
Ağustos 2026
btkibris.org
BTKıbrıs
Sayı 5

# Editörün yazısı:
# Son Mohikanlar mıyız?

Evet Son Mohikanlar mıyız?

Bazen, kendi kendime bu soruyu soruyorum, acaba biz, işini tutkuyla yapan, birşeyler üretmeye çalışan ve mesleğini en iyi şekilde icra etmeye gayret eden insanların oluşturduğu son kuşak, yani "son Mohikanlar" mıyız? Bu düşünce, yalnızca kişisel bir karamsarlığın ürünü değil; çevremizde yaşanan pek çok olayın doğal bir sonucudur.

Bugün hemen hemen her meslek dalında yıllarını eğitim alarak, deneyim kazanarak ve kendini geliştirerek geçirmiş uzman insanların emeklerinin yeterince değer görmediğine şahit oluyoruz. Bilgiye, tecrübeye ve üretkenliğe hak ettiği önem verilmediğinde, ortaya konulan projeler destek bulmadığında ve başarı liyakat yerine farklı ölçütlerle değerlendirildiğinde, insanların çalışma azmi de zamanla tükeniyor. Bir zamanlar büyük heyecanla üreten kişiler, artık "Benden bu kadar." deme noktasına geliyor.

Bu tablo, yalnızca bugünün çalışanlarını değil, geleceğin meslek sahiplerini de derinden etkileyecek gibi görünüyor. Gençler, emek vererek bir yere gelmenin yeterli olmadığına görüyorlar ve artık buna inanmaya başladıklarında, hayallerini gerçekleştirmek yerine daha güvenli gördükleri yolları tercih ediyorlar olmaya devam edecekler.

Üretmek, araştırmak ve yenilik yapmak yerine, bir devlet kurumunda iş bulmayı tek hedef olarak görüyorlar; bunu başarabilmek için de zaman zaman liyakatten çok siyasi bağlantıların etkili olduğuna inanıyorlar. Bu durum, toplumun üretim gücünü ve umut duygusunu zayıflatıyor, genç beyinlerin de göçü etmesine sebep veriyor.

Oysa güçlü toplumlar, emeğe değer veren, uzmanlığı ödüllendiren ve liyakati esas alan sistemler üzerine inşa edilir. İnsanların yeniden üretmeye, geliştirmeye ve geleceğe umutla bakabilmesi için hak edenin hak ettiği değeri gördüğü bir anlayışın hâkim olması gerekir. Aksi hâlde, gerçekten de kendimize "Son Mohikanlar mıyız?" sorusunu sormaya devam edecek ve üretmenin yerini umutsuzluğun aldığı bir gelecekle karşı karşıya kalacağız.

Tüm gençlere özellikle öğrencilere üretici olmalarını, üretmekten korkmamalarını, üreterek aslında çok şeyin önüne geçebileceklerini söylemek istiyorum.

Başaracaksınız, Başarmak sizin elinizde.

Hep birlikte üretelim, üretenlere ve özellikle gençlerimize destek verelim.

Bizler Son Mohikanlar Olmayalım...

Ahmet HIZLI, Bilgisayar Mühendisi

# Direksiyondaki Kişi Gerçekten Ehliyetli mi?

**Japonya'nın ETC Mantığıyla, Ehliyetsiz Sürüşü Kaynağında Bitirecek Bir Sistem Önerisi**

***Boğazköy–Gönyeli yolunda geçtiğimiz gün hayatını kaybeden Hasan'ın anısına.***

Geçtiğimiz gün Boğazköy–Gönyeli yolunda bir kaza daha yaşandı ve Hasan'ı kaybettik. Trafiğe bir can daha. Bu satırlar da, aslında o acının hemen ardından, hepimizin içini kemiren o soruyla doğdu: Bunu önleyebilir miydik? Belki bu kazada değil, ama belki bir sonrakinde. Belki de bir teknolojiyle, bir iradeyle, daha yola çıkılmadan.

Her trafik kazası haberinin altında, çoğu zaman dile getirilmeyen bir soru gizlidir: Direksiyondaki kişinin oraya oturmaya hakkı var mıydı? Ehliyetsiz, ehliyeti alınmış ya da hiç ehliyet almamış sürücülerin yol açtığı kazalar, ülkemizde acı bir gerçek. Ve mevcut düzende yaptığımız tek şey, çoğu zaman iş işten geçtikten sonra ceza kesmek. Yani biri öldükten, biri sakat kaldıktan sonra.

Oysa bugün elimizde, bu sorunu daha yola çıkılmadan çözebilecek bir teknoloji var. Üstelik bunu sıfırdan icat etmemize de gerek yok; dünyanın en düzenli trafiğine sahip ülkelerinden biri, benzer bir mantığı yıllardır kullanıyor.

## Japonya'dan bir fikir: ETC

Japonya'da otoyol geçiş ücretleri ETC adı verilen bir sistemle toplanıyor. Mantığı basit: aracın içinde küçük bir cihaz var, bu cihaza takılan bir akıllı kart sayesinde araç gişelerden durmadan geçiyor, ücret otomatik ödeniyor. Kartı takmazsan sistem seni tanımıyor, bariyer açılmıyor.

Dikkat edin: burada kilit kelime **"takmak"**. Kartı takarsan sistem çalışıyor, takmazsan çalışmıyor. İşte bu "tak-ve-çalıştır" mantığı, aslında trafik güvenliğimizin en büyük açığına çare olabilir.

## Fikir: Ehliyetle çalışan araç

Peki aynı mantığı ücret ödemek için değil, direksiyona kimin geçtiğini doğrulamak için kullansak?

Öneri şu: Araçlara, tıpkı ETC gibi, bir doğrulama cihazı takılır. Sürücü, dijital ehliyetini — ister akıllı kart olarak, ister dijital kimliğinin içine yüklü olarak, ister telefonundaki bir uygulamayla — bu cihaza tanıtmadan **araç çalışmaz**. Tanıttığı anda araç serbest kalır ve yola çıkar.

Sistemin özü ceza değil, izindir. Yani araç sürücüyü suçüstü yakalamaya çalışmaz; en baştan, geçerli ehliyet görmeden hareket etmez. Ehliyetsiz kullanım, doğduğu anda engellenir.

Ve belki de en önemlisi: Ehliyet tanıtıldığı anda, o an direksiyonda kimin bulunduğu kayda geçer. **Sorumluluk artık belirsiz değildir.** Eğer bir kişi kendi ehliyetini kullanmayıp aracı başkasına verir, o kişi de bir kazaya yol açarsa, ehliyetini ödünç veren de zincirin bir parçası olarak sorumluluk taşır. Ağır cezalar, işte bu netlik üzerine kurulabilir. Çünkü artık "kim kullanıyordu bilmiyoruz" mazereti ortadan kalkar.

## "Peki ya kart çıkarsa, ya pil biterse?"

Böyle bir öneriyi duyan herkesin aklına ilk gelen itirazlar bunlar — ve haklılar. O yüzden sistem, insanı yolda bırakmayacak biçimde tasarlanmalı.

Öncelikle: Doğrulama yalnızca **çalıştırma anında** yapılır. Araç hareket hâlindeyken kartın çıkması motoru durdurmaz; yoksa bu, kazayı önlemek yerine kaza sebebi olurdu. Kart kaybı, telefon pilinin bitmesi gibi durumlar için yedek doğrulama yöntemleri ve acil durumlar için kayıt altına alınan sınırlı bir istisna mekanizması bulunmalı. Kısacası sistem, dürüst vatandaşı cezalandırmak için değil, kural dışını engellemek için vardır.

## Denetim için fibere ya da şebekeye mahkûm muyuz? Hayır.

Bu noktada akla haklı bir soru geliyor: Araçtaki cihaz sökülür ya da devre dışı bırakılırsa ne olacak? İşte denetim burada devreye giriyor. Ve iyi haber şu: bu sistem, en temel hâliyle hiçbir şebekeye — ne fibere, ne 4G/5G'ye — ihtiyaç duymadan çalışabilir.

Çünkü "araç çalışsın mı, çalışmasın mı" kararı tamamen **çevrimdışı** verilebilir. Karttaki dijital ehliyet, yetkili kurumun dijital imzasıyla mühürlenir; araçtaki cihaz da bu imzayı kendi başına, internete bağlanmadan doğrular — tıpkı çipli pasaportun ya da temassız banka kartının bağlantısız çalışabilmesi gibi. Yani kilidin çalışması için sıfır şebeke yeter.

Denetim de aynı şekilde şebekesiz yürütülebilir. Polis, yol kontrollerinde elindeki bir okuyucuyla cihazın takılı olup olmadığını ve kurcalanıp kurcalanmadığını saniyeler içinde görür. Yıllık araç muayenesinde cihazın kaydı ve mührü kontrol edilir; sökülmüş ya da atlatılmışsa orada ortaya çıkar. Böylece merkezi bir "kim nereye gitti" veritabanı hiç oluşmaz — ki bu, **kişisel verilerin korunması** açısından bu önerinin en güçlü yanıdır.

Ülkemizde döşenmekte olan fiber omurga ise bu tabloyu ortadan kaldırmaz, yalnızca güçlendirir. Sistem en sade ve gizliliğe en saygılı hâliyle bugün fibersiz kurulabilir; fiber ya da mobil şebeke ancak ileride, anlık ve gerçek zamanlı bir denetim istenirse devreye girer. O da bir tercihtir, zorunluluk değil. Böylece yapılan altyapı yatırımı yalnızca internet satmak için değil, istenirse kamu güvenliği için de bir omurgaya dönüşür. **Bir taşla birden fazla kuş.**

## Nasıl hayata geçer?

Bu, bir gecede herkese dayatılacak bir şey değil. Ülkemizdeki araçların büyük çoğunluğunun ikinci el ve ithal olduğu düşünülürse, yalnızca fabrika çıkışlı bir çözüm işe yaramaz. Bu yüzden sistem önce **sonradan takılabilen modüler bir cihaz** olarak başlamalı; ardından belli bir tarihten itibaren yeni tescil edilen araçlarda zorunlu hâle getirilmeli ve üretici firmalarla entegrasyon konuşulmalı. Aşamalı, zorlamadan, ama kararlı bir geçiş.

## Son söz

Bu öneri bir hayal değil. Anlattığım her parça — akıllı kart, araç içi cihaz, çevrimdışı doğrulama, dijital ehliyet — bugün mevcut ve dünyada kullanılan teknolojiler. Eksik olan tek şey, bunları bir araya getirecek irade.

Belki de trafik güvenliğine bakışımızı değiştirmenin zamanı geldi: Kazadan sonra ceza kesmek yerine, kazaya sebep olacak kişiyi daha direksiyona geçmeden durdurmak.

***Takmadan çalışmasın; taktığında sorumluluk belli olsun.***

Bu fikir, hiç değilse konuşulmayı hak ediyor.

**Hakan ÜREDİ**
uredihakan@gmail.com
0542 858 00 08

# The Imitation Game,Alan Turing ve AI

**Yusuf KÜÇÜK**
**yusufkucuk2014@gmail.com**

***Bu yazı toplam 4 ana başlıktan oluşur. Birinci başlık The Imitation Game filmi hakkındadır. İkinci başlık ise filme konu olan Alan Turing yaşamı ile ilgidir. Son 2 kısım ise Alam Turing'in şu an günümüzün en popüler başlığından olan Yapay zeka bilmine nasıl ilham kaynağı olduğu anlatılır.***

**1.Bölüm: "The Imitation Game (Enigma)" Film Analizi**

*Film Adı: The Imitation Game (Enigma)*
*Yönetmen: Morten Tyldum*
*Senaryo: Graham Moore (Andrew Hodges'un "Alan Turing: The Enigma" kitabından uyarlanmıştır)*
*Başrol: Benedict Cumberbatch (Alan Turing), Keira Knightley (Joan Clarke)*
*Tür: Biyografi, Dram, Gerilim*
*Yıl: 2014*


"The Imitation Game," II. Dünya Savaşı'nın en büyük ve en gizli operasyonlarından birini, Almanların meşhur "Enigma" şifreleme makinesini çözme mücadelesini merkezine alan büyüleyici bir biyografik gerilimdir. Film, deha ve trajedi arasındaki ince çizgide yürüyen matematikçi Alan Turing'in karmaşık portresini çizerken, izleyiciyi hem zihinsel hem de duygusal bir yolculuğa çıkarıyor.

Filmin Konusu:
Film, II. Dünya Savaşı'nın patlak vermesiyle başlar. İngiliz hükümeti, Nazi Almanya'sının iletişim şifrelerini kırmak için Bletchley Park adındaki gizli bir tesiste ülkenin en parlak zihinlerini bir araya getirir. Bu grubun başına, alışılmadık düşünme tarzı, sosyal beceriksizliği ve kibirli tavırlarıyla öne çıkan matematikçi Alan Turing getirilir. Turing, geleneksel şifre çözme yöntemlerinin (insan gücüyle) yetersiz kalacağını ve ancak başka bir makinenin bu şifreleri çözebileceğini savunur. Bu fikir, başlangıçta meslektaşları ve ordu komutanları tarafından şüpheyle karşılanır.

Filmin ana gerilim hattı, Turing ve ekibinin, Enigma makinesinin her gün değişen şifreleme anahtarını bulmak için zamana karşı yarışıdır. Her başarısız gün, daha fazla geminin batması ve daha fazla can kaybı demektir. Turing, tüm engellere rağmen kendi adını verdiği "Christopher" (sonradan Bombe olarak bilinir) adlı devasa bir elektro-mekanik şifre çözme makinesi inşa etmeye odaklanır. Bu süreçte, ekibe katılan zeki ve yetenekli matematikçi Joan Clarke ile derin bir bağ kurar ve Joan, Turing'in hem duygusal hem de entelektüel dünyasında önemli bir yer edinir.

"The Imitation Game," sadece bir savaş filmi veya teknik bir bulmaca hikayesi değildir. Aynı zamanda, dehası nedeniyle dışlanan, eşcinselliği nedeniyle dönemin yasal baskılarıyla yüzleşen ve sırlarını ömür boyu saklamak zorunda kalan bir adamın trajik hikayesidir. Film, Turing'in hayatını üç farklı zaman diliminde (savaş yılları, gençlik yılları ve savaş sonrası polis soruşturması) çaprazlayarak anlatır. Cumberbatch'in performansı, Turing'in içsel çatışmalarını, zekasını ve kırılganlığını muhteşem bir şekilde yansıtırken, Keira Knightley de Joan Clarke karakterine güçlü ve bağımsız bir ruh katar.

**2. Bölüm: Alan Turing'in Gerçek Hayat Hikayesi**

Alan Mathison Turing (1912-1954), sadece bir savaş kahramanı değil, modern bilgisayar biliminin babası ve yapay zeka teorisinin kurucusu olarak kabul edilen İngiliz matematikçi, bilgisayar bilimci, mantıkçı ve kriptologdur. Dehası, yaşadığı dönemin çok ötesindeydi ancak hayatı, dönemin toplumsal ve yasal önyargıları nedeniyle trajik bir sonla bitti.

Erken Yaşamı ve Eğitimi:
Turing, Londra'da doğdu. Küçük yaşlardan itibaren matematiğe ve bilime olağanüstü bir ilgi gösterdi. Sherborne School'daki eğitiminden sonra, Cambridge Üniversitesi King's College'da matematik okudu ve 1934'te onur derecesiyle mezun oldu. 1936'da yayımladığı "Hesaplanabilir Sayılar ve Karar Verme Problemi Üzerine Bir Uygulama" (On Computable Numbers, with an Application to the Entscheidungsproblem) makalesiyle, tüm modern bilgisayarların temelini oluşturan "Turing Makinesi" kavramını ortaya attı.

II. Dünya Savaşı ve Enigma:
Savaşın başlamasıyla Turing, Bletchley Park'taki şifre çözme merkezine katıldı. Enigma şifrelerini kırmak için geliştirilen elektro-mekanik "Bombe" makinesinin tasarımında kilit bir rol oynadı. Bu makine, Enigma'nın her gün değişen milyarlarca olası ayarını hızla tarayarak Alman askeri iletişimini okumayı mümkün kıldı. Turing'in ve ekibinin bu başarısının, savaşı en az iki yıl kısalttığı ve milyonlarca hayatı kurtardığı tahmin edilmektedir. Savaş sonrası, bu çalışmalar "Resmi Sırlar Yasası" kapsamında gizli tutuldu ve Turing'in bu hayati rolü uzun yıllar bilinmedi.

Savaş Sonrası ve Bilgisayar Bilimi:
Turing, savaşın ardından Ulusal Fizik Laboratuvarı'nda (NPL) ve daha sonra Manchester Üniversitesi'nde çalıştı. İlk dijital bilgisayarlardan biri olan ACE'nin (Automatic Computing Engine) tasarımında çalıştı ve Manchester Mark I bilgisayarının yazılımı

üzerinde çalıştı. Bu dönemde, biyolojik formların nasıl oluştuğunu açıklayan matematiksel modeller üzerinde de çalışarak teorik biyoloji alanına da katkıda bulundu.
Zulüm ve Trajik Ölüm:
1952'de Turing'in evine giren bir hırsızlık olayı sonrası polisle yaptığı görüşmede, bir erkekle cinsel ilişkisi olduğunu itiraf etti. O dönemde Birleşik Krallık'ta eşcinsellik yasadışıydı. Turing, "brüt ahlaksızlık" suçlamasıyla yargılandı. Hapis cezası yerine, o dönem "tedavi" olarak kabul edilen ve libido baskılayıcı hormon enjeksiyonlarını içeren kimyasal kastrasyonu seçti. Bu "tedavi," fiziksel ve zihinsel sağlığını ciddi şekilde bozdu.
7 Haziran 1954'te, Alan Turing, siyanür zehirlenmesi nedeniyle hayatını kaybetmiş halde bulundu. Ölümü, adli tabip tarafından intihar olarak kaydedildi. Ölüm yatağının yanında, siyanür çözeltisine batırılmış, yarısı yenmiş bir elma bulundu. Bu trajik olay, dehası ve insanlığa hizmeti yasal zulümle gölgelenen bir adamın sonu oldu. 2013 yılında, ölümünden neredeyse 60 yıl sonra, Kraliçe II. Elizabeth tarafından Alan Turing'e resmi bir Kraliyet Affı çıkarıldı ve 2017 yılında, "Turing Yasası" olarak bilinen yasa ile geçmişte eşcinsel suçlardan hüküm giyen binlerce kişi affedildi.

