşıyacak, bilmiyoruz. Teknik tarafı çözdük, kurumlar arası tarafı kişisel ilişkilerle idare ettik, ortak dil tarafını ise her seferinde yeniden konuşuyoruz. "Tescil numarası" bizim için başka, Sanayi Odası için başka bir alan.

Üçüncüsü, kimlik meselesi. Bir e-devletin kalbi kimlik doğrulamadır. Biz kimliği nüfus servisinden doğruluyoruz, SMS ile ikinci faktör ekliyoruz. Ama bütün bunlar bizim portalımızın kapısında duruyor. Vatandaş yarın ihtiyat sandığının portalına gittiğinde yeniden kayıt oluyor. Ülkenin ortak e-Devlet Kapısı geçen yıl mobil uygulamasını çıkardı, ilk iki ayda iki bin, bu yılın Mart ayında on bin kullanıcıya ulaştı; şifre almak için hâlâ kaymakamlığa gidiliyor.

Küçük e-devlet nedir

Bütün bunlardan sonra "küçük e-devlet" ile ne demek istediğimi toparlayayım.

Büyük e-devlet, tepeden kurulan bir kapıdır. Bir kurum, bir standart, bir kimlik, bir giriş. Türkiye'nin 2008'de açtığı e-Devlet Kapısı bugün 68 milyon kullanıcı ve dokuz binden fazla hizmetle bunun iyi bir örneği. Estonya'nın X-Road'u bir başkası. Bunlar ancak bir devletin bütün kurumlarını aynı anda bir masaya oturabilmesiyle mümkün olur.

Küçük e-devlet ise bir dairenin kendi işini bitirmek için komşularına uzattığı eldir. Ortak bir standart beklemez, çünkü bekleyecek zamanı yoktur. Her kurumla kendi dilinde konuşur. Vatandaş postacıktan kurtarmayı ilk gün hedefler, "bütün-devlet zemini" kurmayı hedeflemez; ama iş bittiğinde ortaya çıkan şey, o zeminin küçük bir parçasıdır. Bir çalışma izni için on dokuz kurum birbirine bağlandıysa, o bağlantılar yarın başka bir iş için de oradadır.

Kitaplardaki merdiveni yukarıdan aşağı değil, aşağıdan yukarı çıkmak gibi bir şey. Önce yatay bütünleşme, sonra işlem, en son katalog. Kâğıt üstünde yanlış sıra; sahada ise tek mümkün sıra.

Kuzey Kıbrıs gibi yerlerde e-devlet böyle kurulacak. Büyük kapı bir gün açılacak ve açıldığında arkasında zaten birbirine bağlanmış, birbirinin dilini öğrenmiş bir avuç daire bulacak. O dairelerden biri de çalışma izinlerini veren daire olacak; kapiya bağlanmak için yapması gereken tek şey, on dokuz bağlantısından birini daha kurmak.

Postacı ise artık başka bir işte çalışıyor. Umarım çalışma izni sorunsuz çıkmıştır.

Kaynaklar

- Layne, K. ve Lee, J. (2001). "Developing fully functional E-government: A four stage model". *Government Information Quarterly*, 18(2).
- e-Estonia, X-Road tanıtım sayfaları.
- KKTC Çalışma ve Sosyal Güvenlik Bakanlığı (4 Ocak 2023). "Online Hizmet Portalı Devrede" basın duyurusu; online.csgb.gov.ct.tr.
- KKTC e-Devlet Kapısı, edevlet.gov.ct.tr; Kıbrıs Postası (Ekim 2025 ve 18 Mart 2026) e-Devlet kullanıcı sayısı haberleri.
- KKTC İstatistik Kurumu, Aralık 2025 işgücü verisi (Diyalog, 6 Haziran 2026 aktarımıyla).
- Türkiye e-Devlet Kapısı istatistikleri (Anadolu Ajansı, Aralık 2025).

MEYVE SİNEĞİNİN DİJİTAL BEYİN HARİTASI

Beyin haritalarından sanal bedenlere ve yeni hesaplama yöntemlerine

Bir meyve sineğinin beyin haritası internete açılıyor. Ardından ekranlarda oyun oynadığı, araba kullandığı, hatta döner kestiği söylenen bir “dijital sinek” beliriyor. Ekim 2026'da sosyal medyada yayılan bu görüntüler, bilimsel bir çalışmayı beklenmedik biçimde gündelik sohbetin konusu hâline getirdi. Peki gerçekten bir hayvanın beyni bilgisayara mı yüklendi? Sinek artık bir yazılımın içinde mi yaşıyor, yoksa gördüğümüz şey başka türlü mü açıklanmalı?

Bu haberlerin temelinde gerçek ve önemli bir başarı var: Araştırmacılar, meyve sineğinin sinir hücrelerini ve aralarındaki bağlantıları olağanüstü ayrıntıyla haritaladı. [1][2] Bu verilerle davranışa ilişkin tahminler üreten modeller kuruluyor [4][7], sanal bedenler kontrol ediliyor [13] ve yeni hesaplama donanımları deniyor. [14] Ancak bir beynin bağlantılarını çıkarmak, o canlının bütün zihinsel yaşamını kopyalamak anlamına gelmiyor. Gelişmeleri anlayabilmek için harita, model ve gösteri arasındaki farkı görmek gerekiyor.

Önce hangi sinekten söz ettiğimizi bilelim

Bu hikâyenin kahramanı, bilimsel adı *Drosophila melanogaster* olan meyve ya da sirke sineği. Kıbrıs'ta da yaygın olarak bulunan Akdeniz meyve sineği *Ceratitis capitata* ile aynı tür değil. [18] Gündemdeki beyin haritaları, genetik araştırmalarında uzun süredir model organizma olarak kullanılan *Drosophila melanogaster* türüne ait. [1][9]

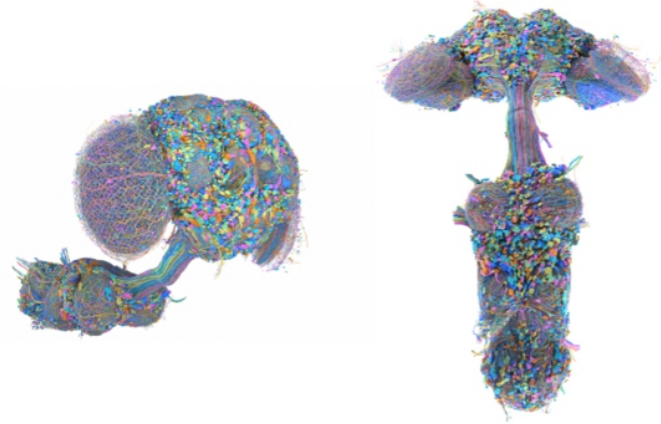
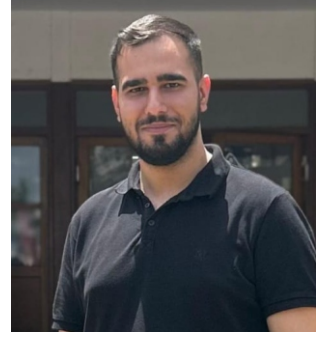


Görsel 1. *Drosophila melanogaster*, beyin bağlantılarının haritalanmasında kullanılan meyve sineği türü. Fotoğraftaki birey, haritası çıkarılan araştırma örneği değildir. Fotoğraf: Mr.checker / Wikimedia Commons. CC BY-SA 3.0. https://commons.wikimedia.org/wiki/File:Drosophila_melanogaster.jpg

Araştırmacıların ilgisini çeken şey, küçük bir sinir sisteminin davranış üretme biçimi. Duyusal bir işaret nasıl değerlendirilir? Hangi hücreler hareketi başlatır? Aynı uyaran neden her durumda aynı tepkiye yol açmaz? Beynin bağlantılarını bilmek, bu soruları tek tek hücreler üzerinden araştırmayı mümkün kılıyor. Küçük olması, bütün işleyişinin kolayca çözülebildiği anlamına gelmiyor. Bir beynin bağlantı haritası nasıl çıkarılıyor? Beyindeki sinir hücrelerine nöron, bu hücrelerin birbirine sinyal ilettiği bağlantı noktalarına sinaps deniyor. Konnektom (connectome), yani sinir bağlantı haritası, hangi nöronun hangi nöronlarla bağlantı kurduğunu gösteriyor. Bir şehrin yollarını düşünelim: Harita, mahallelerin birbirine nasıl bağlandığını anlatır.

O anda hangi araçların geçtiğini ve trafik yoğunluğunu ise ayrıca ölçmek gerekir.

Bu haritalar, canlı sineğin düşüncelerini uzaktan okuyarak elde ediliyor. Hazırlanmış doku örnekleri elektron mikroskopuyla görüntüleniyor; bilgisayarlar ve yapay zekâ yöntemleri, çok sayıdaki görüntüde hücrelerin sınırlarını ve uzantılarını izleyerek üç boyutlu yapıyı yeniden kuruyor. İnsan uzmanlar da hataları düzeltiyor ve hücreleri sınıflandırıyor. Elde edilen veri, dokunun yapısal bir kaydı; yaşamı boyunca değişmeden kalacak kusursuz bir “sinek planı” değil. [1]



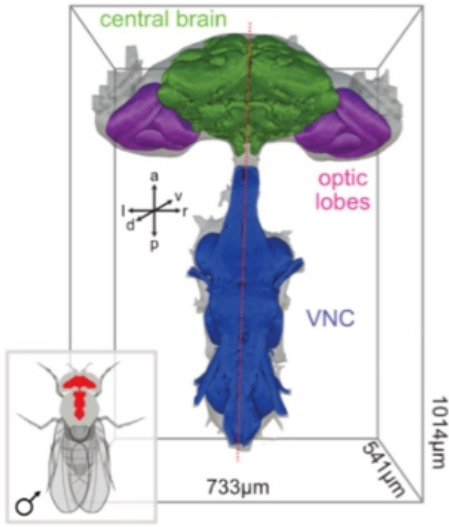
Görsel 2. Erkek meyve sineğinin beyin ve sinir kordonundaki hücrelerin bir bölümü, iki farklı açıdan gösteriliyor. Görsel yapısal bir çizimdir; o anda gerçekleşen düşüncüyü veya sinir etkinliğini göstermiyor. Kaynak: Google Research / HHMI Janelia ve çalışma ortakları, 2026.

(<https://research.google/blog/a-connectomics-milestone-mapping-the-complete-male-fruit-fly-brain/>)

2024 ile 2026 arasındaki önemli fark

Sosyal medyada sanki bütün gelişmeler aynı hafta yaşanmış gibi anlatılıyor. Oysa 2 Ekim 2024'te Nature'da yayımlanan FlyWire çalışması, yetişkin bir dişi meyve sineğinin beyindeki 139.255 nöronu ve 54,5 milyon kimyasal sinapsı haritaladı. Aynı çalışma dizisinin hücre sınıflandırması 8.453 hücre tipi tanımladı; bunların 4.581'i yeni tiplerdi ve çoğu daha önce ayrıntılı biçimde kapsanmayan beyin bölgelerinden geldi. Yani ortaya çıkan şey yalnızca dev bir bağlantı listesi değil, beynin parçalarını adlandırmaya başlayan ayrıntılı bir katalogdu. Bu kaynaklar, 2026'daki daha geniş çalışmaların başlıca dayanaklarından biri oldu. [1][16]

2026'da öne çıkan MaleCNS, yetişkin bir erkek sineğin merkezî sinir sisteminin haritalıyor; merkezî beyni, görme loblarını ve beden hareketleriyle ilişkili karın sinir kordonunu birlikte kapsıyor. 3 Ekim 2026'da yayımlanan nihai Cell makalesi, erkek merkezî sinir sisteminde 166.700 nöron ve uzmanlar tarafından doğrulanmış bağlantı ağında yaklaşık 124,2 milyon sinaptik bağlantı bildiriyor. Çalışma, HHMI Janelia, Cambridge Üniversitesi, MRC Moleküler Biyoloji Laboratuvarı ve Google Research iş birliğine dayanıyor. Böylece yalnızca beyin haritasından, beynin bedenle bağlantısını da izleyebileceğimiz daha geniş bir kapsama geçiliyor. [2][3][9]



Görsel 3. MaleCNS haritasının kapsamı: merkezi beyin yeşil, görme lobları mor, karın sinir kordonu mavi gösteriliyor. Kaynak: Google Research / HHMI Janelia ve çalışma ortakları, 2026.

(<https://research.google/blog/a-connectomics-milestone-mapping-the-complete-male-fruit-fly-brain/>)

Projenin kayıtlarına göre MaleCNS'nin 1.0 sürümü 8 Haziran 2026'da açıldı; hakemli Cell makalesi 3 Ekim 2026'da yayımlandı. Eylül ayındaki duyurular, verilerin çok daha geniş bir kitleye ulaşmasını sağladı. Dolayısıyla internette karşılaştığımız her "dijital sinek", aynı haritayı veya aynı bilgisayar modelini kullanmıyor. [2][3] Beyin ile bedenin birlikte çalışmasını anlamak 2026'nın önemli gelişmelerinden biri de BANC adı verilen, beyin ile karın sinir kordonunu aynı haritada birleştiren çalışma. 8 Haziran 2026'da Nature'da çevrim içi yayımlanan bu araştırma, yetişkin bir dişi sineğe dayanıyor; yukarıda anlatılan erkek MaleCNS örneğinden ayrı bir veri seti. Böylece bir duyunun hareketi nasıl etkileyebileceği, beyin ile beden arasındaki bağlantılar boyunca izlenebiliyor. [12] Haritanın ortaya koyduğu ilginç sonuç, hareketin denetiminin birçok yerel devre arasında paylaşılması. Örneğin bir bacakla ilişkili duyuşal ve hareket sinyalleri, o bölgeye ait geri bildirim döngülerinde buluşuyor. Bu devreler diğer uzuvların devreleriyle iletişim kurarken, öğrenme ve yön bulmayla ilişkili beyin bölgeleri de sistemi yönlendiriyor. Araştırmacılar böylece davranışın, farklı bölgelerin birlikte çalışmasıyla nasıl oluşabileceğini inceleyebiliyor. Robotik açısından bu biyolojik düzenin mühendislikteki dağıtık kontrol sistemlerine benzemesi dikkat çekici. Sinir bağlantılarının ayrıntıları, yerel birimlerin nasıl koordine edildiğini araştırmak için somut bir örnek sunuyor. [12]

Haritadan çalışan bir modele geçmek

Bir bağlantı listesini indirdiğimizde elimizde kendiliğinden çalışan bir beyin bulunmuyor. Hücrelerin gelen sinyallere nasıl tepki vereceğini de tanımlamamız gerekiyor. Philip Shiu ve çalışma arkadaşlarının 2024'te yayımladığı model, bu konuda önemli bir örnek. Araştırmacılar bağlantı verilerini, hücrelerin kullandığı kimyasal iletilere ilişkin tahminlerle birleştirdi ve nöronların etkinliğini hesaplayan bir sistem kurdu. [4]

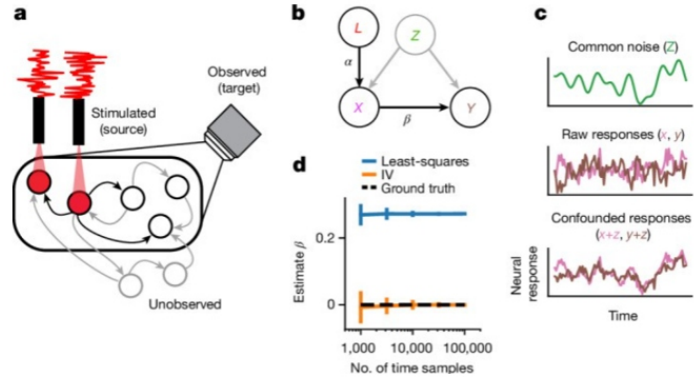
Modelde nöron, basitleştirilmiş biçimiyle, gelen etkileri biriktiriyor; belirli bir eşik aşıncı kısa bir sinyal üretiyor. Birikim zamanla azalıyor. Bu yaklaşım "sızdıntılı bütünleştir ve ateşle" (leaky integrate-and-fire) modeli olarak biliniyor. Sinaps sayıları bağlantıların etkisini tahmin etmekte kullanılıyor; fakat gerçek bir sinapsın gücünü yalnızca sayısından tam olarak öğrenemeyiz. Hücrelerin ayrıntılı biyokimyası ve zaman içinde değişen durumları için ek bilgi gerekir.

[4]

Ardından modeli bir çevreye bağlamak geliyor. Bir bilgisayar oyunundaki görüntüler, sanal duyuşal girdilere dönüştürülebilir. Hesaplanan nöron etkinliği de "sağa dön" veya "ilerle" gibi komutlara çevrilebilir. Bu çevirinin kurallarını geliştirici belirler. Ekranda görülen hareket, hem sinir ağı modelinin hem de bu arayüzün ortak sonucudur. [6]

Bağlantı haritasından etki haritasına: "effectome"

Bir konnektom, A nöronunun B nöronuna bağlandığını gösterebilir; ancak A'nın etkinliğini değiştirdiğimizde B'nin canlı beyinde ne kadar ve hangi yönde etkileneceğini tek başına söylemez. Pospisil ve çalışma arkadaşları 2 Ekim 2024'te Nature'da yayımladıkları çalışmada bu boşluğu hedefleyen "effectome" kavramını kullandı. Araştırmacılar, bağlantı haritasını bir ön bilgi olarak kullanıp stokastik optogenetik uyarımlardan elde edilen verilerle nöronlar arasındaki nedensel etkileri daha verimli tahmin etmeyi amaçlayan istatistiksel bir yöntem geliştirdi. Bu deneysel mantık Görsel 4'te şematik olarak gösteriliyor. [15]



Görsel 4. Effectome çalışmasının deney ve çıkarım mantığını gösteren şema.

Belirli nöronlar optogenetik olarak uyarılırken gözlenen hedef nöronların tepkileri ölçülüyor; ortak gürültünün ve doğrudan gözlenmeyen değişkenlerin yol açabileceği karışıklıklar istatistiksel modellerle ayrıştırılmaya çalışılıyor. Amaç, yalnızca bağlantının varlığını değil, bir müdahalenin hedef nöron üzerindeki nedensel etkisini daha güvenilir biçimde tahmin etmek. Kaynak: Pospisil ve diğerleri, Nature, 2024. Makale ve bu şekil CC BY 4.0 lisansı kapsamındadır.

(<https://doi.org/10.1038/s41586-024-07982-0>)

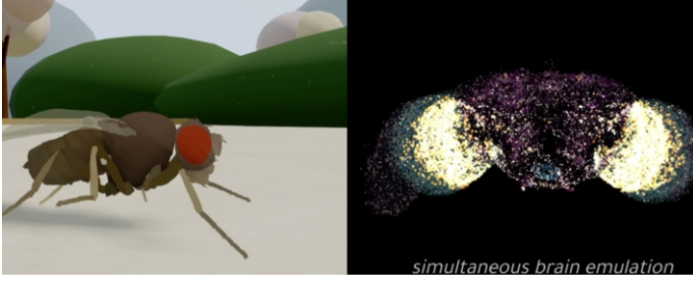
Burada önemli bir sınır var: Çalışma, sineğin tamamlanmış bir "etki haritasını" sunmuyor. Bunun yerine, beyin yalnızca kablo şemasını değil, belirli düğümlere müdahale edildiğinde ağın nasıl tepki verdiğini de ölçebileceğimiz bir yola işaret ediyor. Dijital beyin tartışması açısından bu ayrım kritik; anatomik olarak bağlı olmak ile bir davranış sırasında güçlü ve nedensel bir etki yaratmak aynı şey değil. [15]

Sanal bedende yürümek ve yiyecek aramak

Döner videosundan önce, Mart 2026'da Eon Systems daha doğrudan biyolojik davranışlara odaklanan bir gösteri yayımladı. Ekip, bağlantı haritasına dayanan beyin modelini NeuroMechFly adlı sanal sinek bedeniyle birleştirdi. Gösteride sinek, sanal tat ipuçlarıyla yiyeceğe yöneliyor; üzerinde biriken sanal toza tepki olarak durup antenlerini temizliyor ve ardından beslenmeye devam ediyor. Buradaki önemli adım, algı ile hareket arasındaki döngüyü kurmak: Çevreden gelen sinyal modeli etkiliyor, hareket çevreyle ilişkiyi değiştiriyor ve yeni duyuşal bilgi yeniden modele dönüyor. [13]

Eon'un teknik açıklaması, bu davranışların nasıl üretildiğini de netleştiriyor. Yürüme ve temizlenmede kullanılan beden denetleyicileri, sineğin hareketlerini taklit edecek şekilde önceden eğitilmiş; beyin ile beden arasındaki bazı eşleştirmeleri geliştiriciler elle belirlemiş. Görsel girdiler o sürümde davranışı henüz belirgin

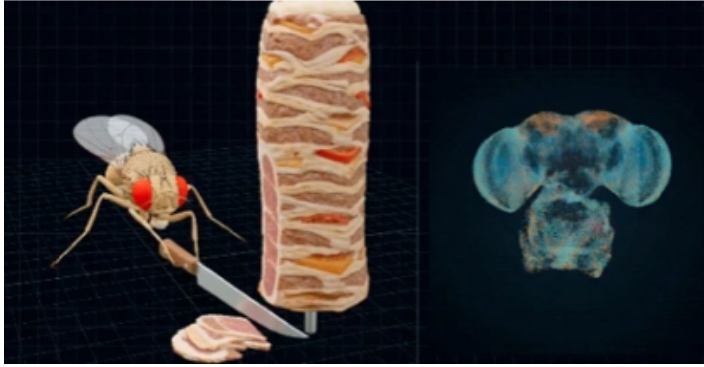
biçimde etkilemiyor; öğrenme ve iç durum değişiklikleri de büyük ölçüde eksik. Dolayısıyla gösterinin değeri, eksiksiz bir canlı kopyalandığını kanıtlamasında değil, beyin modelinin çevreyle etkileşimini oynayabileceğimiz somut bir düzenek sunmasında. [13]