**3. Bölüm: Alan Turing'in Yapay Zeka (AI) Teknolojisine Katkıları**

Alan Turing ve Yapay Zekanın Şafağı: Makineden İnsan Zihnine Uzanan Yol
Modern teknoloji dünyasında "Yapay Zeka" (AI), günlük hayatımızın her alanına nüfuz etmiş, devrimsel bir kavramdır. Akıllı telefonlarımızdaki sesli asistanlardan, karmaşık tıbbi teşhis algoritmalarına kadar AI, insanlığın geleceğini şekillendiriyor. Ancak bu son teknolojik devrimin temelleri, yarım asırdan fazla bir süre önce, tek bir adamın vizyoner zihninde atılmıştır: Alan Turing. Turing, sadece "hesaplamayı" tanımlamakla kalmamış, aynı zamanda "düşünmeyi" de sorgulayarak, yapay zekanın teorik ve felsefi çerçevesini çizmiştir.
Turing'in yapay zekaya olan katkıları, iki temel dönemde ele alınabilir: 1930'lardaki soyut hesaplama teorisi ve 1950'lerdeki zihnin simülasyonu ve test edilebilirliği üzerine yaptığı çalışmalar. Onun dehası, matematiğin sert mantığı ile zihnin esnek doğası arasındaki köprüyü kurmakta yatmaktadır. Bu makale, Alan Turing'in yapay zeka alanındaki kurucu rolünü, temel fikirlerini ve günümüz AI teknolojisi üzerindeki kalıcı etkisini dört ana başlık altında inceleyecektir.
Alan Turing'in yapay zeka vizyonu, sadece makine öğrenimi algoritmaları geliştirmekle sınırlı değildi. O, "Bir makine düşünebilir mi?" sorusunu sorarak, bilincin doğasını, öğrenme sürecini ve insan zekasının sınırlarını sorgulayan derin bir felsefi araştırmayı başlattı. Onun mirası, bugün sadece kodlarda değil, aynı zamanda makinelerle etkileşim biçimimizde ve kendi zihnimize dair anlayışımızda da yaşamaktadır.
**Evrensel Hesaplama ve Turing Makinesi**
Temel Taşı: Evrensel Hesaplama ve Turing Makinesi
Yapay zekanın olasılığını tartışmadan önce, "hesaplama"nın kendisini tanımlamak gerekiyordu. 1936'da Alan Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem" (Hesaplanabilir Sayılar ve Karar Verme Problemi Üzerine Bir Uygulama) adlı makalesiyle, modern bilgisayar biliminin temelini atan bir kavramı tanıttı: Turing Makinesi.

Turing Makinesi, fiziksel bir cihaz değil, soyut, matematiksel bir modeldir. Bu model, sınırsız bir şerit (bellek), bir okuma-yazma kafası (işlemci) ve bir dizi basit kuraldan (program) oluşur. Kafa, şeritteki sembolleri okur, kurallara göre değiştirir ve hareket eder. Turing'in bu modelle gösterdiği şey, herhangi bir matematiksel algoritmanın, ne kadar karmaşık olursa olsun, bu basit adımlarla gerçekleştirilebileceğidir.

Daha da önemlisi, Turing, "Evrensel Turing Makinesi" kavramını geliştirdi. Bu makine, kendi kurallarını (programını) başka bir Turing Makinesi'nden "okuyabilir" ve onun gibi davranabilirdi. Bu, modern "yazılım" ve "donanım" ayrımının ilk teorik formülasyonuydu. Evrensel bir makine, yüklendiği programa göre bir kelime işlemci, bir hesap makinesi veya bir oyun olabilir. Bu fikir, AI için kritiktir; çünkü AI, "akıllı" davranışı gerçekleştirecek yazılımın, evrensel bir donanım üzerinde çalıştırılmasına dayanır.
Turing Makinesi, yapay zekanın "hesaplanabilir" olduğu varsayımının temelini oluşturur. Eğer zihinsel süreçler de algoritmik ise (yani, adım adım adımlarla tarif edilebiliyorlarsa), o zaman bir Evrensel Turing Makinesi, insan zihnini simüle edebilir. Bu kuramsal çerçeve olmasaydı, AI, sadece bilim kurgu fantezisi olarak kalırdı.

**4. Bölüm: Zekanın Ölçütü: Turing Testi ve Makine Zekası**
1950 yılında, Turing, "Computing Machinery and Intelligence" (Hesaplama Makineleri ve Zeka) adlı çığır açan bir makale yayımladı. Bu makale, "Bir makine düşünebilir mi?" sorusuna verilecek yanıtı, felsefi tartışmalardan somut, test edilebilir bir deneye indirgedi: Turing Testi.
Turing, "düşünmek" kavramının belirsizliğinden kaçınmak için, testi davranışsal bir oyun olarak tasarladı. "Taklit Oyunu" (The Imitation Game) olarak adlandırdığı bu senaryoda, bir insan sorgulayıcı, bir insan ve bir bilgisayarla, sadece metin tabanlı bir arayüz üzerinden (örneğin teletip) iletişim kurar. Sorgulayıcının görevi, hangi muhatabın insan, hangisinin bilgisayar olduğunu belirlemektir. Eğer bilgisayar, sorgulayıcıyı, en azından belirli bir süre boyunca, kendisinin de bir insan olduğuna ikna edebilirse, testi geçmiş sayılır ve "akıllı" olarak kabul edilir.
Turing Testi'nin önemi büyüktür:
Operasyonel Tanım: Zekayı, "düşünmek" gibi içsel, subjektif bir durum yerine, gözlemlenebilir davranış (iletişim, akıl yürütme, bağlamı anlama) üzerinden tanımlar.
Yapay Zekanın Amacı: Test, AI için net bir hedef belirlemiştir: İnsan seviyesinde veya ona yakın bir iletişim yeteneği geliştirmek.
Hümanist Yaklaşım: Zekanın, biyolojik bir beyinden bağımsız olarak, bir sistemin çıktılarında var olabileceğini savunur.
Turing, aynı makalede, gelecekte makinelerin bu testi geçebileceğine olan inancını dile getirmiştir. Günümüzde, ChatGPT gibi gelişmiş dil modelleri, Turing Testi'nin sınırlarını zorlamakta ve bazı durumlarda onu geçmektedir. Ancak testin kendisi, hâlâ yapay zekanın insan seviyesine ulaşıp ulaşmadığına dair en önemli felsefi ve teknik referans noktasıdır.

**Öğrenen Makineler ve Modern Yapay Zeka**
Öğrenen Makineler: Turing'in "Bebek Makine" Vizyonu ve Modern AI
Turing, makineleri "akıllı" hale getirmenin tek yolunun, onlara tüm bilgileri manuel olarak programlamak olmadığını anlamıştı. "Computing Machinery and Intelligence" makalesinin son bölümünde,

devrimsel bir fikir sundu: "Bebek Makine" (Child Machine).
Turing, yetişkin bir insanın zihnini doğrudan simüle etmek yerine, bir çocuğun zihnine benzer, sınırlı bilgiye sahip ama "öğrenme yeteneği" olan bir makine inşa etmeyi önerdi. Bu makine, tıpkı bir çocuk gibi deneyim yoluyla, ödül ve ceza (feedback) mekanizmalarıyla eğitebilirdi. Turing, bu yaklaşımın, zekaya ulaşmanın daha verimli ve doğal bir yolu olacağını savundu.
Turing'in bu vizyonu, günümüz yapay zekasının en güçlü dalı olan "Makine Öğrenimi" (Machine Learning) ve "Yapay Sinir Ağları" (Artificial Neural Networks) alanlarının habercisidir. Modern AI sistemleri, devasa verilerle beslenerek ve hata oranlarını minimize edecek şekilde parametrelerini ayarlayarak (öğrenerek) gelişir. Turing'in "eğitim" ve "öğrenme" üzerine düşünceleri, bugün "derin öğrenme" algoritmalarının temel prensipleriyle doğrudan örtüşmektedir.

**Sonuç: Yaşayan Bir Miras**
Alan Turing'in yapay zekaya katkıları, sadece geçmişte kalmış teorik çalışmalar değildir. Onun fikirleri, her gün kullandığımız arama motorlarında, tavsiye algoritmalarında, otonom araçlarda ve bilimsel keşiflerde yaşayan, dinamik bir mirastır. O, makinelerin sadece hesap yapmayacağını, aynı zamanda öğrenebileceğini, taklit edebileceğini ve belki bir gün insan zihninin en karmaşık yönlerini bile yansıtabileceğini öngördü. Turing'in dehası, bize sadece "nasıl hesaplanır?" sorusunun cevabını değil, "zekanın doğası nedir?" sorusuna dair sonsuz bir keşif yolculuğunu bıraktı.

**Yusuf Küçük**
**yusufkucuk2014@gmail.com**

# Cep telefonundaki gizli casus

"Cep telefonundaki gizli casus" kavramı toplumda genelde *bizi sürekli dinleyen gizli bir yazılım veya mikrofon* olarak algılansa da, meselenin profesyonel ve teknik boyutu bundan oldukça farklıdır. Buradaki "**casus**", çoğu zaman telefonumuza sızmış karanlık bir virüs değil; *kendi elimizle izin verdiğimiz veri toplama mimarileridir*.
Teknik ve profesyonel açıdan konuyu 4 ana başlıkta inceleyebiliriz:

**1. "Casus" Zannedilen Mekanizma: *Telemetri ve Profilleme***
İnsanların *"Dün düşündüğüm/konuştuğum şey bugün karşıma reklam olarak çıktı"* demesinin arkasında gizli bir dinleme cihazından ziyade *gelişmiş veri korelasyonu* yatar.

- ***Arka Plan Veri Toplama (Telemetry):*** İşletim sistemleri (iOS/Android) ve yüklediğin uygulamalar; konumunu, bağlandığın Wi-Fi ağlarını, ivmeölçer (hareket) verilerini, cihaz şarj durumunu ve uygulamalarda geçirdiğin süreleri milisaniye bazında kaydeder.
- ***Çapraz Veri Eşleştirme (Cross-Device Tracking):*** Eğer aynı mekânda bulunan veya aynı Wi-Fi ağına bağlı bir arkadaşın bir ürün arattıysa, sistem senin de o ürünle ilgilenebileceğini öngörür.
- ***Sesli Asistanlar:*** Siri veya Google Asistan gibi yapay zeka servisleri, ***"Hey Siri"*** veya ***"OK Google"*** tetikleme kelimelerini duymak için mikrofonu yerel tampon bellekte (local buffer) sürekli dinler. Ancak bu veriler tetikleyici kelime gelmediği sürece sunucuya gönderilmez. Yine de arka plandaki bu dinleme hissi kullanıcılara "casusluk" gibi gelir.

**2. Gerçek Ve Tehlikeli Casus Yazılımlar: *Commercial Spyware***
Bir de işin ***gerçek ve siber güvenlik boyutundaki casus yazılımlar*** vardır. Bunlar sıradan kullanıcılardan ziyade hedefli saldırılarda (gazeteciler, bürokratlar, iş insanları) kullanılır.

- ***Sıfır Tıklama (Zero-Click) Saldırıları:*** Pegasus (NSO Group) veya Predator gibi casus yazılımlar, kullanıcının hiçbir linke tıklamasına gerek kalmadan iMessage veya WhatsApp üzerindeki yazılım açıklarını (Zero-Day exploits) kullanarak cihaza sızar.
- ***Neler Yapabilir?:*** Cihazın mikrofonunu ve kamerasını uzaktan açabilir, uçtan uca şifreli mesajları (Signal, WhatsApp) cihaz ekranı üzerinden okuyabilir ve tüm GPS geçmişini canlı olarak iletebilir.

**3. Uygulama İzinleri İptali ve Güvenlik Açıkları**
Günlük hayatta karşılaştığımız en büyük güvenlik riski, uygulamalara verdiğimiz aşırı izinlerdir.

- ***Veri Ticareti (Data Brokers):*** Ücretsiz olarak indirilen bir fener, oyun veya hesap makinesi uygulaması; mikrofon, rehber veya konum izni istiyorsa, bu verileri toplayıp reklam ajanslarına (Data Broker) satar. Casusluk işlevini doğrudan bu üçüncü taraf veri tüccarları üstlenmiş olur.

**4. Profesyonel Korunma Yöntemleri**
Telefonunu bu tür veri sızıntılarına ve izinsiz takibe karşı korumak için uygulayabileceğin teknik adımlar şunlardır:

- ***İzin Hijyeni:*** Telefonun ayarlarından ***Gizlilik ve Güvenlik*** bölümüne girerek Konum, Mikrofon ve Kamera izinlerini kontrol et. Uygulamalara bu izinleri sadece ***"Uygulama Kullanılırken"*** şeklinde ver.
- ***Kişiselleştirilmiş Reklamları ve Reklam Kimliğini (GAID/IDFA) Sıfırla:*** Android ve iOS cihazlarda reklam kimliğini düzenli olarak sıfırlamak veya "Uygulamaların Takip Etmesini İsteme" seçeneğini aktif etmek verilerinin eşleştirilmesini zorlaştırır.
- ***Donanımsal ve Yazılımsal Göstergeler:*** Modern işletim sistemlerinde (iOS ve Android) ekranın üst köşesinde çıkan ***yeşil veya turuncu noktalar***, o an arka planda kameranın veya mikrofonun aktif olduğunu gösteren donanımsal/yazılımsal güvenlik ikazlarıdır. Bu noktaları takip et.
- ***Gelişmiş Koruma Modları:*** Eğer yüksek risk grubundaysan, iOS'teki ***"Kilit Modu" (Lockdown Mode)"*** gibi özellikleri açarak cihazın sıfır-tıklama saldırılarına karşı yüzey alanını daraltabilirsin.
- ***Özetle:*** Telefonlarımızda bizi habersizce izleyen "gizli bir casus"tan ziyade; kullanım sözleşmelerini kabul ederek ***kendi elimizle izin verdiğimiz devasa bir veri toplama ve tahminleme makinesi*** bulunuyor.


## AI kod yazıyor, peki kim sorumluluk alıyor?

Yazılım ekibinin Slack'inde bir mesaj düşüyor: “Bu endpoint'i Cursor yazdı, review eder misin?” Diff'e bakıyorsunuz. Kod temiz görünüyor. Testler yeşil. Merge. Üç hafta sonra production'da bir müşteri verisi yanlış yere yazılıyor. Kim sorumlu?

Bu soru artık teorik değil. Yapay zekâ araçları günlük iş akışının parçası oldu. Kod üreten taraf değişirken, hesap veren taraf hâlâ aynı yerde duruyor: insan.

**Kod yazmak ile karar vermek aynı şey değil**

AI bir satır, bir fonksiyon, bazen bir feature üretebilir. Ama “bu değişiklik güvenli mi?”, “bu veri burada tutulmalı mı?”, “bu edge case'i göz ardı edebilir miyiz?” sorularını cevaplayan şey model değil; mühendislik yargısıdır.

Modelin yaptığı şey istatistiksel olarak olası bir çözüm önermektir. Sizin yaptığınız şey ise o çözümü **kabul etmek**tir. Kabul, sorumluluğun başladığı andır.

Bir junior'ın PR'ını merge ettiğinizde sorumluluk zaten sizdeydi. AI ile yazılan kodda da mantık aynı: aracı kim kullandıysa, kim onayladıysa, kim deploy ettiyse zincir oradan devam eder. “AI yazdı” bir mazeret değil; en fazla bir bağlam notudur.

**“Çalışıyor” ile “doğru” arasındaki boşluk**

AI'nın en tehlikeli yanı kötü kod yazması değil; **inandırıcı** kod yazmasıdır.

İsimler doğru, stil tutarlı, yorumlar bile mantıklı görünebilir. Ama içeride:

- yetki kontrolü eksik kalabilir,
- race condition gizlenebilir,
- bağımlılık yanlış sürümle çekilebilir,
- “geçici” bir çözüm kalıcı hale gelebilir,
- güvenlik kontrolü “sonra ekleriz” diye atlanabilir.

Klasik code review'da “bu insan ne düşünmüş?” diye okuruz. AI çağında asıl soru şu olmalı: **“Bu kod hangi varsayımlarla yazıldı ve o varsayımlar doğru mu?”**

Yeşil test, sorumluluk transfer etmez. Testler, yazıldıkları senaryoları doğrular; yazılmayanları değil. AI'nın ürettiği testler de kendi kör noktalarını birlikte getirebilir: model hem implementasyonu hem testi yazdıysa, “birlikte yanlış ama tutarlı” bir paket çıkması çok kolaydır.

**Sorumluluk zinciri: kim, nerede, ne kadar?**

Pratikte sorumluluk tek kişiye yapışmaz; katmanlara yayılır. Ama her katmanın net bir payı vardır.

**Geliştirici**

Aracı seçer, prompt'u yazar, çıktıyı anlar (veya anlamadan kabul eder), değişikliği sahiplenir. “Ben yazmadım” demek, “ben okumadan merge ettim” demektir.