Görsel 5. Eon Systems'in sanal sinek gösterisinde beden modeli ile beyin modelinin görselleştirilmesi yan yana görülüyor. Çalışma, belirli davranışları simülasyon düzeneği. Kaynak: Eon Systems, 2026. (<https://eon.systems/updates/embodied-brain-emulation>)

Döner kesen sinek haberinin sınırı

Döner kesme paylaşımı, Onur Özcan'ın 11 Ekim 2026 tarihli gönderisine dayanıyor. Gönderi, sineği döner kesmek üzere eğittiği iddiasını mizahi bir dille sunuyor; Eon Systems'in aynı dönemde derlediği sosyal medya örnekleri arasında da yer alıyor. Burada karşımıza çıkan, gerçek bir hayvanın eline bıçak verildiğini gösteren bir laboratuvar kaydı değil, dijital bir gösteri. [5]



Görsel 6. Onur Özcan'ın 11 Ekim 2026 tarihli döner kesme paylaşımından bir kare. Sosyal medya gösterisi, modelin öğrenme kapasitesine ilişkin bağımsız bilimsel kanıt olarak değerlendirilmemeli. Kaynak: @oozn / X. (<https://x.com/oozn/status/2098508072670912833>)

Bu görüntüyü izlemek, altta hangi bağlantı haritasının kullanıldığını, davranışın ne kadarının önceden yazılmış kurallardan geldiğini veya gerçekten öğrenme gerçekleşip gerçekleşmediğini tek başına açıklamaz. Bunun için kodun, eğitim yönteminin ve karşılaştırmalı testlerin incelenmesi gerekir. "Döner kesen sinek" ifadesi ilgi çekici bir başlık olabilir; bilimsel sonuç olarak kullanıldığında ise gösterdiğinden fazlasını iddia etme riski taşır.

Oyun örneklerinde de aynı dikkat gerekli. Açık kaynaklı DOOMFLY projesinin 26 Ekim 2026'da erişilen güncel açıklaması, deneysel eğitim açık olsa da modelin oyunda hayatta kalmayı öğrendiğinin henüz gösterilmediğini belirtiyor. Mevcut v6 adayının görsel işleme, koşullanma ve hayatta kalma doğrulama kapılarından geçemediği de açıkça yazılıyor. Bir karakterin hareket etmesiyle, oyunu öğrenmesi arasındaki farkı projenin geliştiricileri de vurguluyor. [6]

Asıl bilimsel başarı nerede

Bir modelin değeri, gerçek sinekte sınanabilecek bir tahmin ürettiğinde daha iyi anlaşılır. Örneğin belirli hücreleri susturduğumuzda beslenmeyle ilgili sinyaller nasıl değişir? Başka bir hücre grubunu etkinleştirmek temizlenme davranışını etkiler mi?

Shiu ve arkadaşları, beslenme ve temizlenme devreleri için modelden elde ettikleri tahminleri canlı hayvan deneyleriyle sınadı. Deneysel olarak test edebildikleri 164 tahminin yüzde 91'i gözlenen sonuçlarla uyumluydu; belirli bir optogenetik test grubu dışlandığında bu oran yüzde 84'tü. Bu sayıların "sineğin beyinin yüzde 91'i kopyalandı" anlamına gelmediğini özellikle vurgulamak gerekir: Ölçülen şey, modelin test edilen belirli duyuşal-motor ilişkileri ne kadar doğru öngördüğüdür. [4]

Janne Lappalainen ve arkadaşlarının 2024 tarihli başka bir Nature çalışması da sineğin görsel hareket işleme yollarındaki 64 hücre tipini kapsayan bir model kurdu. Bağlantı yapısı ölçümlerden alındı; bilinmeyen bazı hücre ve sinaps özellikleri, görsel hareketi hesaplama görevine göre ayarlandı. Model, deneylerde ölçülmüş çeşitli nöron tepkilerini tahmin edebildi. Bu sonuç, yapısal haritanın uygun hesaplama yöntemleriyle birleştirildiğinde işleyiş hakkında bilgi verebildiğini gösteriyor. [7]

Bağlantı haritası hafızayı anlamaya da yardım ediyor

Konnektomların kullanım alanı yalnızca yürüme, beslenme veya görsel hareketle sınırlı değil. 22 Temmuz 2024'te Nature'da çevrim içi yayımlanan başka bir çalışma, 500'den fazla meyve sineğinde canlı voltaj görüntüleme deneyleri yaparak kısa ve uzun süreli hafıza devreleri arasındaki ilişkiyi inceledi. Araştırmacılar, dopamin nöronları ile mantar cisimciği adı verilen öğrenme-hafıza merkezindeki bağlantıları, sineğin bilinen bağlantı haritasıyla sınırlandırılmış bir hesaplama modelinde birleştirdi. [17]

Model, kısa süreli hafıza devrelerindeki geri bildirimin uzun süreli hafızanın kurulmasını nasıl etkileyebileceğine ilişkin yeni tahminler üretti; ekip bu tahminlerin bir bölümünü daha sonra deneysel müdahalelerle doğruladı. Bu örnek, bağlantı haritasının yalnızca sabit bir anatomi atlası olmadığını gösteriyor: Doğru deneylerle birleştirildiğinde öğrenme ve hafıza gibi zamana bağlı süreçler hakkında da sınanabilir hipotezler üretilebiliyor. [17]

Erkek ve dişi sinir sistemlerinin karşılaştırılması da ayrı bir araştırma alanı açıyor. 3 Ekim 2026'da Cell'de yayımlanan nihai MaleCNS makalesi, erkek merkezli sinir sisteminde toplam 11.710 nöron tipi tanımladı ve erkek-dişi bağlantı haritalarını sinaps çözünürlüğünde karşılaştırdı. Bu karşılaştırmada araştırmacılar 8.069 tipi iki cinsiyette yapısal olarak eşleşen (izomorfik), 138 tipi dimorfik, 289 tipi erkeğe özgü ve 71 tipi dişiye özgü olarak sınıflandırdı.

Toplam 11.710 nöron tipi ile bu dört karşılaştırma sayısı farklı kapsamları özetlediğinden, dört değer 11.710 toplamının basit bir dökümü olarak okunmamalıdır. Cinsiyete özgü ve dimorfik nöronlar daha çok üst düzey bütünleştirici beyin merkezlerinde yoğunlaşırken, duyuşal giriş ve motor çıkış çevresi büyük ölçüde benzer kaldı. Google Research'in görselleştirdiği AOTU008 örneğinde erkek nöronunda dişi karşılığına göre iki ek uzantı görülmesi, bu farkların somut örneklerinden biri. Bazı proje ve ön baskı sayfalarında daha eski sayılar görülebilir; burada hakemli Cell makalesinin nihai değerleri kullanılmıştır. Sayısal özet Görsel 7'de. [3][8][9]

ERKEK-DİŞİ MEYVE SİNEĞİ HÜCRE TİPİ KARŞILAŞTIRMASI

Nihai Cell makalesi • 3 Eylül 2026



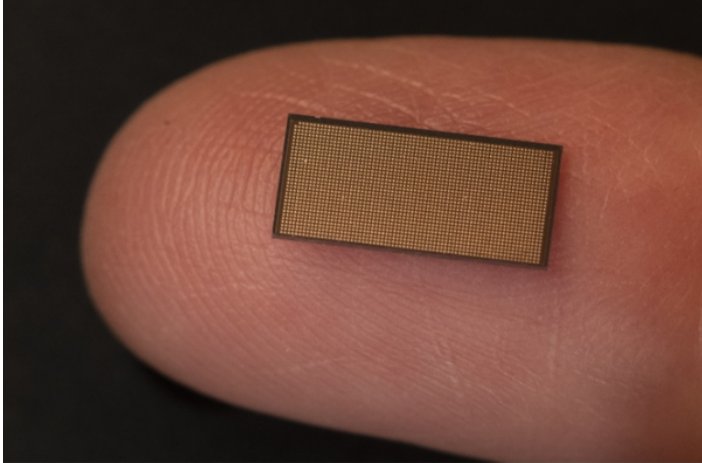
Görsel 7. Nihai Cell makalesinin erkek-dişi beyin karşılaştırmasında raporlanan hücre tipi sınıflarının sayısal özeti. 8.069 tip iki cinsiyette yapısal olarak eşleşen (izomorfik), 138 tip dimorfik, 289 tip erkeğe özgü ve 71 tip dişie özgü olarak sınıflandırıldı. Bu dört değer, erkek merkezli sinir sisteminde tanımlanan toplam 11.710 nöron tipinin basit bir alt toplamı değildir; makalenin cinsiyetler arası karşılaştırmada raporladığı sınıfları özetler. Bu görsel, makaledeki nihai sayılardan BT Kıbrıs için hazırlanmış özgün bir özetdir. Kaynak: Berg ve diğerleri, Cell, 2026.

(<https://doi.org/10.1016/j.cell.2026.08.015>)

Beyin benzeri çiplerde çalışan sinek modeli

Bir başka önemli gelişme donanım tarafında. Sandia Ulusal Laboratuvarları araştırmacıları, Ağustos 2025'te arXiv'de yayımladıkları ön baskı çalışmada FlyWire'a dayanan yaklaşık 140 bin nöronlu ve 50 milyon sinapslı modeli 12 Intel Loihi 2 çipine yerleştirdi. Loihi 2, sinir hücrelerinin kısa sinyallerle haberleşmesinden esinlenen nöromorfik, yani sinir sistemi benzeri bir hesaplama donanımdır. Burada canlı hücreler kullanılmıyor; nöronların matematiksel modelleri elektronik çiplerde çalıştırılıyor. [14]

Araştırmacılar, ağırlık çıktısını başka simülasyonlarla karşılaştırdı ve kendi deneylerinde geleneksel donanımdaki sayısal simülasyonlara göre daha hızlı çalıştığını bildirdi. Bu sonuç, beyin araştırmaları için pratik bir soruya cevap arıyor: Çok sayıda düzensiz sinir bağlantısını nasıl daha hızlı hesaplayabiliriz? Böyle donanımlar, araştırmacıların aynı model üzerinde daha fazla deney yapmasını kolaylaştırabilir. Çalışma bir ön baskı olduğundan, sonuçlarını bu yayın aşamasını belirterek değerlendirmek gerekir. [14]



Görsel 8. Parmak ucunda gösterilen Intel Loihi 2 çipi. Nöromorfik donanım, sinir hücrelerinin işleyişinden esinlenen hesaplamalar yapıyor. Fotoğraf: Intel.