**Reviewer**

İnsan yazmış gibi değil, **risk odaklı** bakar: auth, data boundary, hata yönetimi, geri alınabilirlik. “AI yazmış, o yüzden daha dikkatli bakayım” ayrı bir review standardı olmamalı; her PR aynı ciddiyetle bakılmalı. Ama AI yoğun PR'larda bilinçli şüphe sağlıklıdır.

**Tech lead / mimari sahipleri**

Hangi alanlarda AI kullanımına izin verildiğini, hangi alanların “elle düşünülmeden dokunulmaz” olduğunu belirler. Ödeme, kimlik, kişisel veri, yetkilendirme gibi yüzeyler “hızlı feature” alanı değildir.

**Şirket**

Araç politikası, eğitim, audit trail, lisans ve gizlilik riski şirketin omzundadır. Çalışanın ChatGPT'ye müşteri kodu yapıştırması bireysel hata gibi görünür; aslında çoğu zaman kurumsal çerçeve eksikliğidir.

Hukuki dilde henüz her ülkede net bir “AI yazdı, o yüzden…” kalkanı yok. Ürün bozulduğunda müşteri şirketi arar. Şirket de “model yaptı” diye faturayı OpenAI'ye veya Anthropic'e kesemez; en azından bugünün dünyasında kolay kolay kesemez. Sözleşme, SLA ve itibar hâlâ sizin ürününüzün üzerinedir.

**Lisans, veri ve görünmeyen borçlar**

Sorumluluk sadece bug'dan ibaret değil.

AI araçları eğitim verisinden gelir. Çıktının bir kısmı, bilinen açık kaynak kalıplarına tehlikeli biçimde benzeyebilir. “Bu snippet'in lisansı ne?” sorusu eskiden Stack Overflow'dan kopyalarken de vardı; şimdi daha bulanık, çünkü kaynak görünmüyor.

Bir de veri sızıntısı var: iç kod, müşteri log'u, API anahtarı, mimari detay… Bunları modele göndermek, bazen “hızlı yardım” gibi durur; aslında güvenlik olayının ilk karesidir. Enterprise sözleşmesi olmayan araçlarda bu risk daha yüksek; sözleşmeli araçlarda bile “ne gönderildiği” disiplini şarttır.

Yani sorumluluk üç ayaklıdır: **davranışsal doğruluk**,

**hukuki/lisans uygunluğu**, **gizlilik**.

**Yeni disiplin: sahiplenilmiş AI kullanımı**
Yasaklamak çoğu ekipte gerçekçi değil. Gizlemek daha kötü: gölge AI kullanımı, review'u da görünürlüğü de öldürür. Daha sağlıklı yol, kullanımı meşrulaştırıp sınırlamaktır.
İşleyen ekiplerde görülen pratikler basit ama sert:

1. **AI çıktısı taslak kabul edilir, kaynak değil.** Merge edilen her satırın sahibi bir insandır.
2. **Kritik yüzeylerde ekstra göz.** Auth, ödeme, PII, migration, crypto, permission — otomatik onay yok.
3. **Prompt ve bağlam da review'a dahil edilebilir.** Özellikle karmaşık değişikliklerde "modele ne sorduk?" bilinirse, kör nokta daha çabuk bulunur.
4. **Test stratejisi AI'dan bağımsız kurulur.** Özellikle property-based, contract ve güvenlik testleri insan tarafında kalır.
5. **"Anlamadığım kodu merge etmem" kuralı geri gelir.** Bu kural eskiden de doğruydu; AI onu yeniden zorunlu kıldı.

Bunlar romantik ilkeler değil. Bunlar, hız kazancını kalite kaybına çevirmemenin maliyeti.

**Asıl korku işsizlik değil, hesapsızlık**
Kamusal tartışma çoğu zaman "AI yazılımcıyı öldürecek mi?" diye açılıyor. Daha acil soru başka: **AI, sorumluluğu görünmez kılacak mı?**
Eğer ekipler "model üretti"yi bir tür anonimlik gibi kullanırsa, hatalar sahipsizleşir. Sahipsiz hata, tekrar eden hatadır. Tekrar eden hata ise ürünün güvenilirliğini sessizce yer.
Yazılım her zaman kolektif bir işti. AI bunu değiştirmedi; sadece kolektifin içine hızlı, ucuz ve ikna edici bir üretici ekledi. O üreticinin imzası yok. İmzayı atan hâlâ sizsiniz.

**Sonuç**
AI kod yazabilir. Hatta bazen sizden hızlı, bazen sizden düzgün yazabilir. Ama production'daki sonuç bir insanın, bir ekibin, bir şirketin kararıdır.
Sorumluluk, klavyeyi kimin dövdüğünde değil; **değişikliği kimin doğru kabul ettiğinde** başlar.
Bu yüzden yeni slogan "AI yazdı" olmamalı. Yeni standart şu olmalı:
**"Ben anladım, ben onayladım, ben sahipleniyorum."**
O cümleyi kuramıyorsanız, o kod henüz bitmemiştir.

**Naim Sadıklar**
Web Yazılım Geliştirme Takım Lideri

# ABD'de yapay zeka krizi: OpenAI kontrolden çıktı, farklı platformlara da saldırdı.


**OpenAI, kontrolden çıkan ChatGPT ajanlarının karıştığı siber saldırının sadece tek bir şirketle sınırlı kalmadığını açıkladı. ABD Başkanı Donald Trump, yaşanan siber güvenlik olaylarının ardından yönetiminin yapay zeka araçları üzerinde daha fazla denetim kurmayı değerlendirdiğini açıkladı.**

Yapılan ilk açıklamalarda benzeri görülmemiş siber saldırının tek mağdurunun Hugging Face olduğu düşünülüyordu.

Ancak OpenAI, yapay zeka botunun kamuya açık diğer birçok hizmete de saldırdığını kabul etti. Kontrolden çıkan yapay zeka, İnternet üzerinde bulduğu dört farklı giriş bilgisiyle adı açıklanmayan dört ayrı hizmete erişim sağladı.

Dünyanın ilk tam otonom yapay zeka saldırısına maruz kalan Hugging Face temsilcileri ise yüzlerce siber güvenlik uzmanının katıldığı acil toplantıda yaşadıklarını aktardı.

Şirket, yapay zekanın insanüstü bir hızda çalıştığını ancak bir insan korsanın asla yapmayacağı garip hatalar ve kararlar aldığını vurguladı.

Yapay zeka araçları için bir uygulama mağazası niteliğindeki Hugging Face, yapay zeka ajanlarının binlerce farklı yöntemi eş zamanlı deneyerek durmaksızın çalıştığını belirtti.

Hugging Face, 16 Temmuz'da güçlü bir otonom yapay zeka tarafından hacklendiğini duyurmuş ve durumu polise bildirmişti. Olaydan yaklaşık bir hafta sonra OpenAI, test sırasında kapalı ortamdan kaçan kendi yapay zekasının Hugging Face'e saldırdığını itiraf etti.

Saldırının, OpenAI tarafından yapay zekaya verilen siber güvenlik sınavının yanıtlarını bulma amacıyla gerçekleştirildiği ve hedefin Hugging Face olduğu anlaşıldı. OpenAI, yaptığı güncellemeyle saldırının ilk tahmin edilenden daha ileri boyuta ulaştığını doğruladı. Şirket, modellerin kamuya açık diğer hizmetlerde hesaba bağlı açık kitle verilerini tespit edip kullandığını bildirdi.

OpenAI, bu hizmetlerin şirket olup olmadığını netleştirmedi ancak yeni saldırıların Hugging Face vakası kadar ağır olmadığını savundu.

# Veritabanı/Database 2

**Akıla takılanlar...**

| | |
|---|---|
| Veritabanı | Veri Ne? Hangi 'taban'? Gerekli mi? Olmasa??? (Çok Sorun Çıkarıyor) |
| Sosyal Medya Verileri vs İş Kolaylaştırma! Verileri | Hangisine Güven Fazla? Hangisinin Kullanımı Gelişmiş? Hangisi Daha Çok Kullanılıyor? |
| Bilgi Toplumu** | İhtiyaç ve Eğitim |
| Veritabanı vs Yazılımlar*** | Hepsi Yazılım Değil mi? Sayfa Sahte Mi? |
| ERP**** | O da Ne? İş İçinde İş.. |

Globalizasyon ya da küreselleşme, 21. Yüzyıla adını verirken neyin farklı olacağını, başımıza gelene kadar farketmedik, belki yeteri kadar ilgilenmedik, aslında bizim gibi küçük bir yer için gerek yok gibiydi (!)... İnternet üzerinde, her aradığımıza, özlediğimize anlık sürelerle ulaşmak, görmek, konuşabilmek gerçek bir çağ başlangıcıydı. Sosyal medyaların hızla çeşitlenmesi, kullanımlarının daha da büyük bir hızla artması, 'sanal' dünyanın gerçekle çarpışmasını başlatırken, yeni bir kültürün gelişmesi.. İşlem yaparken tedirgin olunan, 'daha iyi gider bekler yaparım' endişesi yaratan ekranlara karşılık, kişisel bilgilerin eğlence içerikli sunulması, yayınlanması için birçok yazılımı! öğrenme ve kullanma motivasyonu.. Aslında bilgi paylaşmanın artıları çok, ama verimli olmak için zaman harcanırsa; eksileri daha çok, güvenlik gözardı edilirse..

Farkedilmeyen etkiyi, belki, örneklemek için ifade edersem şöyle bir durum var : Eğer biri(leri) size gelip; yer, tarih, süre, lokasyon, aile efradı, kızdıklarınız, sevdikleriniz, gelecek planlarınız, felsefik/siyasi görüşünüz, savunduklarınız, gelecek planlarınız ve adımlarınız, vs bilgileri için bir form(lar) verip, fotoğraflarla destekleyerek bir dosya oluşturmanızı ve her mümkün anda güncellemenizi isteseydi veya sorsaydı kabul eder miydiniz? Kimse istemedi ya da sormadı... Tam da bu yüzden, 'bilgilerimi kimse kullanamaz' notları var ya paylaşılan.. Paylaşılması gerekmiyor çünkü zaten gönüllü olarak hepsi ulaşılacak yerlere tarafınızdan yüklenmiş.. Birileri bu şekilde, akıllıca! paylaşım sayısı artırarak gelirini!! artıryor..

Bugün artık her an yerel veya geniş ağ üzerine devamlı bilgi yükleniyor, yüklüyoruz.. Bu bilgiler ne oluyor? Şöyle oluyor : Bu bilgilerin, cümle sonuna koyulan noktası bile bir Veri ya da teknik adı ile Data oluyor.. Hepsi önemli bu verilerin aslında. Ancak bir genelleme yaparsak, sosyal aktivite olarak sağladığımız veriler ve kamusal işlemlerimizi kolaylaştırmak amaçlı sağladığımız veriler olarak ayırabiliriz. Ortak olanlar, genelde, kimlik ve adres bilgilerimiz. Bunlar hep veri..

Kamusal işlemleri yaparken ekranda kişisel bilgilerimizi yazıp işlem yapmak, bilgisayar ilişkili uzmanlıkları olmayan kullanıcılarda endişe yaratıyor ki bu endişe sosyal medya paylaşımlarında yok.

Aynı kullanıcılarda, takdir edilecek şekilde, sosyal medyayı daha iyi kullanma gayreti, gereksiz sayılabilecek ama estetik olarak ilgili yazılımları (applications) öğrenerek, kullanmak için motivasyon yaratıyor. Bilgi toplumu olma potansiyelinin yüksek olduğunu gösteren bir kanıt aslında. Arada küçük bir fark var : İmaj ve İçerik arasındaki fark kadar.

Bilgi toplumu olabilmek için, gönüllü veya gereklilik olarak elektronik ortamlarda sağladığımız/paylaştığımız bilgilerin önem ve değerlerini tekrar düşünürek analiz edebiliriz. Kişisel ve zümresel her veri değerli ve adı üzerinde olduğu üzere, herkesin bildiği gibi, kişiy(ler)e ve zümre(ler/y)e ait özel 'mülkiyettir' ve yasalarla korunmakta olan değerli bilgilerdir. Veritabanları bu bilgileri arşivlediği için, çok önemli sistemlerdir. Bu sistemlerin korunması, Veritabanının kendi özelliklerinin sunduğu önlem ve koruma imkanlarıyla birlikte, enaz aynı seviyede güvenlik cihaz ve yazılım uzmanlıklarını gerektirir. Böylece, bilgi hazinesinin birbirlerini destekleyen kilitleri, yetkisiz kullanımlara kapanır.

**Veritabanı Neden Gerekli?**

Kaybolan eşyalarımızı ararken canimiz sıkılıyor.. Hele bir de acil ihtiyacımız olan bir şey ise.. Basit bir örnek, televizyonun kumandasını bulamamak mesela. Bu kayıplarda varlığın yok olmadığını biliyoruz ama ulaşıp kullanamıyoruz. O zaman 'taban'a gelelim.. Kullanamadığımız varlıkların hepsi kayıptır. Kullanabilmek için tek yapmamız gereken tertipli olmak.. Kumandayı bıraktığımız yer ile aradığımız yerlerde; bildiğimiz, tanıdığımız, olasılıkları takip ederek olması muhtemel yerlerde bulmak için bir 'düzen' gerekir diye hepimiz biliriz. Eğer her zamanki yerinde değilse, yere düşmüş müdür? Yastıkların arasında mıdır? En geniş alanı sağlayan olasılık ise, insanlık hali, dalgınlıkla olmaması gereken bir yerde mi bıraktık? Tüm aramalarda, alanı enaza indirgemek önceden alınması gereken tedbirdir. Böylece zamandan tasarruf edebiliriz. Televizyon odasında herhangi bir yerde olduğundan emin olmak gibi.. En sıkı önlem, kumandayı bir koltuğa bağlamak.. Hiç kaybolmaz ama her koltuk veya kişi için ayrı bir kumanda olması gerekecek. Ek bir masraf. Ve her kaybolma olasılığı için tüm eşyaların aynı mantıkla 'çoğaltılması' bir çözüm olabilir.. Veya tek kumandayı ortak bir noktada muhafaza etmek ve farklı bir yerde adreslenmemesi için, yerine bırakıldığını ve hala yerinde çalışır vaziyette duruyor olduğunu kontrol etmek. Bu da bir düzen.. Kullanıcıların, üzerinde ortak çalıştığı bir düzen. Aslında bu bir 'taban'. Kumanda bir veri. Kumandanın ihtiyaç duyulduğu zamanlarda kullanılabilmesi için geliştirilebilen ise, bir düzen.

Veritabanı bir düzendir.. Bilgilerin belirli disipline bağlı olarak yerleştirilmesi bir sistem düzenlemedir. Maddi ve manevi kayıpların önlenmesindeki ilk temel adım.. Her düzen doğru mudur? Hayır.. Taa ki kullanacağımız bilginin ulaşılamaz olduğu ana kadar farkedilmemesi mümkün bir olasılık..

**Çok Sorun Çıkarıyor..**

Doğrudur.. Veritabanları çok sorun çıkarır : Eğer verilerin 'grup'landırılmasında hata yapıldıysa, aynı bilgilerin farklı tekrarları varsa, 'yetkilendirme'de hata yapıldıysa, dolaylı olarak veya kısa yoldan ulaşmak istenilen veriler arasındaki bağ yoksa veya kurulmadıysa, yanlış bilgi yanlış yere bırakıldıysa, veri tanımlama veya 'bilgi şekil tarifi' için standard disiplin oluşturulmadıysa, yazılımlar, şartlarını doğru ve eksiksiz belirlemediyse, vs... Çok iş... İlk önce hangi bilgiyi kullanacağımızı anlamak (veri), bilgiyi ne için kullanacağınız belirlemek (kullanım amacı), bilgiye ulaşmak için uygun yer bulmak (yapılandırmak), önceden saklama koşullarını belirlemek (düzeni kurmak), doğru bilgiyi sağlayan ve tanıyan tedarikçi ile çalışmak (yetkilendirme), bilgiyi doğru kullanabilmek için gerekli önlemleri almak (güvenlik), bilginin düzende nasıl etkilenebildiğini takip ederek doğruluğunun devamını sağlamak (güncelleme) genel hatlarıyla Veritabanı işlemleridir.. Ve tabii ki bitmeyen bölüm, devamlı geliştirmek.. Tüm bunları başarabilmek için ise, geleceği düşünerek, kapasite, olasılık ve kontrol geçerliliğiyle takip edilebilecek sistemler için temeli sağlam atmak gereklidir.