(<https://download.intel.com/newsroom/2021/new-technologies/intel-loihi-2.zip>)

Yapay zekâ ile insan beynine uzanan sorular

Bu gelişmelerde yapay zekânın iki rolü var. Önce mikroskop görüntülerinden sinir yapılarının çıkarılmasına yardımcı oluyor. Sonra biyolojik bağlantılar, davranış veya nöron etkinliğini hesaplayan modellerin kurulmasında kullanılabiliyor. Bu modelleri, internetteki metinlerle eğitilmiş bir sohbet sistemiyle aynı yöntem

sanmamak gerekir. Kullanılan veri, amaç ve sinama biçimi farklıdır. [7][9]

Biyolojik bağlantılardan yararlanmak, bir modelin otomatik olarak daha zeki veya daha az enerji tüketen bir sisteme dönüşeceğini de göstermez. Böyle iddialar için aynı görevi yapan alternatiflerle ölçüm gerekir. Bir simülasyonun ilginç davranması, hem mühendislik açısından verimli hem de biyolojik açıdan doğru olduğu anlamına gelmeyebilir.

İnsan beynine gelince ölçek çok değişiyor. Yaklaşık 86 milyar nöronun yanı sıra, bu hücrelerin farklı özelliklerini ve değişen etkileşimlerini de anlamamız gerekiyor. Google Research de yaklaşık 86 milyar nöronlu insan beynini aynı ayrıntı düzeyinde haritalamanın ve modellemenin bugün erişilebilir olmadığını belirtiyor. Sinek çalışmaları, sinir sistemlerinin nasıl işlediğini araştırmak için güçlü bir adım; insan zihninin bilgisayara aktarılabilirliğini gösteren bir deney değil. [9][10]

Ekrandaki modele insan gibi niyetler ve duygular yüklemek de kolay. Ancak bir oyunda "ödül" verilmesi, modelin haz duyduğunu; hasar sinyali alması, acı yaşadığını kanıtlamaz. Böyle bir öznel deneyimin varlığı, yalnızca hareket eden bir görüntüye bakılarak belirlenemez. Bilinç tartışması, bağlantı haritasının ne ölçtüğünden ayrı ve daha zor bir sorudur.

Kıbrıs için erişilebilir bir araştırma alanı

Bu hikâyede Kıbrıs'taki öğrenciler ve araştırmacılar açısından dikkat çekici olan, verilerin ve bazı model kodlarının açık olması. Bir beynin haritasını çıkarmak büyük altyapı gerektiriyor; hazırlanmış harita üzerinde soru sormak içinse aynı laboratuvarı baştan kurmak gerekmiyor. Shiu ekibinin kodları, belirli hücrelerin etkinleştirilmesini veya susturulmasını ve sonuçların incelenmesini mümkün kılıyor. [2][11]

Bence üniversitelerimizde yapılabilecek anlamlı bir başlangıç, yayımlanmış bir sonucu yeniden üretmeye çalışmak olabilir. Ardından birkaç bağlantıyı değiştirip modelin tepkisinin nasıl etkilendiği araştırılabilir. Gerçek bağlantı düzenini karıştırılmış bir ağla karşılaştırmak da, başarının hangi bölümünün biyolojik yapıdan geldiğini sorgulamanın bir yolu olur.

Döner videosu birkaç saniyede dikkatimizi çekiyor. Haritanın kalıcı değeri ise davranışın hangi bağlantılarla ortaya çıktığına ilişkin soruları daha somut biçimde sınıyabilmemiz. Bir sineğin beyni hakkında artık daha ayrıntılı sorular sorabiliyoruz. Cevapların ne kadar doğru olduğunu belirleyecek olan da görüntünün etkileyiciliği değil, modelin gerçek deneylerle ne ölçüde uyduğu.

Ata Ateş

Yapay Zeka Mühendisliği
DAÜ 3. sınıf öğrencisi

Kaynaklar için cep telefonunuzdan QR kodu okutun



Kıbrıs'ta Yapay Zekâ — Geleceğin Teknolojisi Değil, Bugünün Aracı

Yapay Zekâ Artık Geleceğin Değil, Bugünün Teknolojisi

Yapay zekâ artık uzak bir geleceğin teknolojisi değil. Bir zamanlar bilim kurgu filmlerinde gördüğümüz yapay zekâ sistemleri bugün günlük hayatımızın birçok alanında karşımıza çıkıyor. Metin yazmaktan görüntü oluşturmaya, çeviri yapmaktan bilgisayar kodu üretmeye kadar pek çok işlem artık yapay zekâ destekli araçlarla gerçekleştirilebiliyor. Özellikle son yıllarda üretken yapay zekânın yaygınlaşmasıyla birlikte bu teknoloji, yalnızca teknoloji dünyasının değil, toplumun tamamının gündemine girdi.[1]

Dünyada olduğu gibi KKTC'de de yapay zekânın farklı sektörlerde kullanım alanları gündeme geliyor. Üniversitelerde öğrencilerin öğrenme süreçlerini desteklemek, turizm sektöründe ziyaretçilere kişiselleştirilmiş hizmetler sunmak, tarımda ürün ve hastalık takibi yapmak gibi kullanım alanları öne çıkıyor. Bu nedenle asıl soru, yapay zekânın KKTC'ye gelip gelmeyeceği değil; KKTC'nin bu teknolojiyi kendi ihtiyaçları doğrultusunda ne kadar etkili kullanabileceği.[1][2]

Eğitimde Değişen Öğrenme Deneyimi



(<https://unsplash.com/s/photos/artificial-intelligence-education>)

Yapay zekânın KKTC'de etkisini gösterebileceği alanların başında eğitim geliyor. Özellikle farklı ülkelerden öğrencilerin eğitim aldığı üniversitelerde yapay zekâ, öğrenme sürecini daha kişisel ve erişilebilir hale getirebilir. Örneğin Türkçe eğitim alan bir öğrenci İngilizce bir akademik kaynağı anlamak için yapay zekâdan yararlanabilirken, farklı ülkelerden gelen öğrenciler ders içeriklerini kendi dillerinde daha kolay anlayabilir. Öğrenciler ayrıca anlamadıkları ders konularını seviyelerine uygun şekilde açıklayabilir, kodlama hatalarını inceleyebilir veya sınavlara hazırlanmak için kişiselleştirilmiş çalışma soruları oluşturabilir.

KKTC'de **yapay zekâ okuryazarlığı konusunda da çalışmalar yürütülüyor**. Doğu Akdeniz Üniversitesi ile KKTC Milli Eğitim Bakanlığı iş birliğiyle 2026 yılında yapay zekâ okuryazarlığı eğitimleri başlatıldı.[4] Bu tür çalışmalar, yapay zekânın yalnızca teknik bir konu olmadığını, **eğitim süreçlerinde bilinçli kullanımı da önem kazandığını** gösteriyor.

Kıbrıs'taki üniversitelerin farklı bölümlerinde de bu teknolojinin kullanım alanları oldukça geniş. Mühendislik öğrencileri kodlama ve teknik problemlerde, mimarlık öğrencileri tasarım süreçlerinde, işletme öğrencileri veri analizi ve pazar araştırmalarında yapay zekâdan yararlanabilir. Böylece yapay zekâ yalnızca bir bilgi kaynağı değil, öğrencilerin kendi alanlarında pratik yapmalarını sağlayan bir **dijital öğrenme yardımcısına** dönüşebilir.

Ancak bu kolaylık önemli bir dengeyi de beraberinde getiriyor. Öğrencinin bir konuyu anlamak için yapay zekâdan yardım alması ile ödevini tamamen yapay zekâyı yaptırması aynı şey değil. Ayrıca yapay zekânın verdiği bilgilerin her zaman doğru olmayabileceği de unutulmamalı. Bu nedenle KKTC'de yetişen yeni nesil için önemli olan yalnızca yapay zekâyı kullanabilmek değil, **onu doğru, bilinçli ve eleştirel bir şekilde kullanmayı öğrenmek**.

Turizmde Daha Kişisel Bir Kıbrıs Deneyimi



(China Trading Desk, "AI and Smart Tourism in China 2026: Insights for Travel Brands, Hotels and Destinations".

<https://www.chinatradingdesk.com/post/ai-and-smart-tourism-in-china-2026-insights-for-travel-brands-hotels-and-destinations>)

Kıbrıs denildiğinde yapay zekânın önemli potansiyel taşıdığı alanlardan biri de **turizm**. Ada; farklı ülkelerden gelen turistleri, otelleri, restoranları ve tarihi-kültürel noktalarıyla ziyaretçilere çeşitli deneyimler sunuyor. Yapay zekâ ise bu deneyimi ziyaretçinin ihtiyaçlarına göre kişiselleştirmek için kullanılabilir.

Örneğin Kıbrıs'a birkaç günlüğüne gelen bir turistin bütçesi, ilgi alanları ve seyahat süresi analiz edilerek **ona özel bir gezi planı** hazırlanabilir. Tarihi yerleri merak eden bir ziyaretçiye kültürel

rotalar, deniz ve doğayı tercih eden bir başka ziyaretçiye ise plajlar ve doğa aktiviteleri önerilebilir.

Otellerde **kullanılabilecek yapay zekâ destekli sistemler** ise ziyaretçilerin sorularını farklı dillerde yanıtlayabilir, rezervasyon süreçlerine yardımcı olabilir ve konukların ihtiyaçlarına daha hızlı cevap verebilir.[5]

KKTC'nin yapay zekâ alanındaki planlamalarında turizm için **çok dilli turist asistanları, turizm talep tahmini, otel ve ulaşım optimizasyonu ile kültürel mirasın dijitalleştirilmesi** gibi kullanım alanları da yer alıyor.[1][2]

Bu teknoloji, Kıbrıs'ın yalnızca turistlerin ziyaret ettiği bir ada olmasından öte, ziyaretçilerin kendilerine özel bir deneyim yaşayabildiği **daha akıllı bir turizm destinasyonuna** dönüşmesine katkı sağlayabilir. Ancak burada amaç insan iletişiminin yerini tamamen teknolojiye bırakmak değil; teknolojiyi, turizm çalışanlarının sunduğu hizmeti destekleyen bir araç olarak kullanmak olmalı.

Tarımda Yapay Zekâ ile Akıllı Üretim

KKTC'de tarımın geleceği yalnızca toprağa ve hava koşullarına değil, **teknolojiyi ne kadar doğru kullanabildiğimize** de bağlı. Sınırlı su kaynakları, kuraklık, değişen hava koşulları ve üretim maliyetleri çiftçilerin karşılaştığı önemli sorunlar arasında yer alıyor. Yapay zekâ ise bu sorunların tamamını tek başına çözebilecek bir teknoloji olmasa da, doğru kararlar alınmasına yardımcı olabilecek güçlü bir araç sunuyor.

Tarım ve su yönetimi alanında yapay zekâ kullanımı için **akıllı sulama sistemleri, kuraklık tahmini, bitki hastalıklarının görüntü işleme ile tespiti ve verim tahmin modelleri** gibi kullanım alanları gündeme getiriliyor. Böylece tarlalardan elde edilen görüntü ve veriler analiz edilerek bitki hastalıklarının daha erken fark edilmesi, sulama süreçlerinin daha doğru planlanması ve üretim verimliliğinin artırılması mümkün olabilir.

Özellikle **suyun dikkatli kullanılması gereken Kıbrıs'ta**, bitkilerin ne zaman ve ne kadar suya ihtiyaç duyduğunu belirlemek gereksiz tüketimin azaltılmasına yardımcı olabilir.

Çiftçinin yıllara dayanan deneyimi ile yapay zekânın hızlı veri analiz gücü bir araya geldiğinde, teknoloji insanın yerini almak yerine **daha bilinçli, verimli ve sürdürülebilir bir tarımın destekçisi** haline gelebilir.

İşletmelerde Yapay Zekâ Dönemi

Yapay zekânın etkisi yalnızca büyük teknoloji şirketleriyle sınırlı değil. **KKTC'deki küçük işletmeler, oteller, restoranlar ve yerel işletmeler** de bu araçlardan günlük işlerini kolaylaştırmak için yararlanabilir.

Örneğin Girne'deki bir otel, farklı ülkelerden gelen misafirlerin sorularını birden fazla dilde yanıtlamak için yapay zekâ destekli sistemlerden faydalanabilir. Gazimağusa'daki bir restoran ise

menüsünü farklı dillere uyarlayabilir veya müşteri geri bildirimlerini analiz ederek hizmetini geliştirebilir.

Bir işletme sosyal medya içeriklerini hazırlamak, müşteri taleplerini düzenlemek veya satış verilerini incelemek için bu araçlardan yararlanırken çalışanlar daha çok müşteri ilişkileri ve hizmet kalitesine odaklanabilir. Buradaki amaç **insanın yerini teknolojiye bırakmak değil; insanın sahip olduğu zamanı ve yetenekleri daha verimli kullanmak**.

KKTC Bilgi Teknolojileri ve Haberleşme Kurumu'nun çalışmalarında da **bilişim sektöründe yapay zekâ kullanımının artırılması** ve yapay zekânın sektöre sağlayabileceği katkılarının araştırılması hedefleniyor. [2][3] Bu durum, yapay zekânın yerel işletmeler ve bilişim sektörü açısından önümüzdeki dönemde daha fazla gündeme gelebileceğini gösteriyor.

Yapay Zekânın Getirdiği Riskler



(Easy-Peasy.AI, "AI Security&Privacy Concepts".

<https://easy-peasy.ai/ai-image-generator/images/ai-security-privacy-concepts>)

Yapay zekânın sunduğu fırsatların yanında dikkat edilmesi gereken bazı riskler de var. Özellikle **yanlış veya eksik bilgi üretmesi, kişisel verilerin korunması ve yapay olarak oluşturulan gerçekçi görüntü ve videoların yayılması** önemli konular arasında.

Eğitimden işletmelere kadar farklı alanlarda bu araçların kullanılması arttıkça, verilen bilgilerin doğruluğunu kontrol etmek ve hangi verilerin paylaşıldığına dikkat etmek daha önemli hale geliyor.

KKTC'de de **yapay zekâ destekli dolandırıcılık, veri ve kimlik hırsızlığı** gibi konular gündeme geliyor. [6] Bu nedenle yapay zekânın yaygınlaşması yalnızca yeni sistemlerin kullanılmasına değil, insanların bu sistemleri doğru anlayabilmesine de bağlı.

Yapay zekânın her söylediğini doğru kabul etmek yerine **sorgulamak, önemli bilgileri doğrulamak ve kişisel verileri korumak** artık temel bir dijital beceri haline geliyor. Çünkü gelecekte asıl farkı yaratan, yapay zekâyâ sahip olmak değil; **onu ne zaman kullanacağını, ne zaman sorgulayacağını ve nerede sınır koyacağını bilmek** olacak.

Sonuç: KKTC Yapay Zekâyâ Ne Kadar Hazır?

Yapay zekâ KKTC'de de **eğitimden turizme, tarımdan işletmelere kadar farklı alanlarda gündeme gelmeye ve kullanım alanları geliştirilmeye başladı**. Önümüzdeki dönemde bu teknolojinin hangi alanlarda ne kadar yaygınlaşacağını ise yalnızca teknoloji değil, kurumların, işletmelerin, eğitim sisteminin ve kullanıcıların bu teknolojiyi nasıl benimsediği belirleyecek.

Bu noktada yapay zekâ, insanın yerini alan bir sistemden çok, **doğru kullanıldığında işleri kolaylaştıran ve yeni çözümler geliştirmeye yardımcı olan bir araç** olarak görülmeli. KKTC'nin yapay zekâ ile geleceği, teknolojiyi ne kadar hızlı tükettiğinden değil, **onu kendi ihtiyaçları için ne kadar yaratıcı ve bilinçli kullanabildiğinden** geçiyor.

Aynur Kahraman

Yapay Zeka Mühendisliği 3. sınıf Öğrencisi
Doğu Akdeniz Üniversitesi

Kaynakça

[1] KKTC Bayındırlık ve Ulaştırma Bakanlığı — “KKTC, Türkiye'nin Yapay Zekâ Eylem Planında Yerini Alacak”
<https://bub.gov.ct.tr/DA%C4%B0RE-VE-KURUMLAR/KIBRIS-T%C3%9CRK-DEN%C4%B0ZC%C4%B0L%C4%B0K-%C5%9ET%C4%B0/rikli-kktc-t220rk%C4%B0yen%C4%B0n-yapay-zek194-eylem-planinda-yer%C4%B0n%C4%B0-alacak>

[2] Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) — 2026 Yılı İş Planı
<https://www.bthk.org/Documents/2026-Nihai-Is-Plani.pdf>

[3] Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) — 2025–2027 Stratejik Planı
<https://www.bthk.org/Documents/raporlar/BTHK%20Stratejik%20Plan%C4%B1%2025-27.pdf>

[4] Doğu Akdeniz Üniversitesi — “DAÜ ve Milli Eğitim Bakanlığı İş Birliğiyle Yapay Zekâ Okuryazarlığı Eğitimleri Başladı”
<https://www.emu.edu.tr/tr/haberler/haberler/dau-ve-milli-egitim-bakanligi-is-birligiyle-yapay-zek-okuryazarligi-egitimleri-basladi/1206/pid/5647>

[5] DAÜ AI Summit'26 — Doğu Akdeniz Üniversitesi
<https://aisummit.emu.edu.tr/tr>

[6] Türk Ajansı Kıbrıs (TAK) — “Yapay zekâ destekli dolandırıcılık, veri ve kimlik hırsızlığı, siber zorbalık suçları KKTC'de de artıyor”
<https://tak.gov.ct.tr/haber-detay/yapay-zeka-destekli-dolandiricilik-veri-ve-kimlik-hirsizligi-siber-zorbalik-suclari-kktcde-de-artiyor>

KKTC'de Kamera İzin ve Denetim Rejimi: Özel Hayat, Veri Koruma ve Çözüm Önerileri

Kuzey Kıbrıs Türk Cumhuriyeti'nde kamuya açık alanları görüntüleyen sabit kameralar, 31/2018 sayılı Kent Güvenlik Yönetim Sistemi Yasası kapsamında Kent Güvenlik Sistemleri Kurulunun kararına bağlanmıştır. Yeni sistemler için temel kural ön izin, Yasa öncesindeki sistemler için ise bildirim ve sonradan uygunluk mekanizmasıdır.

Uygulamadaki başlıca sorun, kararların teknik ve hukukî bakımdan yeterince anlaşılır olmamasıdır. “Kamuya açık alan görüntüsü bulunmadığı için kameranın iznendirilmesi Kurul yetkisinde değildir” ifadesi, kameranın KGY Kurulunun görev alanı dışında bırakıldığını anlatır; başka bir hukukî yükümlülüğü ortadan kaldırmaz. Başvuru makamı açıklanmadığında vatandaşın “Öyleyse kimden izin alacağım?” sorusu cevapsız kalır.

Bu yazı bütün kamera sistemlerinin kesin olarak hukuka aykırı olduğunu ileri sürmez. Fakat kamera bazında gerekçe, canlı maskeleye, saklama, erişim günlüğü, veri sahibi hakları, etki değerlendirmesi ve bağımsız denetim bakımından görünür boşluklar vardır. Çözüm, süreci ölçülebilir ve şeffaf hale getirmektir.

Hukukî çerçeve ve kurul kararları

Yasanın 9. maddesi, Kurul kararı olmadan kamuya açık alanları görüntülemek amacıyla bilişim sistemi kurulumayacağını düzenler. Bu nedenle yeni sistem bakımından genel kural “önce kur, sonra izin al” değildir. Ekipman satın almak ile sistemi fiilen kurmak farklı aşamalardır; izin zamanının rehberde gösterilmesi gerekir.

Yasa öncesinde kurulmuş sistemler için bildirim ve sonradan uygunluk mekanizması vardır. Uygun bulunmayanlar kaldırılabilir, taşınabilir veya azaltılabilir. Bu geçiş hükmü, yeni sistemlerin ön izinsiz kurulması için genel dayanak yapılamaz.

Kurul kararlarındaki ifadenin en makul anlamı, kameranın KGY Yasası kapsamında kamuya açık alanı görüntüleyen bir sistem sayılmamasıdır. Bu, kameranın kesin olarak hukuka aykırı veya onaylanmış olduğu değil, KGY Kurulundan izin verilmediği anlamına gelir.

17 Nisan 2026 ve 3 Ekim 2026 tarihli kararlardaki açıklamaya göre, kamera kamuya açık alanı veya başkasına ait herhangi bir alanı görüntülemiyorsa KGY Kurulunun iznine gerek olmayabilir. Ancak bu, hiçbir hukukî yükümlülük bulunmadığı anlamına gelmez. Kimliği belirlenebilir kişilerin görüntüsü işleniyorsa 89/2007 sayılı Kişisel Verilerin Korunması Yasası gündeme gelebilir. Başka sektörel düzenlemeler de uygulanabilir. Kapsam dışı bırakma kararında neden, bunun otomatik hukukî serbestlik anlamına gelmediği ve varsa başka başvuru mercii yazılmalıdır. Kısmi onaylarda sonuçlar kamera bazında gösterilmelidir.

Özel hayat ve veri koruma riskleri

KKTC Anayasası özel hayatı korur. 89/2007 sayılı Yasa, kişisel verilerin yasal, amaçla sınırlı, gerekli ve güvenli biçimde işlenmesini öngörür. Kimliği belirlemeye elverişli görüntü kişisel

veridir; kamu güvenliği amacı sınırsız toplama izni vermez. Başlıca risk, kurul izni ile veri işleme dayanağının karıştırılmasıdır. Kamera izni; canlı izleme, kayıt, dışa aktarma, başka kuruma verme, plaka eşleştirme veya yüz tanıma faaliyetlerine otomatik izin sayılmamalıdır. Her işlem ayrıca değerlendirilmelidir.