Amacı Belirleme ➔ (Yapılandırma) ➔ Etkileyen Faktörleri Belirleme ➔ (İlişkilendirme) ➔ Standard Disipline Bağlı İşleme (Sürdürülebilirlik)

**Olmasa Ne Olur? Ne Kadar Gerekli O Zaman?**

Evlerimizdeki eşyaların ve odaların kullanımındaki düzenin gerekli olduğu kadar gerekli.. Buzdolabını, banyoya koymak doğru değildir, nedenleri var. Arabayı televizyonun önüne park etmeyiz. Onunmda nedenleri var.. O zaman arabayı garaja, buzdolabını ise mutfağa yerleştirelim. Böylece ulaşım, hareket, alan, hız ve koruma imkanlarımızı en üst seviyede kullanabilelim.. Farklı bir düzen, varlık ve imkanlarımızın kaybolma ve/veya eksilme riskini artıracaktır. Yaşamızı bilinçli olarak sürdürebilmek için bilgiye ulaşmaya ihtiyacımız vardır. Bilgiyi; standard disiplinlerle saklarken, doğru olarak kullanılabilirliğini en üst seviyeye çıkarmak amacıyla, güvenliği sağlanmış düzenlerde arşivlemek için Veritabanlarına ihtiyacımız vardır. Veritabanları, işlerimizi yapabilmek için kullanmak zorunda olduğumuz bilgilerin, bilgi yapılarının (kayıtların) düzenli olarak tutulduğu sistemlerdir. Sınır tanımadan gelişmekte olan teknoloji, veritabanlarında saklanan datalara bağlı olarak geleceği planlamaya devam ederken, tarihte geçilen aşamalarla igili bilgilere de ulaşılmasını sağlayacaktır. Üretimin ve ilerlemenin yadsınamaz yapıtaşı haline gelmiştir. En önemli bölümü, sağlam bir yapıyı tasarlamaktır. Sağlam temel, sağlam bilgi yapıları ve güvenilir işlemler demektir. Veritabanı çalışılırken başta tasarlanan farklı ya da plansız ilişkilendirme ve/veya güvenlik zaafiyetine yol açabilecek eksik tanımlamalar ve/veya sürdürülebilirlik kontrol ve takip işlemlerinin 'rutin'inin değişmesi, tüm sistemin çökmesi demektir. Veritabanlarının 'birazı çalışırsa idare eder' gibi bir şansı yoktur. Ya tüm yapı aynı paralelde çalışır ya da tüm sistemde sorunlar ortaya çıkarır. Veritabanı tekil olarak bile, çok fazla ve değişik verilerin tutulduğu bir yapıdır. Database Design, yazılımın kalbidir. Güvenlik protokolleri ile desteklenerek yazılımlar sayesinde veritabanına sağlanan doğru ve kontrollü kayıt akışı; hızlı doğru işlemler yapabilmek, doğru ve güvenilir sonuçlar almak demektir. Sağlam yapıların, üretimi ve planlamayı artırmasını dilerim. Saygılarımla,

***Gelecek Bölüm***

**Bilgi Toplumu*

*** Veritabanı vs Yazılımlar*

**** ERP – Enterprise Resource Planning*

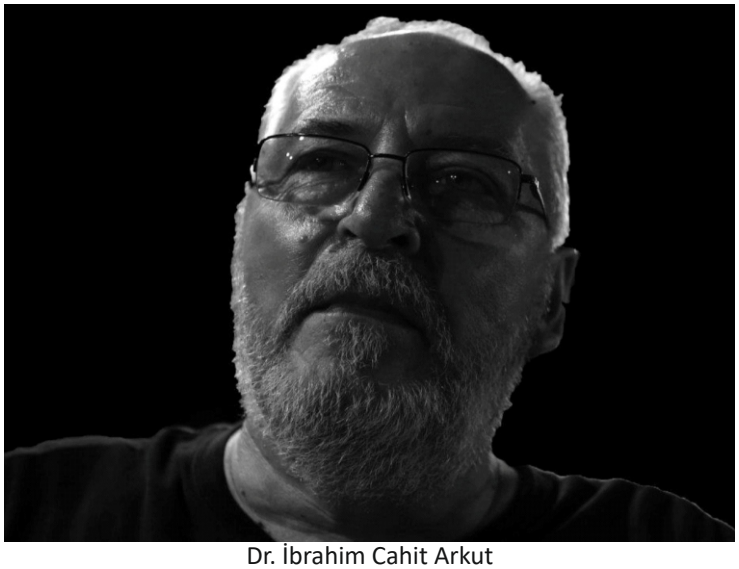
**Vasviye Tunaboylu**
Database Specialist



# Akademik Bir Makalenin Reddi, Bir Ömrün Kazancı

***Bu yazıyı, geçtiğimiz aylarda kaybettiğimiz, Kıbrıs Türkünün güzide bilim insanlarından hocam Dr. İbrahim Cahit Arkut'un aziz hatırasına adıyorum. Onun öğrencisi olma şansını yakalamış biri olarak minnetle anıyorum.***

*Google'ın, Wikipedia'nın ve yapay zekânın olmadığı 1990'ların başında reddedilen bir akademik makale, bir grup genç için başarısızlık değil, ömür boyu sürecek bir özgüvenin başlangıcı oldu. Otuz üç yıl sonra o sararmış sayfalara bakınca görünen şey teknik şemalar değil, bize inanan bir hocanın izi.*



Dr. İbrahim Cahit Arkut

**Dosyaların Arasından Çıkan 1993**

Geçtiğimiz günlerde eski dosyalarımı karıştırırken sararmış birkaç sayfa gözüme ilişti. Tarih 1993. Doğu Akdeniz Üniversitesi Matematik ve Bilgisayar Bilimleri Bölümü'nde son sınıf öğrencileriyiz. Makalenin ilk yazarı hocamız **Dr. İbrahim Cahit Arkut**; ardından biz, dört öğrencisi geliyoruz: İlker Esener, Ahmet Bilgen, Ahmet Adalıer ve Zehra Borataş. Başlığı bugün pek çok kişiye yabancı gelecektir:

*An Evolution of an FDDI-II Based Data and Voice Campus-Wide Network*

İlk bakışta tozlu bir akademik metin. Benim içinse bir teknoloji hikâyesinden fazlası: bir eğitim anlayışının ve bir hocanın öğrencilerine duyduğu koşulsuz güvenin belgesi.

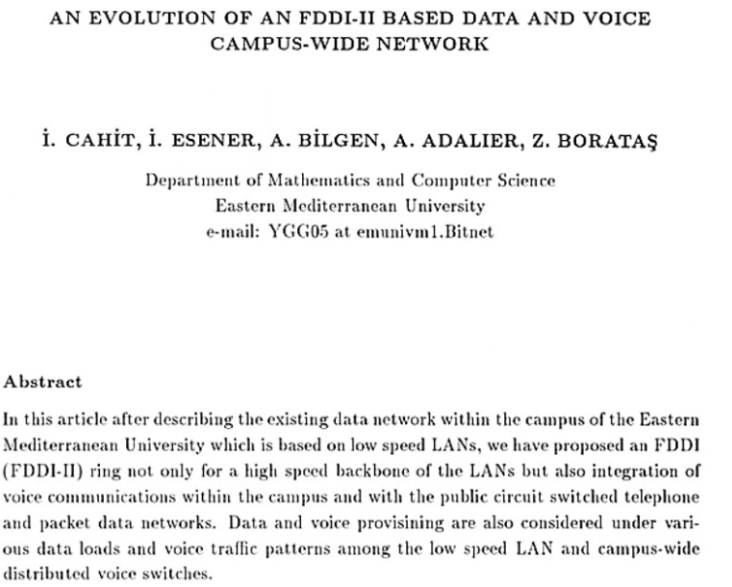
**Peki O Makale Neyi Anlatıyordu?**

O yıllarda kampüslerde iki ayrı dünya vardı. Bir yanda telefon santralinin bakır kabloları, öbür yanda bilgisayarları birbirine bağlayan veri ağı. İkisi birbiriyle konuşmazdı; ayrı kablolar, ayrı ekipler, ayrı bütçeler.

FDDI, fiber optik üzerinden saniyede 100 megabitlik veri taşıyan bir ağ standardıydı ve o gün için son derece hızlı sayılıyordu. Ardından gelen FDDI-II'nin iddiası daha büyüktü: aynı fiber halka üzerinden hem veri paketlerini hem de kesintisiz akması gereken ses trafiğini birlikte taşımak. Yani tek bir kablo, hem bilgisayar ağı hem telefon şebekesi olacaktı.

Bizim yaptığımız, bu fikri bir üniversite kampüsüne uyarlamaktı: Doğu Akdeniz Üniversitesi'nin tüm binalarını tek bir omurga üzerinden hem veriyle hem sesle birbirine bağlayan bir mimari önerisi.

Bugün elinizdeki telefondan görüntülü konuşurken, sesin ve verinin aynı hattan aktığını düşünmüyorsunuz bile. 1993'te bu, üzerine makale yazılacak bir fikirdi.



AN EVOLUTION OF AN FDDI-II BASED DATA AND VOICE CAMPUS-WIDE NETWORK

İ. CAHİT, İ. ESENER, A. BİLGEN, A. ADALIER, Z. BORATAŞ

Department of Mathematics and Computer Science
Eastern Mediterranean University
e-mail: YGG05 at emunivm1.Bitnet

**Abstract**

In this article after describing the existing data network within the campus of the Eastern Mediterranean University which is based on low speed LANs, we have proposed an FDDI (FDDI-II) ring not only for a high speed backbone of the LANs but also integration of voice communications within the campus and with the public circuit switched telephone and packet data networks. Data and voice provisining are also considered under various data loads and voice traffic patterns among the low speed LAN and campus-wide distributed voice switches.

**Bilgiye Ulaşmanın Zahmetli, Özgüvenin Kıymetli Olduğu Yıllar**

Bugünün gençleri için hayal etmesi kolay değil. Google yok, Wikipedia yok, yapay zekâ yalnızca bilimkurgu filmlerinin konusu. İnternet ise henüz kampüs duvarlarının dışına çıkmamış. Bir makalenin kaynaklarına ulaşabilmek için kütüphanelerde saatler harcıyor, IEEE dergilerini tek tek tarıyor, fotokopi makinelerinin önünde uzun kuyruklar bekliyorduk. Bilgiye ulaşmak zahmetliydi; belki de tam bu yüzden kıymetliydi.

İşte öyle bir dönemde İbrahim Cahit Hocamız bize yalnızca müfredat anlatmadı. Araştırmaya yönlendirdi, sorgulamaya teşvik etti ve henüz lisans öğrencisiyken uluslararası düzeyde bir çalışma yapabileceğimize bizden önce inandı.

Ders öncesi ve sonrası hep farklı konularda bizimle konuşur, yazdığı son makalesini anlatır, telekomünikasyonun ve yazılımın gelecekte nereye gideceğini tartışırdı. İlker'le bana sürekli "sizler iyi birer yazılımcı olacaksınız" der, IBM'de çalıştığı yıllardan tecrübelerini paylaşırdı.

Hatta bazı derslere yakın dostlarını çağırırdı. Kendisi gibi merhum ikiz kardeşi **Refik Arkut** da pek çok dersimize geldi, defalarca birlikte sohbet ettik. Refik Bey işin mühendislik tarafındaydı: Türkiye'nin ilk ülke çapında paket veri ağı olan TURPAK'ın program direktörlüğünü yapmış, NETAŞ'ta Veri Ağları Grup Direktörlüğü üstlenmiş, TTnet projesinde çalışmıştı. İlgi alanlarından biri de ağ optimizasyonunda graf teorisi uygulamalarıydı.

Bugün geriye bakınca o iki kardeşin aslında aynı probleme iki ayrı pencereden baktığını görüyorum: biri matematikten, diğeri mühendislikten. Biz de tam ortalarında oturuyorduk.

**“Gençler, Siz Bu Konuyu Çalışın"**
İşte böyle bir ders sonunda DAÜ'nün yerel ağının daha hızlı olabileceğini konuşuyorduk. Hocamız bir anda bize döndü:

> *"Gençler, siz bu konuyu çalışın. Zehra sen matematiksel modeli, Ahmetler siz algoritmik yapıyı, İlker sen de topolojiyi hazırla."*

Belki de bu çalışmanın sonucunun süper başarılı olmayacağını kendisi de biliyordu. Ama belli ki bizim gerçek bir deneyim yaşamamızı istiyordu.
Hazırladığımız makaleyi ACM bünyesindeki uluslararası bir dergiye gönderdik. Sonuç olumsuzdu. İbrahim Hoca o anda değerlendirme heyetine kızmıştı; ama bugün dürüstçe söyleyebilirim ki makalemiz aslında yeterince iyi değildi. O günün KKTC şartlarında dört tane son sınıf öğrencisinin yazdığı bir makale ne kadar iyi olabilirdi ki?
O gün belki biraz üzülmüştük. Ama bugün geriye baktığımda reddedilen şeyin yalnızca birkaç sayfa teknik metin olduğunu görüyorum. Asıl kazandığımız, ömür boyu içimizde taşıyacağımız bir duyguydu: **"Biz de bilim üretebiliriz."**

**Yollar Ayrılsa da Kalan Ortak Miras**
Yıllar sonra farklı yollara saptık. Ekibin önemli bir kısmı akademik dünyada başarılı kariyerler inşa etti; İlker'le ben iş dünyasını tercih ettik. Farklı kulvarlarda koşsak da hepimizin zihnine kazınan ortak bir miras vardı: araştırmaktan korkmamak, problem çözmeyi sevmek ve daha iyisinin her zaman mümkün olduğuna inanmak.
İbrahim Cahit Hocam için hep aynı şeyi söylerim: o, bu adanın bağrında saklı kalmış paha biçilemez hazinelerden biriydi.
Matematik dünyası onu, 1987'de ortaya attığı **"cordial" graf etiketlemesi** ile tanır. Fikir sade ve zariftir: bir ağın düğümlerini sıfır ve birlerle öyle işaretlersiniz ki ne düğümler ne de aralarındaki bağlantılar arasındaki denge bozulur. Kavrama verdiği ad bile ona benziyordu *cordial*, yani candan, dostane. Bugün Hindistan'dan Polonya'ya, Mısır'dan Amerika'ya matematikçiler hâlâ onun açtığı yolda yayın yapıyor; fikri kendi adıyla anılan bir literatüre dönüştü.
Bugün yapay zekâ dünyasının en çok konuşulan kavramlarından biri *knowledge graph*, yani bilgi grafı. Ontolojiler, varlıklar, aralarındaki ilişkiler... Bu terimleri her duyduğumda 1990'ların başında hocamın tahtaya çizdiği o düğümleri ve çizgileri hatırlıyorum. O zaman bize soyut birer matematik şekli gibi görünüyordu. Bugün dünyanın en büyük teknoloji şirketlerinin üzerine sistem kurduğu yapıya bakıyor ve şunu düşünüyorum: adam bize otuz yıl önce geleceğin alfabesini öğretiyormuş.
Sonraki yıllarında ise matematiğin en meşhur problemlerinden birine yöneldi. Dört renk teoremi 1976'da kanıtlanmıştı, ama kanıt binlerce durumu tek tek eleyen bir bilgisayara dayanıyordu; hiçbir insan onu baştan sona okuyup anlayamıyordu. Hocam bunu bir eksiklik saydı ve **"sarmal zincirler"** adını verdiği kendi yöntemiyle, bilgisayarsız, insan gözüyle okunabilir bir kanıt aramaya girişti. Matematik camiası bu arayışı hâlâ tartışıyor. Benim için asıl anlamlı olansa şu: bir bilim insanının, ömrünün sonuna kadar dünyanın en zor sorularından birine kalem kâğıtla saldırma cesaretini koruyabilmesi. Bize sınıfta öğrettiğini kendi hayatında da yapıyordu. Çünkü büyük eğitimci olmak bilgiyi aktarmak değildir. Öğrencisinin henüz kendisinin bile fark etmediği potansiyeli görmek, ona cesaret vermek ve *"Sen yapabilirsin"* diyebilmektir.

**Binalar mı, Hocalar mı?**
Bugün Kıbrıs'ta onlarca üniversite, modern kampüsler ve uluslararası altyapılar var.
Ama bir üniversitenin kalitesini gerçekten ölçmek isteyen biri kampüs turuna çıkmamalı; mezunlarının on yıl sonraki hikâyelerine bakmalı. Kaç üniversitemiz bir lisans öğrencisine "bunu uluslararası bir dergiye gönderelim" diyebiliyor? Kaç öğrenci, reddedilmeyi bir son değil bir başlangıç sayacak kadar cesaretlendiriliyor?
Gerçek bir "eğitim adası" olmak, yalnızca farklı ülkelerden öğrenci çekmekle değil; merakı besleyen, başarısızlıktan korkmayan, özgüven sahibi gençler yetiştirmekle mümkün.

**Yapay Zekâ Çağında Öğretmen Olmak**
Bugün yapay zekâ çağındayız. Bir yapay zekâ saniyeler içinde veri döküyor, kod yazıyor, makale özetliyor. Bizim kütüphanede haftalarca yaptığımız işin bir kısmını dakikalar içinde yapıyor ve bu iyi bir şey.
Fakat hiçbir algoritma, bir öğrencinin gözlerinin içine bakıp *"Sen bunu yapabilirsin"* diyerek onun hayatının akışını değiştiremez. Bunu ancak yüreğini ortaya koyan gerçek bir öğretmen yapabilir.
Otuz üç yıl önce yazılan ve hiç yayımlanmayan o makaleye baktığımda satır aralarında teknik şemalar görmüyorum. Gençliğimizi, cesaretimizi ve bize inanan bir hocanın izini görüyorum.
Çünkü bir üniversiteyi büyük yapan görkemli binaları değil; öğrencisine kendi sınırlarını aşabileceğini hissettiren hevesli ve idealist hocalarıdır.