İkinci risk, gereklilik ve ölçülülüğün görünür olmamasıdır. Somut güvenlik riski, alternatiflerin neden yetersiz kaldığı ve yeniden değerlendirme zamanı açıklanmalıdır. Kamusal alanda bulunmak, sürekli izleme için önceden rıza anlamına gelmez.

Üçüncü risk, canlı görüntü ile kayıt görüntüsünün karıştırılmasıdır. Kayıt oynatılırken yapılan maskeleye, canlı görüntüyü daha önce izleyen kişinin alanı görmüş olmasını ortadan kaldırmaz. Maskeleyenin hangi aşamada uygulandığı belirtilmeli; mümkünse gereksiz alan fiziksel açıyla dışlanmalı veya canlı akışın kaynağında maskelenmelidir.

Dördüncü risk, saklama ve erişim zinciridir. KGY Yasası suçla ilgili olmayan canlı görüntülerin üç aydan fazla tutulmamasını ve üzerine yazılmasını öngörür. Ancak suçla ilgili görüntünün ne zaman ayrılacağı, muhafaza emrini kimin vereceği, emrin ne zaman gözden geçirileceği ve soruşturma sonunda görüntünün ne zaman silineceği ortak protokole bağlanmalıdır. Kimlerin görüntüyü izlediği, kopyaladığı veya dışa aktardığı kaydedilmelidir.

Beşinci risk, veri sahibi haklarına erişim güçlüğüdür. Kişi veri sorumlusunu ve başvuru kanalını bilmiyorsa erişim, düzeltme, silme ve itiraz haklarını kullanamaz. Kamera levhası bu bilgilere yönlendirmelidir.

Altıncı ve en dikkat çekilmesi gereken risk, yapmış olduğumuz çalışmalar neticesinde bir NVR kayıt cihazına canlı kamera görüntüsü yerine sahte video görüntüsünün aktarılabilmesi ve böylelikle digital delilin aldatılabileceğidir. Test ortamında bu çalışma tamamlanmış ve akademik bir makale olarak şu anda onay beklemektedir.

GDPR ve uluslararası standartlarla karşılaştırma

GDPR KKTC'de doğrudan uygulanmaz; bu nedenle bütün kameraların GDPR'ye aykırı olduğu söylenemez. Ancak GDPR, Avrupa Veri Koruma Kurulu rehberliği, kolluk amaçlı veri işleme için 2016/680 sayılı AB Direktifi, AİHM içtihadı ve Convention 108+ karşılaştırmalı bir güvence çerçevesi sunar. Bu standartlar, büyük ölçekli ve sistematik kamu alanı izlemelerinde önceden veri koruma etki değerlendirmesi bekler. KKTC belgelerinde teknik bilgi ve fotoğraf istenmekle birlikte bütün sistemler için zorunlu ve kamuya açık bir DPIA standardı doğrulanamamıştır. Veri sorumlusu ve analitik işlevler de her kararda açık değildir.

Dolayısıyla KKTC mevzuatı bazı güvenceler içerse de amaç ve hukukî dayanak, veri minimizasyonu, katmanlı bilgilendirme, erişim günlükleri, suç kayıtlarının yaşam döngüsü ve bağımsız denetim bakımından uluslararası standartların beklediği açıklık henüz görünür değildir.



Karar arşivi ve kamera ölçeği

24 Ekim 2026 tarihinde Başbakanlığın resmi karar arşivinde 2019–2026 dönemine ait 22 karar kaydı incelenmiştir. “Onay” olarak görünen başvuru veya konum satırları toplandığında 296 olumlu satır ortaya çıkmaktadır. Bu sayı 296 benzersiz fiziksel kamera değildir; kararlar çoğu zaman kamera adedi yerine başvuru sahibi veya konum yayımlar ve bazı başvurular tekrarlanmış olabilir.

8 Eylül 2025 tarihli bir kararda üç olumlu satır içinde altı kamera belirtilmiştir. Ortalama 1,5–3 kamera varsayımıyla yayımlanmış olumlu başvuruların kapsadığı sistemler için yaklaşık 450–900 kamera birimi düşünülebilir. Bu resmi ithalat verisi değil, karar satırlarından üretilmiş ihtiyatlı bir senaryodur. KGY iznine ihtiyaç duymayan özel alan sistemleri arşivde görünmeyebileceği için gerçek toplam daha yüksek olabilir.

Karar arşivi bütün KKTC kameralarının envanteri değildir. Gerçek ölçek için gümrük verileri, kamu alımları, kurum envanterleri ve saha denetimleri karşılaştırılmalıdır.

Somut çözüm adımları

İlk olarak, kamera bazlı standart karar şablonu oluşturulmalıdır.

Şablonda kamera kimliği, görüş alanı, kamuya açık alan değerlendirmesi, maskeleyme, canlı izleme, analitik işlevler, veri sorumlusu, saklama süresi, sonuç ve itiraz yolu bulunmalıdır.

İkinci olarak, üç sonuç kategorisi ayrılmalıdır: onay, yalnızca belirtilen teknik ayarlar için; ret, eksik şartı ve düzeltme imkânını gösteren; KGY Kurulunun görev alanı dışında, başka mevzuat bakımından serbest kullanım anlamına gelmediğini ve varsa başvuru makamını açıklayan karar olmalıdır.

Üçüncü olarak, sistem kurma izni ile veri sahibi hakları için ayrı başvuru kanalları kurulmalıdır. Kamera kurmak isteyen kişi, görüntüsüne erişmek isteyen kişi, polis hakkında şikayette bulunan kişi ve suç ihbarı yapan kişi aynı prosedüre yönlendirilmemelidir. Elektronik başvuru, takip numarası ve eksik belge bildirimi sağlanmalıdır.

Dördüncü olarak mevcut kameralar için tekil kimlik, konum, veri sorumlusu, görüş alanı ve saklama süresini içeren envanter oluşturulmalıdır. Büyük ölçekli veya analitik sistemler için DPIA ya da eşdeğer risk değerlendirmesi zorunlu hale getirilmelidir.

Son olarak, teknik mahremiyet ve delil protokolü yayımlanmalıdır. Ses varsayılan olarak kapalı tutulmalı; özel alanlar kaynaktan maskelenmeli; erişim, kopyalama ve dışa aktarma işlemleri kaydedilmeli; zaman damgası ve bütünlük doğrulaması kullanılmalı; süresi dolan kayıtların silinmesi denetlenmelidir. Her yıl başvuru, onay, ret, kapsam dışı karar, itiraz ve kaldırma sayılarını içeren anonim şeffaflık raporu yayımlanmalıdır.

Sonuç

KKTC’de sorun yalnızca kameraların varlığı değildir. Sorun, kamera izin kararının özel hayat, kişisel veri ve idari denetim bakımından ne anlama geldiğinin açık biçimde anlatılmamasıdır. “Kurul yetkisinde değildir” ifadesi, KGY Kurulunun kamusal alan görmeyen kameralar üzerindeki yetkisinin doğmadığını anlatabilir; fakat başka hukuki yükümlülükleri ve başvuru yollarını da açıklamalıdır.

Güvenlik amacı meşrudur, ancak her kamera açısını veya veri kullanımını otomatik olarak haklılaştırmaz. Sürdürülebilir çözüm; ön izin, kamera bazlı gerekçe, veri koruma etki değerlendirmesi, canlı görüntüde mahremiyet, erişim günlüğü, açık başvuru

kanalları, bağımsız denetim ve yıllık şeffaflık raporlarının birlikte uygulanmasıdır.

KGY Kurulu ve beraberindeki avukat, üyeler, polis mensupları ve bağımsız katılımcılar ile daha önce izinlendirilmiş sistemler sıralı veya gelişigüzel şekilde ziyaret edilerek sistemlerin bütünlüğü ve izinlendirme sonrasındaki durumu kontrol edilmelidir.

Kayıtsız ve izinsiz kurullu kayıt sistemleri için vatandaş polise bildirim veya KGY Kuruluna gizli olarak bildirimde bulunabilmesi amaçlı kanallar açılmalıdır.

Kazım Ateş

Elektronik ve Bilişim Uzmanı

IT Projelerinin Başarılı Olabilmesi Nelere Bağlıdır?

IT projelerinin hedeflenen bütçe, zaman ve kalite standartları dahilinde tamamlanabilmesi, yalnızca doğru teknolojilerin seçilmesine değil, disiplinli yönetim ve çalışma prensiplerine bağlıdır.

Teknoloji projelerindeki karmaşıklık, belirsizlik ve hızlı değişim oranları göz önüne alındığında, ekiplerin benimsemesi gereken temel prensipler vardır.

Açık ve Ölçülebilir Hedef Tanımı (Scope & Alignment)

Projenin başarısızlık nedenlerinin başında belirsiz kapsama sahip gereksinimler gelir. Proje başlamadan önce "Başarı nedir?" sorusunun yanıtı somut metriklerle (KPI- Key Performance Indicator) tanımlanmalıdır. İş birimi ile teknik ekibin aynı dili konuşması, aynı seviyede bilgi ve sadakata sahip olması, beklenti karmaşasını önler.

IT projelerinde başarısızlığın ve bütçe/zaman sapmalarının en yaygın nedeni, projenin başında neyin, neden ve nasıl yapılacağını netleştirilmemesidir.

Açık ve Ölçülebilir Hedef Tanımı (Scope & Alignment), projenin pusulasıdır; teknik ekip ile iş birimi (iş paydaşları) arasında ortak bir vizyon ve anlaşma zemini oluşturur.

Kapsam Yönetimi (Scope Management) ve Kapsam Kayması (Scope Creep)

Net Sınırların Çizilmesi: Kapsam, projede nelerin yapılacağını belirttiği kadar, **nelerin yapılmayacağını (Out of Scope)** da açıkça tanımlanmalıdır.

Scope Creep Engelleme: Proje ilerlerken kontrolsüzce eklenen "küçük" istekler, birikerek projenin teslim tarihini ve bütçesini patlatır. Net bir kapsam tanımı, değişiklik isteklerinin (Change Request) resmi bir değerlendirme sürecinden geçmesini zorunlu kılar. Ekler, tanımlanan sonuca ulaştıktan sonra üzerinde çalışılacak noktalar.

Gereksinimlerin Detaylandırılması:

Kullanıcı senaryoları (User Stories) ve kabul kriterleri (Acceptance Criteria), hedeflenen sisteme geçilirken, kullanıcılarla birlikte planlanması gerekir.

İş ve Teknik Hizalanması (Alignment)

Ortak Dil Oluşturma: İş birimi iş ihtiyaçlarına (ciro, verimlilik, müşteri memnuniyeti), teknik ekip ise mimari ve altyapıya odaklanır. Alignment, bu iki dünyanın aynı dili konuşmasını sağlar. Teknik ekibin geliştirdiği her modül, doğrudan iş biriminin bir hedefine hizmet etmelidir.