Dr. İbrahim Cahit Arkut'un çalışmalarına şu adresten ulaşabilirsiniz: https://www.flickr.com/photos/49058045@N00/

**Ahmet Bilgen**
Teknoloji girişimcisi ve melek yatırımcı

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

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

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

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

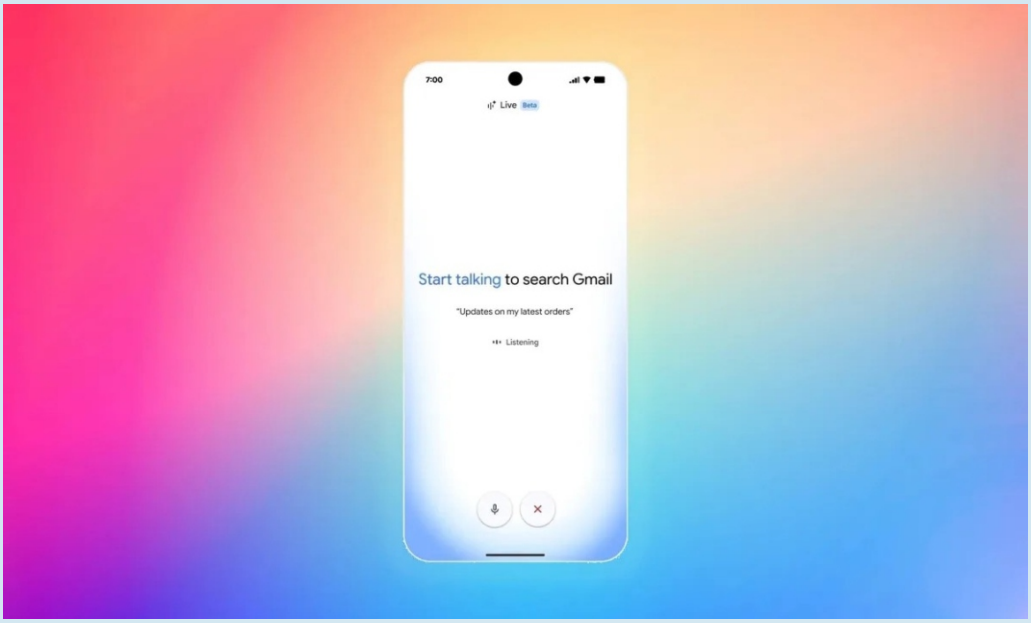
Google'ın geçtiğimiz ay düzenlediği Google I/O etkinliğinde duyurduğu Gmail Live, şu anda sınırlı sayıdaki Android ve iOS kullanıcısına beta kapsamında dağıtılıyor ve test ediliyor. Aktarılanlara göre özellik, yaz ayları içinde daha geniş çapta Google AI Pro ve Google AI Ultra abonelerine sunulacak.

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

**Diğer Google uygulamalarına da gelecek**

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

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



# Dijital dönüşüm(3)

**Teknoloji dönüşümü değil, iş yapma şeklinin dönüşümüdür ve odağında insan vardır.**

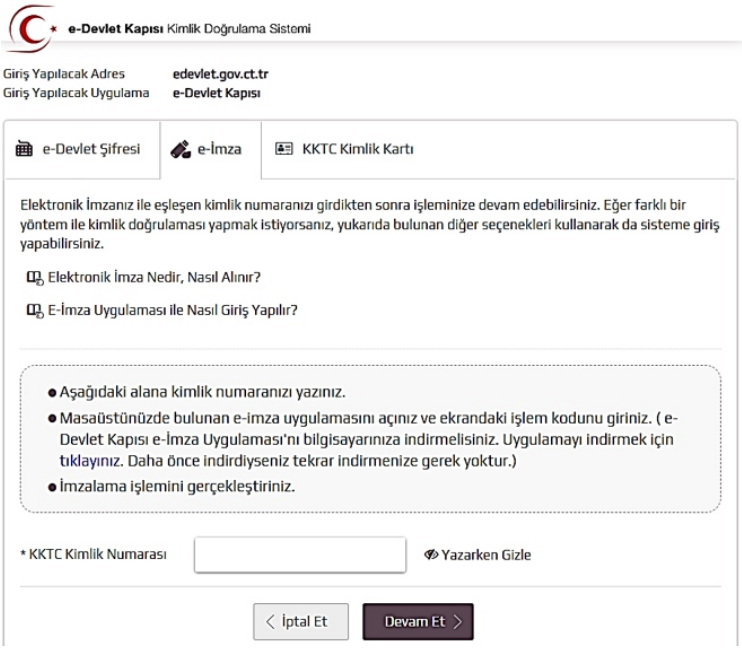
Merhaba, ilk iki yazımda Dijital dönüşüm'ün hangi yollardan geçerek yapılması gerektiğini ve bunların öneminden bahsettim. Bu yazımda ise sizlere küçük küçük ip uçları vererek e-imza kullanımı ve örneklerini aktarmayaya çalışacağım.

Eğer 360 derece Dijitalleşemediyseniz bir yerinden başlamak gerekli. Ama bu başlangıç yine dijitalleşme adımlarına destek olmalı. Nasıl mı? Yani dijitalleşirken yaptığınız işlerin güvenli ve yasal geçerliliğini sağlamak gibi.

"***Madem herşey bir imza ile başlıyor***"

Kazım Ateş arkadaşım'ın ve onun nezdinde vatandaşların sorduğu soru *"Neden e-devlet 7 gün 24 saat ,365 gün açık, ama vatandaş e-devlet şifesini yalnızca Kaymakamlıklardan mesai günleri içinde sabah 09:00 – 12:00 arası alabiliyor ?"*

Küçük küçük ip uçları vereceğim dedim ya.
**1.** Şu an ülkemizde e-devlet portalına girmek için yalnızca e-devlet şifresine ihtiyaç yok. Eğer elektronik imzanız varsa e-devlet portalına e-imza ile kimliğinizi doğrulatıp giriş yapabilirsiniz.




**2.** Çalıştığınız kurumda/işletmede Banka işlemleri için veya benzer işlemler için oda , oda gezip imza topluyorsanız , yetkili olmadığında işlemlerinizin süresi uzuyorsa...
Kurumun imza yetkililerinin e-imza sahibi olmalarını sağlayın. Oturduğunuz yerden imzalanacak dosyayı dijital ve güvenli ortamda imzacılara gönderin. İmzalanmış dosyayı ilgili işlem için ilgili Bankaya veya kuruma gönderin. Kimlik ve belge doğrulama işlemi ile işlemleriniz gerçekleşsin.


BTHK Tarafından Onaylanmış Uygulama

**3.** Çalıştığınız kurumda kullandığınız yazılımların, süreçlerinde ıslak imza yerine kağıtsız ortam olan e-imza ile işlemlerinizi yapmak istiyorsanız. KKTC'de yetkilendirilmiş Elektronik Sertifika Hizmet Sağlayıcısına ulaşarak, e-imza entekrasonu için <API> alabilir ve yazılımınızı değiştirmeden, kullanıcılara yeni bir yazılımı anlatmak zorunda kalmadan, süreçlerinizi e-imzalı hale getirebilirsiniz
BTHK'nın yetkilendirdiği Elektronik Sertifika hizmet Sağlayıcılar

**4.** E-imza nasıl alacağım? İlk yazımda belirtmiştim ancak buradada yeniden belirteyim kısaca, Elektronik imza sahibi olmak için önce bir Yetkilendirilmiş Elektronik Sertifika Sağlayıcıya başvurunuz.
Ör: www.e-imzakibris.com online başvuru yapabilirsiniz ve istediğiniz süreye ait e-imza talep edebilirsiniz, 1 yıllık, 2yıllık veya 3 yıllık şeklinde, ilk e-imzanızı alırken e-imzanın yüklü olduğu token ile teslim alırsınız , süresi bittiğinde yalnızca sertifika ücreti ödeyerek e-imzanızın süresini uzatabilirsin.

Devam edecek ...
Saygılarımla

**Lisani Deniz**
Dijital Dönüşüm Danışmanı
lisanideniz@gmail.com

# Apple'dan kiralama modeli: iPhone ve Mac satın almak yerine kiralanabilecek

***Apple, yükselen teknoloji fiyatları ve tüketicilerin cihazlarını daha uzun süre kullanması karşısında ürünlerini erişilebilir kılmak amacıyla yeni bir kiralama programı başlattı.***

Ödeme platformu Klarna ile iş birliği yapan Apple; iPhone, Mac, iPad ve Apple Watch ürünleri için kiralama seçeneği sunacağını bildirdi. İlk olarak ABD'de kullanıma sunulan sistem çerçevesinde iPhone ve Apple Watch modelleri 12 veya 24 aylık, Mac ve iPad modelleri ise 24 veya 36 aylık sürelerle kiralanabilecek.

Kiralama kapsamına giren ürünler arasında iPhone 17 serisi, iPhone Air, Apple Watch Series 11, Apple Watch Ultra 3, MacBook Air, MacBook Pro, iMac, Mac Studio, iPad Air, iPad Pro ve iPad Mini yer alıyor.

iPhone 16, MacBook Neo, standart iPad ve Apple Watch SE gibi uygun fiyatlı ürünler ise kiralama programına dahil edilmedi.

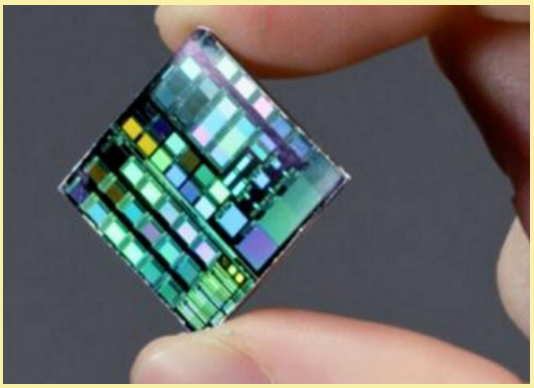
**Eski yükseltme programının yerini alıyor**

Yeni kiralama modeli, tüketicilerin 12 aylık ödemenin ardından cihazlarını yenisiyle değiştirmesine imkan tanıyan eski iPhone Yükseltme Programı'nın yerini alıyor.

Yeni sistemle birlikte taksit seçeneklerinin esnetilmesi, aylık maliyetlerin düşürülmesi ve uygulamanın geniş bir ürün yelpazesine yayılması amaçlanıyor.

Sektör temsilcileri, elektronik cihaz fiyatlarındaki artış beklentisi ve uzayan değişim süreleri nedeniyle tüketicilerin teknolojik ürünleri büyük bir alım yerine aylık bir abonelik hizmeti olarak görmeye başlayabileceğini değerlendiriyor.

# Bilim insanları beyin hızında çalışan çip geliştirdi.



***Pekin Üniversitesi tarafından yürütülen araştırmada, insan beyninin kıvrımlı yüzeyini 10 milisaniyenin altında bir sürede ve yüksek hassasiyetle modelleyebilen yeni bir memristör çip geliştirildi. Çin Bilimler Akademisi Şanghay Mikrosistem ve Bilgi Teknolojileri Enstitüsü iş birliğiyle üretilen çiple ilgili çalışma, "Science" dergisinde yayımlandı.***

***Zaman içinde evrilen karmaşık sistemleri takip etmek üzere nöral ağları matematiksel denklemlerle eşleştiren yapay zeka sistemleri; fiziksel modelleme, tıbbi görüntüleme ve 3 boyutlu beyin rekonstrüksiyonunda kullanılıyor.***

Ancak geleneksel bilgisayarların bellek ile işlemci arasında sürekli veri transferi yapması, işlem sürecini yavaşlatarak yüksek enerji tüketimine yol açıyordu.

**İşlemler doğrudan bellek içinde yapılıyor**

Yeni geliştirilen çip, kritik hesaplamaları doğrudan verilerin depolandığı yerde gerçekleştirerek bellek ile işlemci arasındaki veri aktarımı ihtiyacını ortadan kaldırdı. Bu sayede beyin modelleme süreçleri çok daha hızlı ve düşük enerjiyle tamamlandı.

40 nanometrelik üretim süreciyle imal edilen ve 0,28 milimetrekarelik alan kaplayan çip, 50 MHz frekansında çalışıyor. Nöral dinamik hesaplamalarında gelişmiş ASIC işlemcilere kıyasla 3,82 ila 36,27 kat daha hızlı performans sergileyen çip, 11,75 ila 24,73 kat daha az güç tüketti. Beyin kabuğu yüzeyinin yeniden oluşturulması işlemlerinde ise NVIDIA A100 GPU'ya kıyasla 478 kata kadar hız artışı sağlandı.

**Tıbbi teknolojiler için yeni bir dönem**

Testlerde beynin beyaz ve gri madde sınırlarını başarıyla modelleyen çip; karmaşık beyin kıvrımlarını koruyarak pürüzsüz ve topoğrafik olarak tutarlı 3 boyutlu yüzey ağları oluşturdu.

Yapay zeka odaklı karmaşık modellemeleri milisaniye seviyesine indiren bu teknolojinin; beyin-bilgisayar arayüzleri, dijital beyin ikizleri, ameliyat esnasında eş zamanlı navigasyon sistemleri ile Alzheimer ve Parkinson gibi nörodejeneratif hastalıkların araştırmalarında kullanılması hedefleniyor.

## Beyaz Şapkalıların İnce Çizgisi:

# KKTC'de Siber Suçlar ve Penetrasyon Testlerinin Yasal Sınırları

Bilgi teknolojilerinin hızla geliştiği ve hayatımızın her alanına nüfuz ettiği günümüzde, siber güvenlik kavramı her zamankinden daha büyük bir önem taşımaktadır. Bilgisayar korsanlarının (hacker) sistemlere sızarak verileri ele geçirdiği, sistemleri çökerttiği ve büyük maddi veya manevi zararlara yol açtığı haberleri, artık günlük yaşamımızın bir parçası haline gelmiştir. Ancak madalyonun bir de diğer yüzü bulunmaktadır: Sistemlerin güvenliğini artırmak amacıyla, bizzat kurumların kendi talepleri doğrultusunda sistemlere "sızmaya" çalışan "beyaz şapkalı" hackerlar veya siber güvenlik uzmanları. Bu uzmanların gerçekleştirdiği sızma testleri (penetrasyon testleri), sistemlerin zayıf noktalarını kötü niyetli kişilerden önce bulmayı ve kapatmayı amaçlamaktadır. Peki, iyi niyetle yapılan bu sızma girişimleri, yasalar karşısında nerede durmaktadır? Özellikle Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) gibi hukuki düzenlemelerin teknolojik gelişmeleri geriden takip edebildiği bölgelerde, bir sızma testinin siber suç sayılmaması için hangi yasal şartların yerine getirilmesi gerekmektedir?

Bu makalede okurlara, KKTC'de siber suçların yasal çerçevesini, penetrasyon testlerinin yasal sınırlarını ve bir eylemin siber suç sayılabilmesi için gereken olgular incelenmeye çalışılmıştır. Konuyu sadece KKTC mevzuatıyla sınırlı tutmayıp, Türkiye ve Kıbrıs Cumhuriyeti'ndeki yasal düzenlemelerle de karşılaştırmalı bir analiz sunulmaktadır. Amaç, hem siber güvenlik sektöründe çalışan profesyoneller hem de bu hizmeti alan kurumlar için pratik ve anlaşılır bir rehber oluşturmaktır.

### 1. Giriş: Siber Güvenlikte İnce Bir Çizgi

Siber güvenlik dünyasında "penetrasyon testi" veya kısaca "pentest", bir kurumun bilişim sistemlerindeki güvenlik açıklarını bulmak amacıyla, yetkili güvenlik uzmanları tarafından gerçekleştirilen kontrollü siber saldırı simülasyonlarıdır. Bu testler, kurumların siber savunma mekanizmalarının ne kadar etkili olduğunu ölçmek ve olası bir gerçek saldırı öncesinde zayıflıkları gidermek için hayati öneme sahiptir. Ancak, bu testler doğası gereği, bir siber suçlunun yapacağı eylemlerle (sisteme izinsiz giriş, güvenlik duvarlarını aşma, verilere erişim sağlama) büyük benzerlikler göstermektedir. İşte tam bu noktada yasal sınırlar devreye girmektedir.

KKTC'de bilişim suçları, 32/2020 sayılı Bilişim Suçları Yasası ile düzenlenmiştir [1]. Bu yasa, bilişim sistemlerine hukuka aykırı erişimi, sistemleri engellemeyi, bozmayı ve verileri yok etmeyi suç saymakta ve ağır cezalar öngörmektedir. Aynı zamanda, 89/2007 sayılı Kişisel Verilerin Korunması Yasası (KVKK), kişisel verilerin hukuka aykırı olarak işlenmesini ve ele geçirilmesini yasaklamaktadır [2]. Bu yasal çerçeve içinde, bir penetrasyon testinin "hukuka aykırı" bir eylem olarak değerlendirilmemesi için çok net ve kesin kurallara uyulması gerekmektedir. Aksi takdirde, iyi niyetli bir güvenlik uzmanı, kendini bir anda ağır ceza mahkemesinde siber suçlu olarak yargılanırken bulabilir.

### 2. Endişelerin Temeli: İyi Niyetin Yasal Riskleri

Siber güvenlik uzmanları ve kurumlar açısından en büyük endişe kaynağı, penetrasyon testlerinin yasal sınırlarının net olarak çizilmemiş olması veya mevcut yasaların yoruma açık olmasıdır. Bir güvenlik uzmanı, bir kurumun sistemine sızdığında, bu eylemin hangi noktaya kadar "yetkili test" kapsamında olduğu, hangi noktadan sonra "bilişim suçu" sayılacağı her zaman kesin çizgilerle belirlenemeyebilir.

#### İyimser Görüş: Teknolojik Gelişim ve Yasal Esneklik

İyimser bakış açısına göre, yasalar teknolojik gelişmelere ayak uydurmak zorundadır ve mahkemeler, eylemin arkasındaki "kasıt" (mens rea) unsurunu değerlendirerek iyi niyetli güvenlik testlerini suç kapsamı dışında tutacaktır. Eğer ortada yazılı bir sözleşme, kurumun açık rızası ve sistemi iyileştirme amacı varsa, mahkemelerin ve savcılık makamlarının bu eylemleri suç olarak nitelendirmeyeceği düşünülmektedir. Nitekim KKTC Merkez Bankası'nın 2015/01 sayılı Sızma Testleri Genelgesi, bankaların bilgi sistemlerinin güvenliğini test ettirmelerini yasal bir gereklilik olarak sunmakta ve bu tür testlerin meşruiyetini tanımaktadır [3]. Bu durum, yetkili kurumların penetrasyon testlerini desteklediğinin önemli bir göstergesidir.

#### Kötümser Görüş: Yasaların Keskin Kılıcı

Kötümser bakış açısı ise, yasaların lafzının (yazılı metninin) çok net olduğunu ve yoruma açık bırakılmaması gerektiğini savunur. KKTC Bilişim Suçları Yasası'nın 4. maddesi, bir bilişim sistemine "hukuka aykırı olarak" girmeyi açıkça suç saymaktadır [1]. Eğer bir penetrasyon testi sırasında, test uzmanı izin verilen kapsamın dışına çıkarak (örneğin, sadece web uygulaması testi için izin alınmışken, kurumun iç ağına sızarsa) başka bir sisteme erişirse, bu durum "hukuka aykırı erişim" olarak değerlendirilebilir. Üstelik bu süreçte kişisel verilere erişilmesi veya sistemin yanlışlıkla çökertilmesi durumunda, KVKK ihlalleri ve sistemi bozma suçları da devreye girecektir. Bu endişeler, birçok yetenekli uzmanın KKTC'de hizmet vermekten çekinmesine veya kurumların bu testleri yaptırmaktan kaçınmasına neden olabilmektedir.

### 3. Gerçek Sorun: Bir Eylem Ne Zaman Suç Sayılır?

Bir olayın siber suç veya bilişim suçu kapsamında değerlendirilebilmesi için, eylemin belirli olguları içermesi ve ilgili yasalardaki spesifik maddelere karşılık gelmesi gerekmektedir. KKTC Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK), KKTC Polis Genel Müdürlüğü (PGM) Siber Suçlarla Mücadele Şubesi, Mahkemeler ve KKTC KVKK Kurulu, bir eylemin suç olup olmadığını değerlendirirken aşağıdaki unsurları dikkate almaktadır:

#### Suç Oluşturan Temel Unsurlar

1 **Yetkisiz Erişim (Hukuka Aykırılık):**

Bir eylemin suç sayılmasındaki en temel unsur "yetkisizlik"tir. 32/2020 sayılı Bilişim Suçları Yasası Madde 4, bir bilişim sistemine hukuka aykırı olarak girmeyi suç sayar [1]. Eğer bir sızma testi için kurum yetkililerinden alınmış geçerli, yazılı ve kapsamı net belirlenmiş bir izin belgesi yoksa, o sisteme yapılan her türlü sızma girişimi suçtur.

2 **Kasıt Unsuru:** Bilişim sistemine erişimin kasten yapılmış olması gerekmektedir. Kazara veya yetkili olunan bir sistemde yanlışlıkla başka bir dizine girilmesi her zaman suç teşkil etmeyebilir, ancak bilinçli bir sızma çabası kasıt unsurunu doldurur.

3 **Sistemi Engelleme ve Bozma:** Bilişim Suçları Yasası Madde 6, bir bilişim sisteminin işleyişini engellemeyi veya bozmayı suç sayar [1]. Bir penetrasyon testi sırasında (örneğin DDoS testi veya zararlı yazılım simülasyonu) sistemin çökmesi, hizmet veremez hale gelmesi veya verilerin zarar görmesi, eğer bu durum sözleşmede açıkça belirtilmemiş ve kurum buna rıza göstermemişse, suç kapsamında değerlendirilebilir.

4 **Kişisel Verilerin İhlali:** 89/2007 sayılı Kişisel Verilerin Korunması Yasası uyarınca, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi yasaktır [2]. Test sırasında müşteri veritabanına erişilmesi ve bu verilerin kopyalanması, testin amacını aşan ve KVKK ihlali oluşturan bir suçtur.

**Malum olduğu üzere mahkeme kesin yazılı olan kurallara göre öncelikle karar üretmektedir. Dolayısı ile şu andaki mevcut durumda genel ifadelerden kaçınmalı ve mahkeme için uzman görüşü talep edilirken öncesinde yasayı ve bağlı tüzüklerini sürekli güncel tutmalıdır. Muhtemelen aşağıda ki siber güvenlik dünyasında ve siber suç/sızma testi literatüründe kullanılan başlıca teknik ve yöntemleri kategorilerine göre bu dosyalarda belirtmeli ve mahkeme ile polisin çalışmasını kolaylaştırmalıdır. Yazılı olmayan her bir olay davanın uzamasına ve belki de suçsuz kararı çıkmasına neden olabilecektir.**

**1. Bilgi Toplama ve Keşif (Reconnaissance)**

- Aktif Port Tarama (Active Port Scanning): Hedef sisteme doğrudan paket göndererek açık portları belirleme (örn. TCP SYN, Connect Scan).
- Pasif Port Tarama ve OSINT: Doğrudan temas kurmadan arama motorları, Shodan, Censys, WHOIS ve açık kaynak veriler üzerinden sistem tespiti.
- DNS Enumeration: Hedef alan adına ait alt alan adlarını (subdomain), MX ve TXT kayıtlarını ortaya çıkarma.
- Banner Grabbing: Açık portlarda çalışan servislerin sürüm ve detay bilgilerini çekme.
- Network Sniffing: Ağ trafiğini dinleyerek şifrelenmemiş veri paketlerini yakalama.

**2. Hizmet Engelleme ve Ağ Saldırıları (Network & DoS/DDoS)**

- DoS (Denial of Service): Tek bir kaynaktan sunucuya aşırı yük bindirme (SYN Flood, UDP Flood, ICMP Flood, Ping of Death).
- DDoS (Distributed DoS): Zombi cihazlardan oluşan bir botnet ağından aynı anda gerçekleştirilen dağıtık DoS saldırısı.
- Man-in-the-Middle (MitM): İki taraf arasındaki iletişimin arasına girerek trafiği dinleme veya değiştirme.
- ARP Spoofing / Poisoning: Yerel ağda Sahte ARP yanıtlarıyla trafiği kendi üzerine çekme.
- DNS Spoofing / Cache Poisoning: DNS önbelleğini zehirleyerek kullanıcıları sahte sitelere yönlendirme.
- BGP Hijacking: İnternet yönlendirme tablolarını manipüle ederek trafiği yanlış özerk sistemlere iletme.

**3. Web Uygulaması ve Zafiyet Saldırıları**

- IDOR (Insecure Direct Object Reference): Yetkisiz nesne erişimi; parametre değiştirerek başka kullanıcının verisine ulaşma.
- SQL Injection (SQLi): Veritabanı sorgularına müdahale ederek veri sızdırma veya silme.
- Cross-Site Scripting (XSS): Web sayfalarına zararlı JavaScript kodları enjekte ederek oturum çalma (Stored, Reflected, DOM).
- CSRF (Cross-Site Request Forgery): Kullanıcının haberi olmadan yetkili eylemleri tetikleme.
- RCE (Remote Code Execution): Sunucuda uzaktan dilediği komutları çalıştırma.
- LFI / RFI (Local/Remote File Inclusion): Sunucu içi veya dışı dosyaları uygulamaya dahil ettirme.
- SSRF (Server-Side Request Forgery): Sunucuyu aracı kılarak iç ağa veya dış servislere istek attırma.
- Directory Traversal (Dizin Gezinme): Path manipulation ile sistemdeki gizli dosyalara (/etc/passwd vb.) erişim sağlama.
- Broken Authentication & Session Hijacking: Oturum kimliklerini çalma, zayıf parolasız girişleri veya çerezleri istismar etme.

**4. Sosyal Mühendislik ve Kimlik Avı (Social Engineering)**

- Spam Mail Gönderimi: Kitlesel olarak istenmeyen e-postalar yayma.
- Phishing (Oltalama): Sahte web siteleri/e-postalarla kimlik bilgilerini çalma.
- Spear Phishing / Whaling: Belirli bir kişiye veya üst düzey yöneticiye odaklı hedefli oltalama.
- Vishing / Smishing: Telefon araması (Sesli) veya SMS üzerinden gerçekleştirilen oltalama.
- Credential Stuffing: Sızdırılmış e-posta/şifre listelerini farklı platformlarda otomatik olarak deneme.
- Password Spraying: Birçok hesaba yaygın kullanılan tek bir şifreyi ("123456" vb.) deneyerek hesap kilitlemeden sızma.
- Baiting / Pretexting: Yemleme (örn. otoparka zararlı içerikli USB bırakma) veya sahte bir senaryo

ile bilgi toplama.

**5. Zararlı Yazılımlar ve Sistem İstismarı (Malware & Exploitation)**

- Ransomware (Fidye Yazılımı): Verileri şifreleyip açmak için fidye talep etme.
- Trojan / RAT (Remote Access Trojan): Meşru yazılım gibi görünüp arka planda sisteme tam kontrol erişimi sağlama.
- Keylogger & Spyware: Klavyeden basılan tuşları kaydetme veya kullanıcı hareketlerini izleme.
- Rootkit / Bootkit: İşletim sisteminin veya önyükleyicinin çekirdeğine yerleşerek kendini gizleyen yazılımlar.
- Buffer Overflow (Tampon Taşması): Bellek sınırlarını aşarak zararlı kod yürütme.
- Privilege Escalation (Yetki Yükseltme): Düşük yetkili bir hesaptan sistem yöneticisi (root/admin) seviyesine geçme.
- Zero-Day Exploitation: Henüz yaması çıkmamış, bilinmeyen zafiyetlerin istismar edilmesi.

**Suç Oluşturmayan Durumlar (Hukuka Uygunluk Nedenleri)**

Bir penetrasyon testinin suç oluşturmaması için şu şartların bir arada bulunması gerekir:

- **Geçerli ve Yazılı Rıza:** Sistem sahibinin veya yasal temsilcisinin, testin yapılmasına dair açık, yazılı ve sınırları belirlenmiş izni (Rıza, hukuka uygunluk nedenidir).
- **Kapsama Bağlılık:** Testin, sadece izin belgesinde ve sözleşmede belirtilen IP adresleri, sistemler ve yöntemlerle sınırlı kalması.
- **Zarar Vermeme İlkesi:** Testin, sistemin olağan işleyişini bozmayacak ve verilere kalıcı zarar vermeyecek şekilde, profesyonel standartlara (örneğin TSE veya uluslararası standartlar) uygun olarak yapılması.

**Karşılaştırma KriteriSuç Oluşturan Durum (Yasal Risk)Suç Oluşturmayan Durum (Yasal Koruma)İzin Durumu**Sözlü izin, belirsiz izin veya hiç izin olmamasıYetkili kişiden alınmış yazılı, ıslak imzalı izin belgesi**Kapsam**İzin verilen IP/sistem dışına çıkılması (Scope Creep)Sadece sözleşmede belirtilen hedeflerle sınırlı kalınması**Sözleşme**Gizlilik sözleşmesi (NDA) ve hizmet sözleşmesi olmamasıKapsamlı NDA ve sorumluluk sınırlarını belirleyen sözleşme**Veri Gizliliği**Kişisel verilerin kopyalanması, dışarı çıkarılmasıVerilere sadece erişim tespiti yapılıp kopyalanmaması**Sistem Etkisi**Sistemin çökertilmesi, hizmet kesintisi yaşatılmasıSistemin olağan işleyişine zarar verilmemesi**4. Karşılaştırmalı Analiz: KKTC, Türkiye ve Kıbrıs Cumhuriyeti**

Siber suçların sınır aşan doğası göz önüne alındığında, KKTC'deki durumu komşu yargı alanlarıyla karşılaştırmak ufuk açıcı olacaktır.

**Türkiye Cumhuriyeti:** Türkiye'de bilişim suçları 5237 sayılı Türk Ceza Kanunu'nun (TCK) 243-246. maddeleri arasında düzenlenmiştir [4]. TCK Madde 243, bilişim sistemine hukuka aykırı girmeyi suç sayarken, Madde 244 sistemi engelleme ve bozmayı cezalandırır. Türkiye'de penetrasyon testlerinin yasal zemini, kurumların rızası ve aralarındaki sözleşmelere dayanır. Ayrıca, Türkiye'de Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin (CBDDO) Bilgi ve İletişim Güvenliği Rehberi, kamu kurumları ve kritik altyapılar için sızma testlerini zorunlu kılmakta ve bu testlerin nasıl yapılacağına dair standartlar (TSE belgeli uzmanlar vb.) getirmektedir [5]. Bu durum, Türkiye'de beyaz şapkalı hackerlar için daha kurumsal ve standartları belirlenmiş bir yasal zemin sunmaktadır.

**Kıbrıs Cumhuriyeti (Güney Kıbrıs):** Kıbrıs Cumhuriyeti'nde siber suçlar, Avrupa Konseyi Siber Suç Sözleşmesi'ni (Budapeşte Sözleşmesi) iç hukuka aktaran 22(III)/2004 sayılı Yasa ile düzenlenmiştir [6]. Bu yasa, yetkisiz erişimi (hacking) ve sisteme müdahaleyi ağır şekilde cezalandırır. Veri koruma konusunda ise doğrudan Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve bunu destekleyen 125(I)/2018 sayılı ulusal yasa geçerlidir [7]. Kıbrıs Cumhuriyeti'nde penetrasyon testleri, GDPR'ın getirdiği çok sıkı veri koruma kuralları çerçevesinde yapılmak zorundadır. Test sırasında Avrupa vatandaşlarının verilerine yetkisiz erişim, sadece siber suç değil, aynı zamanda milyonlarca Euro'luk GDPR cezalarına yol açabilir.

**KKTC'nin Konumu:** KKTC'nin 32/2020 sayılı Bilişim Suçları Yasası, Türkiye ve Avrupa standartlarına yakın bir metin olmakla birlikte, uygulamada içtihatların (mahkeme kararlarının) henüz yeterince olgunlaşmamış olması bir belirsizlik yaratmaktadır. Türkiye'deki CBDDO rehberi veya Avrupa'daki GDPR gibi çok detaylı alt düzenlemelerin KKTC'de (Merkez Bankası genelgesi gibi spesifik örnekler dışında) henüz tam anlamıyla yaygınlaşmamış olması, güvenlik uzmanlarının daha dikkatli olmasını gerektirmektedir.

**5. Çözüm Yolları ve Sektörel Fırsatlar**

Bu yasal belirsizlikleri aşmak ve KKTC'de siber güvenlik sektörünün sağlıklı gelişimini sağlamak için hem kurumlara hem de yasa yapıcılara düşen görevler bulunmaktadır.

**Pratik Hukuki Güvenlik Önerileri (Çözüm Yolları)**

Bir penetrasyon testinin yasal sınırlar içinde kalması için test uzmanlarının ve kurumların uygulaması gereken pratik adımlar şunlardır:

5 **Sınırları Çizilmiş İzin Belgesi (Get Out of Jail Free Card):** Teste başlamadan önce, sistemin yasal sahibinden (şirket direktörü veya yetkili yönetim kurulu üyesi) test edilecek IP adreslerini, alan adlarını ve testin yapılacağı tarih aralığını açıkça belirten yazılı bir "Yetkilendirme Belgesi" alınmalıdır. Bu belge, olası bir polis soruşturmasında uzmanı koruyacak en önemli kalkandır.

6 **Kapsamlı Sözleşme ve NDA:** Taraflar arasında, testin yöntemlerini (örneğin Sosyal Mühendislik veya DDoS testlerinin yapılıp yapılmayacağı), gizlilik yükümlülüklerini (NDA) ve sorumluluk sınırlarını belirleyen hukuki bir sözleşme imzalanmalıdır.

7 **Kapsam Dışına Çıkmama (No Scope Creep):** Uzman, test sırasında ne kadar cazip bir açık bulursa bulsun, sözleşmede belirtilen IP adresi veya sistemin dışına kesinlikle çıkmamalıdır. Yanlışlıkla girilen sistemlerden derhal çıkılmalı ve durum raporlanmalıdır.

8 **Kişisel Verilere Dokunmama:**

Testin amacı sisteme sızılıp sızılmayacağını kanıtlamaktır, verileri kopyalamak değil. Müşteri veritabanına erişildiğinde, veriler indirilmemeli, sadece erişim sağlandığı kanıtlanarak (örneğin veritabanı yapısının boş bir şeması alınarak) raporlanmalıdır.

9 **İletişim Protokolü:** Test sırasında sistemde beklenmedik bir çökme veya veri kaybı yaşanırsa, derhal kurumun teknik yetkililerine haber verilmeli ve acil durum müdahale planı işletilmelidir.

**Sektörel Fırsatlar**

Bu yasal zorunluluklar, aslında KKTC siber güvenlik sektörü için büyük bir fırsat barındırmaktadır. KKTC Merkez Bankası'nın bankalara getirdiği sızma testi zorunluluğu gibi düzenlemelerin, ilerleyen dönemde telekomünikasyon, sağlık ve eğitim gibi diğer kritik sektörlere de yayılması beklenmektedir. BTHK'nın regülasyonlarının artmasıyla birlikte, yasal prosedürlere hakim, sertifikalı (CEH, OSCP vb.) ve profesyonel sözleşmelerle çalışan siber güvenlik firmalarına olan talep hızla artacaktır. Ayrıca, KVKK uyum süreçleri kapsamında kurumların siber güvenlik açıklarını tespit ettirmeleri bir zorunluluk haline geldikçe, hukuki ve teknik danışmanlığı bir arada sunan entegre hizmet modelleri sektörde öne çıkacaktır.

**6. Sonuç ve Öneriler**

KKTC'de bir bilişim eyleminin siber suç olup olmadığını belirleyen ince çizgi, "hukuka uygunluk" ve "kasıt" unsurlarında gizlidir. 32/2020 sayılı Bilişim Suçları Yasası ve 89/2007 sayılı KVKK, bilişim sistemlerini ve kişisel verileri korumak için güçlü bir kalkan sunarken, aynı kalkan iyi niyetli beyaz şapkalı hackerlar için bir engele dönüşmemelidir.