Beklenti Yönetimi: Paydaşların teslim edilecek ürünle ilgili algısıyla teknik ekibin taahhüt ettiği ürünün %100 örtüşmesi gerekir. Görsel mock-up'lar, prototipler ve erken sunumlar bu uyumu sağlar. Beklentinin karşılanması, IT grubunun, minimal sorumluluğudur. Projeler, en az mevcut sistemin devamını sağlamaktan sorumlu ancak, gelişimini devam ettirerek mükemmeli yakalayabilmek için, gelecekte uyarlanacak ek görevler, güvenilirliğin devamı ve kullanıcılar için kolaylığı sürekli olarak devam ettirecek bir altyapı üzerine kurulması gerekir.

Risk ve Hata Yönetimi

Risklerin Erken Açığa Çıkması: Mimarideki teknik aksaklıklar, entegrasyon problemleri veya performans darboğazları projenin sonundaki "canlıya alma" aşamasında değil, ilk iterasyonlarda fark edilir.

Hata Maliyetinin Düşmesi: Erken tespit edilen bir mimari hatayı düzeltmek, aylar sonra tamamlanmış devasa bir kod tabanında düzeltmekten katbekat daha kolay ve ucuzdur.

Sürekli Teslimat ve İyileştirme (Continuous Delivery)

Otomasyon Odaklılık: Çevikliği sürdürülebilir kılmak için teknik altyapının buna uygun olması gerekir. CI/CD (Sürekli Entegrasyon / Sürekli Yayınlaştırma) süreçleri ve otomatize testler sayesinde yeni kod parçaları güvenle ve hızla canlı ortama aktarılır.

Sürdürülebilir Tempo: İlerlemenin ve başarılı projelerin sonuca ulaşmasının bir anahtarı da uzun süreli, stresi yüksek "son dakika canlıya geçiş" maratonları yerine, düzenli ve kurallı testler ile hedefe ulaşmaktır.

Çeviklik bir yöntemden ziyade bir **zihniyet dönüşümüdür (mindset)**. Amaç, kusursuz bir planı milimetrik takip etmek değil, değişen koşullara en hızlı ve en az maliyetle

uyum sağlayarak kesintisiz değer üretmektir.

Sağlam Mimari ve Teknik Mükemmellik (Technical Excellence)

IT projelerinde teslimat hızına ve görsel arayüze odaklanırken göz ardı edilen en kritik unsur arkadaki teknik altyapıdır. **Sağlam Mimari ve Teknik Mükemmellik (Technical Excellence)**; bir yazılımın sadece bugün çalışmasını değil, gelecekte de esnek, güvenli, performanslı ve bakımı kolay bir şekilde ayakta kalmasını sağlayan mühendislik prensiplerinin bütünüdür.

Ağaç örneğiyle açıklamak gerekirse; arayüz ve fonksiyonlar ürünün görünen yaprakları ise, mimari ve teknik mükemmellik toprağın altındaki kök sistemidir. Kökleri zayıf bir sistem, ilk büyük yük artışında veya kapsam genişlemesinde çökmeye mahkûmdur.

Sürdürülebilir Mimari Tasarım

Modülerlik ve Gevşek Bağlılık (Loose Coupling): Sistem parçalarının (servisler, modüller, bileşenler) birbirine sıkı sıkıya bağımlı olmaması gerekir. Bir modülde yapılan değişiklik veya oluşan hata, diğer modülleri çöktürmemelidir.

Ölçeklenebilirlik (Scalability): Mimari, artan kullanıcı sayısını, veri hacmini ve işlem yükünü kaldırabilecek şekilde kurgulanmalıdır. Hem dikey (hardware artırımı) hem de yatay (sunucu/instance artırımı) ölçeklenmeye uygun olmalıdır.

Bakımı Kolaylık (Maintainability): Kod tabanı; temiz, okunabilir ve kendi kendini açıklayabilir olmalıdır (Clean Code). Projeye yeni katılan bir yazılımcı, sistemi kolayca kavrayabilmelidir.

Kalite Güvencesi ve Otomasyon (CI/CD)

Test Otomasyonu: Manuel test süreçleri yavaştır ve insani hatalara açıktır. Birim testleri (Unit Test), entegrasyon testleri (Integration Test) ve uçtan uca testler (E2E) süreçlerin merkezine konmalıdır.

Sürekli Entegrasyon ve Dağıtım (CI/CD): Kod değişikliklerinin otomatik testlerden geçerek güvenle canlıya alınmasını sağlayan boru hatları (pipelines) kurulmalıdır. Bu, insan müdahalesinden



kaynaklanan dağıtım (deployment) hatalarını engeller.

Güvenlik ve Dayanıklılık (Security & Resilience)

Tasarım Gereği Güvenlik (Security by Design): Güvenlik önlemleri proje bittikten sonra eklenen bir yama değil, mimarinin ilk satırından itibaren uygulanan bir prensip olmalıdır (Yetkilendirme, veri şifreleme, OWASP standartları).

Hata Toleransı (Fault Tolerance): Üçüncü parti bir servis çöktüğünde veya veritabanı yavaşladığında, tüm sistemin kilitlenmesini önleyecek mekanizmalar (Circuit Breaker, Fallback yapıları) mimariye dahil edilmelidir.

Standartlar ve Mühendislik Disiplini

Kodlama Standartları: Ekipteki herkesin aynı stil kılavuzunu (Style Guide) takip etmesi, kod inceleme (Code Review) süreçlerinin aksatılmadan yürütülmesi esastır.

Dokümantasyon: Kodun ne yaptığı kadar, mimari kararların **neden** alındığını gösteren dokümantasyon (Örn: ADR - Architecture Decision Records) tutulmalıdır.

Özetle; teknik mükemmellik projeyi yavaşlatan bir lüks değil, tam aksine projenin uzun vadede **hızlı, güvenli ve kesintisiz** bir şekilde büyümesini sağlayan en temel yatırımdır.

Şeffaf İletişim ve Paydaş Yönetimi (Stakeholder Management)

IT projeleri sadece yazılımcıların değil, iş analistleri, tasarımcılar, yöneticiler ve son kullanıcıların ortak ortaklığıdır. İlerlemenin, karşılaşılan blokajların ve risklerin açıkça paylaşıldığı şeffaf bir iletişim kültürü; kriz anlarında hızlı aksiyon alınmasını sağlar.

IT projelerinde en gelişmiş teknolojileri kullanmak veya en kaliteli kodu yazmak, projenin başarılı kabul edilmesi için tek başına yeterli değildir. Bir projenin kaderini çoğu zaman teknik bileşenler kadar **insan faktörü ve ilişki yönetimi** belirler.

Şeffaf İletişim ve Paydaş Yönetimi (Stakeholder Management), projedeki tüm tarafların (iş birimi, yöneticiler, teknik ekip, tedarikçiler ve son kullanıcılar) aynı vizyon etrafında kenetlenmesini, beklentilerin doğru yönetilmesini ve krizlerin büyümeden çözülmesini sağlayan köprüdür.

Paydaş Analizi ve Haritalandırma (Stakeholder Mapping)

Her paydaşın projeden beklentisi, projeye

etkisi ve ilgisi aynı değildir. Başarılı bir yönetim için ilk adım paydaşları doğru analiz etmektir:

Etki ve İlgili Matrisi: Paydaşlar "Etki" (güç) ve "İlgili" seviyelerine göre gruplandırılır.

Yüksek Etki / Yüksek İlgili (Kilit Oyuncular): Sürekli yakın iletişimde olunmalı ve kararlara dahil edilmelidir (Örn: Proje Sponsoru, İş Birimi Liderleri).

Yüksek Etki / Düşük İlgili: Memnun tutulmalı, üst düzey özet bilgilendirmeler yapılmalıdır (Örn: Üst Yönetim, Uyum/Uyum Departmanları).

Düşük Etki / Yüksek İlgili: Düzenli bilgilendirilmeli ve görüşleri alınmalıdır (Örn: Son Kullanıcılar, Operasyon Ekibi).

Düşük Etki / Düşük İlgili: Minimum çabayla izlenmeli ve genel duyurulara dahil edilmelidir.

Şeffaflık Radikal Bir Prensiptir (Radical Transparency)

Şeffaflık, sadece işler iyi giderken rapor sunmak değil, **riskleri ve aksaklıkları erken aşamada masaya yatırabilmektir.**

Kötü Haberi Erken Vermek: Bir gecikme veya teknik engel ortaya çıktığında bunu saklamak veya "hallederiz" diyerek ertelemek, kriz anında telefisi imkansız güven kayıplarına yol açar. Problemi erken paylaşmak, çözüme paydaşları da ortak eder.

Geçerli Durum Raporlaması: İlerleme raporları "pembe tablolar" çizmek yerine gerçek durumu yansıtmalıdır. Kullanılan panolar (Jira, Trello vb.) ve ilerleme metrikleri tüm paydaşların erişimine açık olmalıdır.

Beklenti Yönetimi (Managing Expectations)

Gereksinimler ile imkanlar (zaman, bütçe, teknoloji) arasındaki en büyük çatışma beklenti uyumsuzluğundan doğar.

"Hayır" Diyebilmek ve Alternatif Sunmak: İş biriminden gelen her talebe doğrudan "evet" demek, kapsamın patlamasına (Scope Creep) neden olur. Şeffaf iletişim, bir talebin neden yapılamayacağını veya yapılması durumunda nelerin ertelenmesi gerektiğini (Maliyet-Zaman-Kapsam üçgeni üzerinden) somut veriyle açıklamaktır.

Prototip ve Demo'lar: Uzun metinler içeren dokümanlar yerine, çalışan ara sürümleri (Sprint Demo) paydaşlara göstermek beklenti kaymalarını anında tespit etmeyi sağlar.

İletişim Kanallarının ve Ritminin Standartlaştırılması

Kimle, ne zaman, hangi kanaldan ve hangi derinlikte iletişim kurulacağı net kurallara bağlanmalıdır:

İletişim Planı: Üst yönetime haftalık/aylık özet KPI raporları sunulurken; operasyonel ekiple günlük veya sprint bazlı detaylı toplantılar (Daily, Sprint Review) yapılmalıdır.

Gürültüyü Azaltmak: Çok fazla toplantı ve ilgisiz e-posta trafiği iletişimi güçlendirmez, aksine verimsizlik yaratır. Doğru bilgiyi, doğru kişiye, doğru kanaldan iletmek esastır.

Empati ve Hizalanma (Alignment)

İş Dilini Konuşmak: Teknik ekibin kullandığı karmaşık mimari terimler (mikroservisler, teknik borç, CI/CD) iş paydaşları için anlamsız olabilir. İletişim kurulurken teknik detaylar yerine bu durumun **iş değerine, maliyete veya riske olan etkisi** anlatılmalıdır.

Ortak Sahiplenme: Proje bir "Biz (IT) ve Onlar (İş Birimi)" çatışmasına dönüşmemeli; başarının da başarısızlığın da ortak olduğu hissettirilmelidir.