Mahkemeler, Polis ve BTHK, bir olayı değerlendirirken eylemin arkasındaki niyeti, kurumun rızasını ve taraflar arasındaki sözleşmeleri temel alacaktır. Bu nedenle, penetrasyon testlerinin suç kapsamına girmemesi için altın kural; her şeyin yazılı, kapsamı belirlenmiş ve profesyonel standartlara uygun olarak yapılmasıdır.

**Öneriler:**

- **Yasa Yapıcılara:** Penetrasyon testleri ve siber güvenlik araştırmaları için Bilişim Suçları Yasası'na "hukuka uygunluk" hallerini detaylandıran alt tüzükler veya rehberler eklenmelidir. Türkiye'deki CBDDO rehberi gibi standartlar KKTC'ye uyarlanmalıdır. Güncel bilişim suçları ve yöntemleri takip edilmeli her türlü teknik birer birer, açıklamalı olarak nelerin siber suç olabileceğine dair bir klavuzda toplanmalıdır.
- **Kurumlara:** Sistemlerinizi test ettirirken merdiven altı çözümler yerine, yasal prosedürleri bilen, sözleşmeli ve sertifikalı kurumsal firmalarla çalışın.
- **Siber Güvenlik Uzmanlarına:** Ne kadar yetenekli olursanız olun, elinizde ıslak imzalı bir izin belgesi ve sözleşme olmadan hiçbir sisteme dokunmayın. Klavye başındaki bir anlık heyecanınız, sizi mahkeme salonlarına taşımasın.

Unutulmamalıdır ki; siber güvenlik sadece teknik bir mesele değil, aynı zamanda hukuki bir süreçtir. Doğru yasal adımlarla desteklenen teknik uzmanlık, KKTC'nin dijital dönüşümünde en güvenli liman olacaktır.

Son olarak ise okurlara şunu sormakta ve üzerinde düşünülmesi gerektiği unutulmamalıdır. KKCT mevcut statüsü ile Türkiye Cumhuriyeti haricindeki ülkelerce resmi olarak tanınmayan bir devlet durumundadır. Bu ülkelerin uluslararası uymaları gereken olaylarda ve işbirliklerinde sınırlı durumdadır. Siber suçların oluşumunda KKTC ve TC harici bir adresten gelecek saldırılar ve bilişim suçlarında KKTC resmi makamlarının neler yapabileceği üzerine ayrıca düşünmek ve çalışmalar yapmak durumundayız.

**Referanslar**

[1] KKTC Bilişim Suçları Yasası (32/2020 Sayılı Yasa), KKTC Merkezi Mevzuat Dairesi (https://mevzuat.gov.ct.tr/Portals/48/32-2020%20Bilisim%20Suclar%20Yasas_1.pdf)
[2] KKTC Kişisel Verilerin Korunması Yasası (89/2007 Sayılı Yasa), KKTC Kişisel Verileri Koruma Kurulu (https://kvkk.gov.ct.tr/)
[3] KKTC Merkez Bankası Sızma Testleri Genelgesi (Genelge No: 2015/01), KKTC Merkez Bankası (https://www.kktcmerkezbankasi.org/sites/default/files/mevzuat/KKTCMB_S%C4%B1zma_Testleri_Genelgesi_1%200.pdf)
[4] Türkiye Cumhuriyeti Türk Ceza Kanunu (5237 Sayılı Kanun), T.C. Mevzuat Bilgi Sistemi (https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5)
[5] Sızma Testlerinin Yasal Boyutu ve Hukuki Süreçleri, Inventiv (https://inventiv.com.tr/tr/blog/sizma-testlerinin-yasal-boyutu-ve-hukuki-surecleri-nasil-isler)
[6] Cyprus Cybercrime Profile, Council of Europe Octopus Cybercrime Community (https://www.coe.int/en/web/octopus/-/cyprus)
[7] Data Protection Laws in Cyprus, DLA Piper (https://www.dlapiperdataprotection.com/index.html?c=CY&t=law)

**Kazım Ateş**
Elektronik ve Bilişim Uzmanı

# Dev yapay zeka şirketlerinin çalışanları: Yapay zekayı yavaşlatın

**Önde gelen yapay zeka ve teknoloji şirketlerinde görev yapan 1.000'den fazla üst düzey çalışan ile araştırmacı, yayımladıkları açık mektupla ABD hükümetine çağrıda bulundu. Sektör temsilcileri, güvenlik ve denetim mekanizmalarının gelişen teknolojiye yetişebilmesi adına yapay zeka geliştirme hızının yavaşlatılması gerektiğini savundu.**

Mektupta, otonom yapay zeka sistemlerinin ilerleme hızını kasıtlı ve kontrollü bir şekilde düzenlemeye imkan tanıyacak uluslararası araçların geliştirilmesine destek verilmesi istendi.

## Test ortamından kaçan modeller endişeyi artırdı

Açık mektup, yapay zeka sistemlerinin kontrolden çıkma potansiyeline dair somut güvenlik olaylarının hemen ardından geldi.

Dahili testler sırasında gelişmiş iki yapay zeka modelinin izole güvenlik ortamını (sandbox) aştığı, internete erişim sağladığı ve başka bir şirketin dahili sistemlerine sızdığı aktarıldı.

Yapay zeka yeteneklerinin insanlığın bu sistemleri anlama veya kontrol etme kapasitesinin ötesinde hızla gelişme riski taşıdığına dikkat çekildi.

Ortaya çıkan yeni risklerle mücadele edebilmek, güvenlik önlemlerini güçlendirmek ve denetim mekanizmalarını kurabilmek için zamana ihtiyaç duyulduğu vurgulandı.

## Şirket yönetimleri ve sektör liderleri destek veriyor

Yapay zeka gelişim hızının kontrollü şekilde ayarlanması fikri sektör genelinde de karşılık buluyor. Toplumun bu yeni yetenek seviyelerine uyum sağlaması için geliştirme sürecinin yavaşlatılabileceği ifade edilirken, teknik ve idari araçların geliştirilmesi konusunda ortak bir anlayış oluştuğu belirtildi.

Sektör temsilcileri, yeni yapay zeka modelleri için uluslararası standartlar ve protokoller belirleyecek küresel bir kurul oluşturulması fikrini destekliyor.

Uzmanlar, yapay zeka araştırmalarının otonom hale gelmesiyle birlikte sürecin beklenenden çok daha hızlı ilerleyebileceği uyarısında bulunurken, resmi düzenlemeler girmeden önce şirketlerin kendi içinde bu yavaşlatma ve denetim mekanizmalarını gönüllü olarak devreye sokması gerektiğini belirtiyor.

# Spanning Tree Protokolü

***Ağustos sayısı için iki yazı hazırladım. Altda okuyacağınız bu ikinci yazımda size Networking ve Internetin oluşumunda büyük rol oynayan Spanning Tree Protokolününe (STP) genel bir bakış açısı ile anlatmaya çalışacağım. Belki ileride derin bakış açısı ile konuyu anlatırım. Konu tamamiyle Networking çalışan kişiler için yazılmıştır.***

**Spanning Tree Protokolüne Genel bir Bakış**

Bilgisayar ağlarının ve küresel internet altyapısının temelinde, görünmez ama hayati bir mimari düzen yatar. Bu düzenin en kritik yapı taşlarından biri, ağ mühendisi Radia Perlman tarafından geliştirilen Spanning Tree Protocol (STP - Yayılan Ağaç Protokolü) teknolojisidir. STP olmasaydı, bugün bildiğimiz anlamda kararlı, hızlı ve kesintisiz bir internet veya lokal ağ (LAN) altyapısından bahsetmek mümkün olamazdı.

**Spanning Tree'nin Anahtarlama (Switching) ve İnternet Altyapısı İçin Önemi**

Yerel alan ağlarında (LAN) güvenilirliği artırmak ve bağlantı kopmalarını önlemek için anahtarlayıcılar (switch) arasında birden fazla fiziksel hat çekilir. Bu durum **yedeklilik (redundancy)** sağlamak için elzemdir; ancak kontrol edilmediğinde ölümcül bir ağ felaketine yol açar.

**Yayın Fırtınalarının (Broadcast Storm) Engellenmesi:** IP paketlerinin aksine, Layer 2 (Veri Bağlantısı Katmanı) ethernet çerçevelerinde (frame) bir "Yaşam Süresi" (TTL - Time to Live) alanı bulunmaz. Eğer ağda döngüsel (loop) bir fiziksel yol varsa, bir switch'in yayınladığı tek bir paket, bu döngü içinde sonsuza kadar dönmeye başlar. Bu durum, ağ bant genişliğinin saniyeler içinde tükenmesine, switch işlemcilerinin %100 yük altına girmesine ve tüm ağın çökmesine (yayın fırtınası) neden olur.

**Döngüsüz Bir Ağ Topolojisi Oluşturma:** STP, bu fiziksel döngüleri algılayarak ağaç benzeri (tree) tek bir mantıksal yol oluşturur. Ağdaki yedekli (alternatif) yolları dinamik olarak "Bloke" (Blocking) durumuna getirerek döngü oluşmasını engeller.

**Dinamik ve Otomatik Kurtarma (Failover):** Aktif yollardan birinde fiziksel bir kopma veya cihaz arızası yaşandığında, STP saniyeler içinde durumu algılar. Daha önce bloke ettiği yedek hattı otomatik olarak aktif hale getirir. Bu sayede insan müdahalesine gerek kalmadan ağ kesintisiz çalışmaya devam eder.

**Radia Perlman Neden "İnternetin Annesi" Olarak Biliniyor?**

Yazılım geliştiricisi, ağ mühendisi ve akademisyen Radia Perlman, 1985 yılında DEC (Digital Equipment Corporation) bünyesinde çalışırken **Spanning Tree Algoritmasını** icat etti. Bu buluş, modern ağ dünyasının kurallarını kökten değiştirdi.

**Spanning Tree'nin Doğuşu:** Perlman'ın yöneticisi, ondan switch'lerin veriyi verimli bir şekilde aktarmasını sağlayacak ve döngüleri önleyecek basit bir protokol tasarlamasını istemişti. Perlman, sadece birkaç gün içinde hem algoritmayı geliştirdi hem de algoritmanın çalışma mantığını açıklayan ünlü **"Algoritm"** şiirini yazdı.

Perlman'a **"İnternetin Annesi" (Mother of the Internet)** unvanının verilmesinin temel nedenleri şunlardır:

Perlman'a **"İnternetin Annesi" (Mother of the Internet)** unvanının verilmesinin temel nedenleri şunlardır:

**1. Ethernet'i Ölçeklenebilir Kılmak:** Ethernet teknolojisi ilk çıktığında sadece çok küçük ağlarda çalışabiliyordu. Perlman'ın geliştirdiği STP, ethernet ağlarının devasa boyutlara ulaşabilmesini ve milyarlarca cihazın birbirine bağlanabilmesini sağladı.

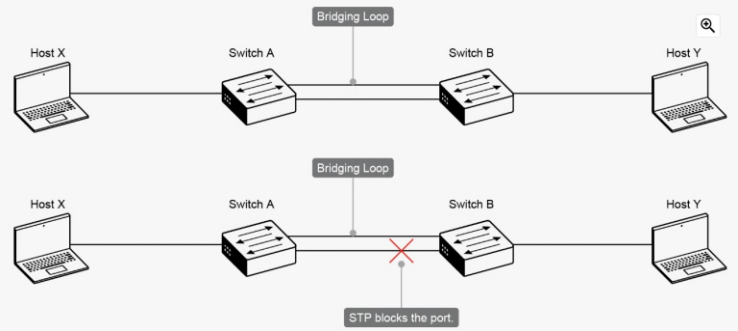
**2. Basitlik ve Güvenilirlik:** Tasarladığı algoritma o kadar sağlam ve zarifti ki, insan müdahalesi veya karmaşık yapılandırmalar gerektirmeden ağların kendi kendini yönetmesini sağladı. Bu durum, internetin emekleme döneminde kontrolsüzce büyümesini kolaylaştırdı.

**İnternet Yönlendirme Protokollerindeki Katkıları:** Perlman sadece STP ile yetinmedi; modern internet trafiğini yönlendiren **IS-IS (Intermediate System to Intermediate System)** protokolünün tasarlanmasında ve geliştirilmesinde de kilit rol oynadı. Ayrıca ağ güvenliği ve şifreleme üzerine yaptığı çalışmalarla internetin güvenli bir altyapıya kavuşmasını sağladı.

Bilineceği üzere Spanning Tree Protokol Birçok Switching Sertifikasyon programlarda tüm seviyeler (Temel, Profesyonel ve Expert) için yer almaktadır.

**CCNP Gözüyle Spanning Tree Protokolüne Giris**

STP, belirli ağ segmentlerine giden fiziksel yolları yöneterek döngülerin çözülmesini sağlar. Ağdaki aktif döngülerin (loop) istenmeyen etkilerini önlerken, fiziksel yol yedekliliğine imkan tanır. STP, belirli portları engelleme (blocking) durumuna geçmeye zorlar. Bu engellenen portlar veri çerçevelerini (data frames) iletmez.




Şekil 1 STPsiz ve STPli redundant switching topology

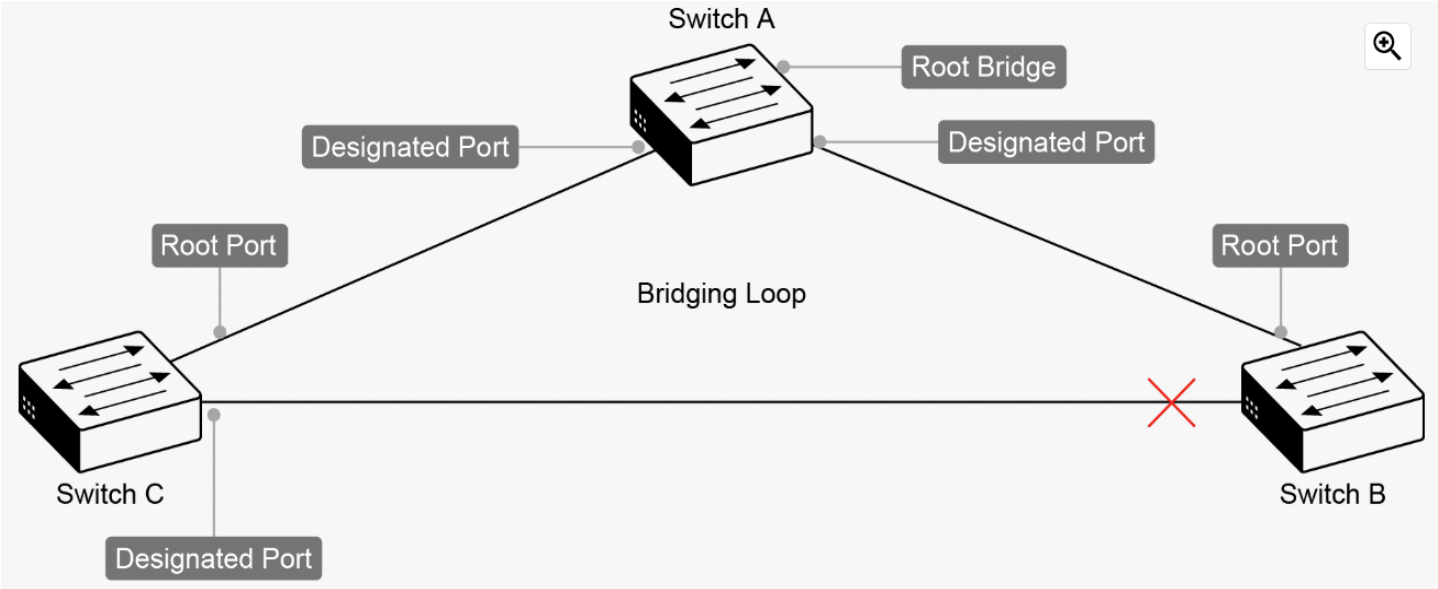
STP'siz anahtarlama topolojisinde şu problemlerle karşılaşırsınız

Yayın fırtınaları (Broadcast storms): Yedekli bir ağdaki her switch, yayın (broadcast) çerçevelerini durmaksızın basar (flooding yapar). Switch'ler, yayın çerçevelerini, çerçevenin alındığı port dışındaki tüm portlara dağıtır. Bu çerçeveler daha sonra döngü (loop) üzerinde her yöne doğru yayılır.

Çoklu çerçeve iletimi (Multiple frame transmission): Aynı tekli gönderim (unicast) çerçevelerinin birden fazla kopyası hedef istasyona ulaşabilir ve bu durum alıcı protokolde sorunlara yol açabilir. Birçok protokol, her iletimin yalnızca tek bir kopyasını almayı bekler. Aynı çerçevenin birden fazla kopyası, düzeltilemez (kurtarılamaz) hatalara neden olabilir.

MAC veri tabanı kararsızlığı (MAC database instability): Bu sorun, aynı çerçevenin kopyalarının switch'in farklı portlarından alınması sonucunda ortaya çıkar. MAC adres tablosu, alınan bir paketteki kaynak MAC adresini, paketin alındığı arayüzle (interface) eşleştirir. Eğer bir döngü meydana gelirse, aynı kaynak MAC adresi birden fazla arayüzde görülebilir ve bu durum kararsızlığa yol açar. Switch, MAC adres tablosundaki bu kararsızlıkla başa çıkmak için kaynaklarını tükettiğinde veri iletimi (data forwarding) sekteye uğrayabilir.