Şeffaf iletişim ve güçlü paydaş yönetimi; projede oluşabilecek belirsizlik ve stresi azaltır, güven ortamı inşa eder ve zorlu kriz anlarında ekibin arkasında duracak güçlü bir destek mekanizması oluşturur.

Risk ve Kaynak Yönetimi (Risk Assessment)

Olası bağımlılıklar, üçüncü parti entegrasyon kısıtları veya altyapı riskleri önceden analiz edilmeli, alternatif B planları hazırlanmalıdır. Ekiplerin aşırı yüklenmesini önlemek ve sürdürülebilir bir çalışma temposu (sustainable pace) korumak da kritik bir insan kaynağı prensibidir.

IT projelerinde hedeflenen bütçe, zaman ve kaliteye ulaşmanın yolu sadece iyi planlama yapmaktan değil, öngörülemez engellerle karşılaşıldığında projenin savrulmasını önlemekten geçer. **Risk ve Kaynak Yönetimi (Risk Assessment & Resource Management),** olası tehditleri henüz gerçekleşmeden tespit edip önlem almayı ve eldeki insan, finans, teknoloji ile zaman kaynaklarını verimli kullanmayı hedefleyen stratejik bir disiplindir.

Risk Yönetimi (Risk Assessment & Management)

Risk, projenin hedeflerine ulaşmasını

olumsuz etkileyebilecek potansiyel olaylardır. Risk yönetimi pasif bir "kriz tepkisi" değil, aktif bir "önlem alma" sürecidir ve 4 temel adımdan oluşur:

A. Risklerin Tespiti (Risk Identification)

Proje başlamadan önce ve proje boyunca olası riskler listelenir. IT projelerindeki yaygın risk kategorileri şunlardır:

Teknik Riskler: Yeni veya olgunlaşmamış teknoloji kullanımı, üçüncü parti sistem entegrasyon aksaklıkları, performans ve güvenlik açıkları.

Kapsam ve Gereksinim Riskleri: Belirsiz ihtiyaçlar, sürekli değişen talepler (Scope Creep).

İnsan Kaynağı Riskleri: Kilit personelin projeden ayrılması (Key Person Dependency), yetkinlik eksikliği.

Dışsal / Organizasyonel Riskler: Tedarikçi gecikmeleri, mevzuat değişiklikleri, bütçe kısıtlamaları.

B. Risk Analizi ve Önceliklendirme (Risk Evaluation)

Her risk iki temel eksenle değerlendirilir:

- Olasılık (Probability):** Riskin gerçekleşme ihtimali nedir?
- Etki (Impact):** Riskin gerçekleşmesi durumunda projeye vereceği zarar ne kadar büyük olur?

Bu iki değer çarpılarak bir **Risk Skoru** elde edilir. Skoru yüksek olan kritik riskler birinci öncelik haline getirilir.

C. Risk Yanıt Stratejileri (Risk Response Strategies)

Tespit edilen riskler için şu 4 stratejiden biri seçilir:

Kaçınma (Avoid): Riski tamamen ortadan kaldıracak plan değişikliği yapmak (Örn: Güvenilmez bir kütüphane yerine rustünü ispatlamış bir kütüphane seçmek).

Azaltma (Mitigate): Riskin olasılığını veya etkisini düşürmek (Örn: Entegre olunacak harici servis için erken aşamada PoC/prototip yapmak).

Devretme (Transfer): Riski üçüncü bir tarafa aktarmak (Örn: Bulut altyapı sorumluluğunu ve SLA taahhüdünü AWS/Azure'a bırakmak veya sigorta yaptırmak).

Kabul Etme (Accept): Düşük etkili veya

kaçınılması çok maliyetli riskleri bilerek kabul etmek ve B planı hazırlamak.

D. İzleme (Monitoring)

Riskler statik değildir. Proje ilerledikçe mevcut risklerin durumu güncellenmeli ve düzenli toplantılarla (Risk Review) yeni beliren riskler **Risk Siciline (Risk Register)** eklenmelidir.

Kaynak Yönetimi (Resource Management)

IT projelerindeki en kritik kaynak **insan gücü** ve **zamandır**. Kaynakların yanlış dağıtımı, ekibin tükenmesine (burnout) veya projenin kilitlenmesine yol açar.

Sürdürülebilir Çalışma Temposu (Sustainable Pace)

Kapasite Planlaması: Ekip üyelerinin %100 kapasiteyle çalıştırılması teorik olarak doğru görünse de pratikte felakettir. Beklenmedik hatalar, acil canlı destekleri ve toplantılar dikkate alınarak kapasite %70-80 bandında planlanmalıdır.

Aşırı Yüklenmeyi Önleme: Sürekli mesaiye dayalı çalışma modeli, kod kalitesini düşürür, hata oranını artırır ve kilit yeteneklerin kaybolmasına neden olur.

Bağımlılık ve Darboğaz Yönetimi (Dependency Management)

Kritik Yol (Critical Path): Birbirine bağımlı görevlerin dizilimi doğru analiz edilmelidir. Bir geliştiricinin işini bitirmesi için başka bir ekibin API teslimini beklemesi gibi durumlar (blocker) önceden tespit edilip takvimlendirilmelidir.

Single Point of Failure (SPOF): Projede sadece bir kişinin bildiği, bağımlı olunan kritik modüller veya görevler olmamalıdır. Bilgi paylaşımı (Pair Programming, Code Review) ile risk dağıtılmalıdır.

Finansal ve Altyapı Kaynakları

Risk ve kaynak yönetimi, projede yaşanabilecek sürprizleri en aza indirerek ekibe güvenli bir çalışma alanı sağlar. Belirsizliklerin yüksek olduğu IT dünyasında projenin zamanında ve bütçesinde bitmesini sağlayan ana emniyet supabıdır.

Süreç Odaklılık ve Sürekli İyileşme (Continuous Improvement)

Proje süresince yapılan düzenli geriye dönük incelemeler (retrospective) sayesinde nelerin iyi gittiği ve nelerin aksadığı analiz edilmelidir. Süreçleri ve çalışma alışkanlıklarını adaptif bir şekilde güncelleyen ekipler, proje ilerledikçe daha yüksek verimliliğe ulaşır.

IT projelerinde başarı yalnızca teslim edilen

son kod veya tamamlanan bir ürünle ölçülmez; o ürünü ortaya çıkaran **süreçlerin ve çalışma yöntemlerinin kalitesiyle** doğrudan ilgilidir. **Süreç Odaklılık ve Sürekli İyileşme (Continuous Improvement)**, projenin başından sonuna kadar yapılan işlerin, iletişim biçimlerinin ve mühendislik pratiklerinin düzenli olarak gözden geçirilip geliştirilmesini amaçlayan dinamik bir prensiptir.

Japon felsefesindeki **Kaizen** (sürekli daha iyiye gitme) yaklaşımına dayanan bu anlayış, projelerde statik bir çalışma biçimini değil, adapte olabilen ve sürekli öğrenen bir organizasyon yapısını savunur.

Süreç Odaklılık (Process Orientation)

"İyi süreçler, iyi sonuçlar doğurur." Süreç odaklılık, tesadüfi başarılarla veya bireysel kahramanlıklara güvenmek yerine; tekrarlanabilir, ölçülebilir ve sürdürülebilir çalışma standartları oluşturmayı hedefler.

Standartlaştırma: Kod inceleme (Code Review) adımları, test süreçleri, canlıya alma (Deployment) prosedürleri ve görev tanımları standartlaştırılır.

Ölçülebilirlik: Sürecin performansı somut verilerle izlenir. Örneğin:

Lead Time / Cycle Time: Bir görevin başlamasından tamamlanıp canlıya çıkmasına kadar geçen süre.

Hata Dönüş Oranı (Defect Rate): Test aşamasından veya canlıdan geri dönen hatalı işlerin oranı.

Dağıtım Sıklığı (Deployment Frequency): Canlıya ne kadar sıklıkla ve güvenle kod gönderilebildiği.

Sürekli İyileşme Döngüsü: (PDCA Cycle)

Sürekli iyileşme, rastgele değil sistemli bir döngü çerçevesinde yürütülür:

- Planla (Plan):** Nelerin iyileştirilebileceğini belirle ve hedef koy (Örn: Test sürelerini %30 kısaltmak).
- Uygula (Do):** İyileştirme adımını küçük bir ölçekte veya belirli bir sprintte uygula.
- Kontrol Et (Check):** Elde edilen verileri ve sonuçları eski durumla karşılaştır.
- Önlem Al / Uyarla (Act):** İyileştirme başarılı olduysa bunu yeni standart olarak benimse, başarısız olduysa yeni bir yaklaşım dene.

Geriye Dönük İnceleme: Retrospective (Retro)

Çevik (Agile) metodolojilerin kalbinde yer alan **Retrospective** toplantıları, sürekli

iyileşmenin en somut aracıdır. Her sprint veya faz sonunda ekip bir araya gelerek şu 3 temel soruya yanıt arar:

Neler İyi Gitti? *(Sürdürülmesi gereken başarılı pratikler)*

Neler Aksadı / Nerede Takıldık? *(Süreçteki darboğazlar, iletişim kopuklukları, teknik engeller)*

Neleri Farklı Yapabiliriz? *(Bir sonraki döngüde uygulanacak somut eylem planları)*

Bu toplantıların verimli geçmesi için **suçlayıcı olmayan (Blameless Culture)** bir ortamın sağlanması şarttır. Odak nokta "hatayı kimin yaptığı" değil, "sistem veya sürecin bu hataya nasıl izin verdiği" olmalıdır.

Öğrenen Organizasyon Kültürü (Learning Organization)

Hatalardan Ders Çıkarma (Post-Mortem):

Canlı ortamda ciddi bir kesinti veya hata yaşandığında, bu olay bir ceza nedeni değil, öğrenme fırsatı olarak görülür. Olaya neyin sebep olduğu kök neden analizi (Root Cause Analysis - 5 Why Yöntemi) ile incelenir ve benzer durumun tekrar etmemesi için süreç güncellenir.

Dönüşüme Açıklık: "Biz işi öteden beri böyle yapıyoruz" anlayışı terk edilir. Yeni araçlar, güncel yazılım mimarileri veya daha verimli proje yönetim teknikleri süreçlere kademeli olarak dahil edilir.

Özetle; süreç odaklılık ve sürekli iyileşme, IT ekiplerinin zamanla daha az eforla daha yüksek kaliteli iş üretmesini sağlar. Proje ilerledikçe ekibin olgunlaşmasına, stresi azaltmasına ve sürdürülebilir bir başarı grafiği yakalamasına olanak tanır.

Vasviye Tunaboylu
Database Specialist



**İnsan aklın sınırlarını zorlamadıkça
hiçbir şeye ulaşamaz.**
Albert Einstein

Tüm yazılar, yazarların kendi yorumlarıdır.
Yazıların tüm hakları, yazarların kendilerine aittir.