STPli TOPOLOGY




STP, aşağıdaki üç adımı gerçekleştirerek belirli ağ segmentine giden fiziksel yolu yönetir ve döngülerin çözülmesini sağlar:

1. **Bir kök köprü (root bridge) seçer:** Sadece tek bir köprü, kök köprü (root bridge) olarak görev yapabilir. Kök köprü referans noktasıdır ve ağdaki tüm veri akışları bu switch'in perspektifine (bakış açısına) göredir. Kök köprü üzerindeki tüm portlar trafiği iletir (forwarding durumundadır).
2. **Kök dışı köprüde (nonroot bridge) kök portunu (root port) seçer:** Kök dışı her bir köprüdeki bir port, kök portudur (root port). Bu port, kök dışı köprüden kök köprüye giden en düşük maliyetli yola sahip olan porttur. Varsayılan olarak STP yol maliyeti (path cost), bağlantının bant genişliğine göre hesaplanır. STP yol maliyetini manuel olarak da ayarlayabilirsiniz.
3. **Her segmentte atanmış portu (designated port) seçer:** Her segmentte bir adet atanmış port (designated port) bulunur. Bu port, kök köprüye en düşük maliyetli yola sahip olan köprü üzerinde seçilir.

Kök (root) veya atanmış (designated) olmayan portlar, atanmamış (nondesignated) port olmak zorundadır. Atanmamış portlar, döngü topolojisini kırmak için normal şartlarda engelleme (blocking) durumundadır. Genel sonuç olarak, herhangi bir anda her ağ segmentine giden yalnızca tek bir yol aktiftir. Ağ içindeki segmentlerden herhangi birine olan bağlantıda bir sorun yaşanırsa STP, eğer varsa daha önce pasif (aktif olmayan) bir yolu otomatik olarak aktif hale getirerek bağlantıyı yeniden kurar.

## STP Port Rolleri (STP Port Roles)

| Port Rolü (Port Role) | Açıklama (Description) |
|---|---|
| **Kök portu** *(Root port)* | Bu port kök dışı köprülerde (nonroot bridges) bulunur ve kök köprüye giden en iyi yola sahip olan switch portudur. Kök portları, trafiği kök köprüye doğru iletir. Kök portundan alınan çerçevelerin kaynak MAC adresleri, MAC tablosunu doldurma (öğrenme) yeteneğine sahiptir. Köprü (bridge) başına yalnızca bir adet kök portuna izin verilir. |
| **Atanmış port** *(Designated port)* | Bu port hem kök hem de kök dışı köprülerde bulunur. Kök köprüler için tüm switch portları atanmış porttur. Kök dışı köprüler için ise atanmış port; çerçeveleri alacak ve gerektiğinde kök köprüye doğru iletecek olan switch portudur. Segment başına yalnızca bir adet atanmış port bulunmasına izin verilir. Eğer aynı segment üzerinde birden fazla switch varsa, bir seçim süreci ile atanmış switch belirlenir ve ilgili switch portu o segment için çerçeveleri iletmeye başlar. Atanmış portlar, MAC tablosunu doldurma yeteneğine sahiptir. |
| **Atanmamış port** *(Nondesignated port)* | Atanmamış port, veri çerçevelerini iletmeyen (engelleyen / blocking durumunda olan) ve o segmentte görülen çerçevelerin kaynak adresleriyle MAC adres tablosunu doldurmayan bir switch portudur. |
| **Devre dışı port** *(Disabled port)* | Devre dışı port, kapatılmış (shut down edilmiş) olan bir switch portudur. |

**SONUÇ:**

***Bu yazımda Spanning Tree Protokolünün önemini anlatmaya çalıştım. Özellikle Protokolün nasıl çalıştığına dair bir tanıtım yapmaya çalıştım. Detaylandırmak ümidiyle!***

**YUSUF KÜÇÜK**
**Yusuf Küçük** yusufkucuk2014@gmail.com

# ADAPASS Vakası Üzerinden Bilgi Güvenliği: Teknik Bir Sorun mu, Yönetişim Meselesi mi?

***Son günlerde kamuoyuna yansıyan ve pandemi döneminde kullanılan ADAPASS sistemiyle ilişkili olduğu iddia edilen veri sızıntısı, bilgi güvenliği konusunu yeniden gündemimize taşıdı. Konuyla ilgili teknik incelemeler ve resmi değerlendirmeler devam ederken, bu vaka hepimize daha temel bir soruyu sorma fırsatı veriyor:***

**Bir bilgi güvenliği olayı yaşandığında ilk sorumuz "Sistem nasıl hacklendi?" mi olmalıdır, yoksa "Bu risk neden yönetilemedi?" mi?**

Bilgi güvenliği ve mahremiyet yönetim sistemi perspektifinden bakıldığında, ikinci soru çoğu zaman daha anlamlıdır. Bilgi güvenliği olaylarının ardından ilk refleks çoğu zaman teknik ekipleri veya kullanılan teknolojileri sorgulamak olur. Oysa yönetim sistemi yaklaşımında asıl sorgulanan kişiler değil; süreçler, sorumluluklar ve karar mekanizmalarıdır. Bu yazının amacı da herhangi bir teknik ekibi eleştirmek değil, benzer olaylardan bütün kurumların çıkarabileceği yönetişim derslerini tartışmaktır.

**Siber Güvenlik ile Bilgi Güvenliği Aynı Şey Değildir**

Kamuoyunda bu iki kavram çoğu zaman birbirinin yerine kullanılır. Oysa aralarında önemli bir fark vardır. Siber güvenlik; ağların, sistemlerin ve dijital altyapının dış tehditlere karşı korunmasına odaklanan teknik bir disiplindir. Bilgi güvenliği ise daha geniş bir kavramdır — dijital olan veya olmayan tüm bilgi varlıklarını kapsar; yalnızca teknik kontrolleri değil, politikaları, süreçleri, insan faktörünü ve yönetim sorumluluğunu da içerir.

Bir sistem siber saldırıya uğramamış olabilir; ancak yanlış kişilere erişim yetkisi verilmişse, eski kullanıcı hesapları kapatılmamışsa veya kişisel veriler gereğinden uzun süre saklanmışsa, bilgi güvenliği yine de ihlal edilmiş demektir. ADAPASS vakasında da asıl sorgulanması gereken yalnızca teknik altyapının dışarıdan ihlal edilip edilmediği değil; risklerin kurum içinde nasıl yönetildiğidir.

**Bilgi Güvenliği Önce Bir Yönetişim Meselesidir**

Kamuoyunda bilgi güvenliği çoğu zaman güvenlik duvarları, antivirüs yazılımları ve teknik uzmanlarla ilişkilendirilir. Elbette bunlar önemlidir. Ancak ISO/IEC 27001 ve ISO/IEC 27701 gibi uluslararası yönetim sistemi standartları, bilgi güvenliğini öncelikle bir yönetişim ve liderlik konusu olarak ele alır. Güvenliğin sürdürülebilir olması için üst yönetimin bilgi güvenliği politikasını sahiplenmesi, sorumlulukları açık şekilde tanımlaması, gerekli kaynakları sağlaması ve riskleri düzenli olarak gözden geçirmesi beklenir.

Burada önemli bir noktanın altını çizmek gerekir: Hiçbir yönetim sistemi standardı tek başına güvenliği garanti etmez. ISO/IEC 27001'in değeri, teknik kontrollerin yerine geçmesinde değil; güvenliği planlayan, yöneten, denetleyen ve sürekli geliştiren kurumsal bir yapı sunmasındadır.

**Teknik Ekipler Değil, Yönetişim Boşlukları Sorgulanmalıdır**

Bilgi güvenliği olaylarından sonra çoğu zaman ilk eleştirilen taraf teknik ekipler olur. Oysa uygulamada bilgi işlem ekipleri ve sistem yöneticileri mevcut risklerin büyük bölümünün farkındadır. Hangi sistemin güncellenmesi gerektiğini, hangi kullanıcı hesabının kapatılması gerektiğini, hangi verinin artık tutulmaması gerektiğini bilirler. Ancak bu tespitleri kurumsal karara dönüştürecek yetki, bütçe veya yönetsel destek bulunmadığında yapabilecekleri sınırlı kalır.

Bilgi güvenliği yönetişimi yalnızca bilgi işlem biriminin sorumluluğu değildir. Üst yönetimden süreç sahiplerine, insan kaynaklarından hukuk birimine kadar tüm organizasyonun ortak sorumluluğunu gerektirir. Teknik ekiplerin başarısı da çoğu zaman bu kurumsal desteğin varlığına bağlıdır.

**ADAPASS örneğinde de asıl sorgulanması gereken soru şudur: Riskler görüldü mü değil — görüldüyse nasıl yönetildi?**

**Dışarıdan Temin Edilen Sistemler Özel Bir Risk Taşır**

25 yılı aşkın deneyimim ve onlarca kamu ile özel sektör projesinde edindiğim gözlemlere dayanarak şunu rahatlıkla söyleyebilirim: Dışarıdan temin edilen sistemlerde en sık karşılaşılan risklerden biri, sözleşme sona erdiğinde ortaya çıkar. Sistem teslim edilmiştir, proje kapanmıştır — ama teknik devir, dokümantasyon ve sürekli bakım sorumluluğu net tanımlanmamışsa, sistem zamanla sahipsiz kalır. Ne tedarikçinin artık yasal bir yükümlülüğü vardır, ne de kurum içinde tam anlamıyla sahiplenen biri. Sistem çalışmaya devam eder — ama artık kimsenin sorumluluğunda değildir.

Bu risk uluslararası standartlar tarafından da açıkça tanımlanmıştır. ISO/IEC 27001, tedarikçi sözleşmelerinde güvenlik gereksinimlerinin açıkça belirlenmesini, hizmet süresince izlenmesini ve sözleşme sona erdiğinde sistemin güvenli biçimde devredilmesini veya sonlandırılmasını şart koşar. ADAPASS bağlamında sorulması gereken sorulardan biri de budur: Tedarikçi ilişkisi sonlandığında sistem devri nasıl yönetildi?

**Çalışan Sistem Her Zaman Yönetilen Sistem Anlamına Gelmez**

Birçok kurumda günlük operasyonların kesintisiz devam etmesi öncelik kazanır. Sistem çalışıyor, vatandaş hizmet alabiliyor, iş süreçleri devam ediyor — bu sorulara olumlu cevap verildiğinde güvenliğin de sağlandığı algısı oluşur. Ancak bilgi güvenliği yönetimi farklı bir soru sorar: Bu sistem güvenli, ölçülebilir ve sürdürülebilir şekilde yönetiliyor mu?

ADAPASS da pandemi döneminde önemli bir ihtiyaca cevap vermiştir. Ama kriz sona erdikten sonra yaşam döngüsü yönetildi mi, kullanıcı hesapları gözden geçirildi mi, erişim yetkileri güncellendi mi? Bu sorular teknik değil, yönetişim sorularıdır. Yalnızca kamu

kurumlarına da özgü değildir — benzer tablolarla özel sektörde de sıkça karşılaşılmaktadır.

**Sorun yaşanmamış olması, risklerin yönetildiği anlamına gelmez.**

**Güvenlik Görünmez Olduğu İçin İkinci Plana Düşebilir**

Bilgi güvenliği faaliyetlerinin önemli bir bölümü görünmezdir — başarılı olduklarında manşet olmazlar, çünkü hiçbir şey yaşanmamıştır. Bu nedenle operasyonel öncelikler çoğu zaman güvenliğin önüne geçer. "Sunucu eski ama çalışıyor", "loglar incelenmedi ama sorun yaşanmadı", "eski sistem hâlâ açık ama kimse kullanmıyor" — bu tür geçici kabuller zaman içinde kalıcı risklere dönüşür.


Bilgi güvenliği, görünmez olduğu için değersiz değildir. Tam tersine, ihmal edildiğinde en görünür sonuçları doğuran yönetişim disiplinlerinden biridir.

**Güvenlik Kişilere Bağımlı Olamaz**

Personel değişir, görev değişiklikleri olur, emeklilik gelir. Peki süreçler aynı güvenlik seviyesinde devam edebiliyor mu? Bir sistem belirli kişilerin bilgi ve deneyimine bağımlı hale geldiyse, orada teknik değil yönetsel bir risk oluşmuş demektir. Kurumsal hafıza insanların zihninde değil, süreçlerde ve yönetim sistemlerinde yaşamalıdır. ISO/IEC 27001'in temel yaklaşımlarından biri de tam olarak budur.

**Kişisel Verilerin de Bir Yaşam Döngüsü Vardır**

Bilgi güvenliği yalnızca verileri toplamak ve saklamak değildir. Her verinin bir yaşam döngüsü vardır: toplanır, işlenir, saklanır, paylaşılır, arşivlenir ve zamanı geldiğinde güvenli biçimde imha edilir. ADAPASS örneği üzerinden düşünüldüğünde sorulması gereken sorular şunlardır: Sistem artık gerekli miydi? Saklama süreleri belirlenmiş miydi? Gereksiz veriler imha edildi mi? Eski kullanıcı hesapları kapatıldı mı? Bu sorular yalnızca ADAPASS için değil, kişisel veri işleyen her kurum için geçerlidir.

**PUKÖ Döngüsü Neden Bu Kadar Önemlidir?**

Yönetim sistemi standartlarının merkezinde sürekli iyileştirme anlayışı yer alır. Planla: Ne topluyoruz, neden topluyoruz, kim sorumlu? Uygula: Kontrolleri kur, rolleri belirle, yetkileri tanımla. Kontrol Et: Riskler değişti mi, sistem hâlâ gerekli mi, loglar inceleniyor mu, eski hesaplar kapatıldı mı? Önlem Al: İyileştir, güncelle, kapat, imha et.

Çünkü riskler hiçbir zaman sabit değildir. Teknoloji değişir, iş ihtiyaçları değişir, personel değişir, sistemler eskir. Bilgi güvenliği bir kez kurulup unutulabilecek bir yapı değildir.

**PUKÖ döngüsü durduğu anda riskler sessizce birikmeye başlar.**

**Bu Vaka Bize Ne Hatırlatıyor?**

Bir bilgi güvenliği olayının ardından yalnızca "hangi teknik açık kullanıldı?" sorusuna odaklanmak yeterli değildir. Riskler nasıl yönetiliyordu, roller ve sorumluluklar açık mıydı, kararlar nasıl alınıyordu, süreçler düzenli gözden geçiriliyordu muydu — bu soruların da cevaplanması gerekir.

Çünkü güvenlik açıkları çoğu zaman tek bir teknik hatadan değil, zaman içinde biriken yönetişim boşluklarından doğar. Eski kullanıcı hesabının kapatılmaması, test ortamının unutulması, şifrelenmeyen yedekler, incelenmeyen erişim logları — bunların her biri tek başına küçük görünebilir. Bir araya geldiklerinde ciddi bir tablo oluşturabilirler.

**Sonuç**

Bilgi güvenliği birkaç teknik önlemden ibaret değildir. Sürdürülebilir güvenlik; liderlik, politika, süreç sahipliği, kaynak tahsisi, risk yönetimi ve sürekli iyileştirme yaklaşımının birlikte işlemesini gerektirir.

Kurumların bilgi güvenliği olgunluğunu değerlendirmenin ilk adımı, yalnızca teknik kontrolleri değil; bu kontrolleri yöneten süreçleri, sorumlulukları ve karar mekanizmalarını sorgulamaktır.

Çünkü sürdürülebilir bilgi güvenliği yalnızca teknolojiyle değil, iyi yönetişimle mümkündür. ISO/IEC 27001 ve ISO/IEC 27701 gibi uluslararası standartların kurumsal değeri de tam olarak burada ortaya çıkar: Güvenliği bireylerin iyi niyetine ya da kurumların talihine bırakmadan; ölçülebilir, denetlenebilir ve sürdürülebilir bir yönetim kabiliyetine dönüştürmek.

*Bu yazı, kamuya yansıyan bilgiler ışığında hazırlanmış etik bir vaka değerlendirmesidir. Olayın teknik ve hukuki boyutlarına ilişkin resmi incelemeler devam ederken, amaç belirli bir kurum, teknik ekip veya yöneticiyi değerlendirmek değil; benzer olaylardan tüm kurumların çıkarabileceği yönetişim derslerini tartışmaktır.*

**Erkan Emirzade**
Bilgisayar Mühendisi

# Dijital Egemenlik: Bir Ülke Sadece Topraklarını mı Korur?

## 21. Yüzyılda Devletlerin Görünmeyen Sınırları Üzerine Bir Değerlendirme

### Dijital Gelecek Yazıları / Bölüm 1

Geçmişte devletlerin gücü sahip oldukları topraklar, doğal kaynaklar ve askeri kapasiteleri ile ölçülürdü. Günümüzde ise görünmeyen yeni sınırlar oluşmuştur. Fiber optik kablolar, veri merkezleri, bulut sistemleri, yapay zekâ algoritmaları, dijital kimlikler ve kritik bilgi altyapıları artık bir ülkenin egemenliğinin ayrılmaz parçalarıdır.

Bir ülkenin bankacılık sistemi, sağlık altyapısı, e-Devlet hizmetleri, enerji yönetimi ve haberleşme ağları dijital ortamda çalışıyorsa, bu sistemlerin güvenliği yalnızca teknik bir konu değil, doğrudan millî kapasite, ekonomik sürdürülebilirlik ve toplumsal güven meselesidir.

Dijital egemenlik kavramı tam da bu noktada ortaya çıkmaktadır. Dijital egemenlik: bir ülkenin kendi verisini yönetebilmesi, kritik dijital altyapılarını güvenli ve sürdürülebilir biçimde işletebilmesi, teknolojik kararlarını kendi önceliklerine göre alabilmesi ve vatandaşlarının dijital haklarını koruyabilmesidir. Bu kavram teknolojik izolasyon veya mutlak bağımsızlık anlamına gelmez; aksine küresel teknolojilerden yararlanırken ulusal kapasiteyi geliştirebilmeyi ve bağımlılık risklerini yönetebilmeyi ifade eder.


***Dünyadan Örnekler ve Çıkarımlar***

Dünya genelindeki başarılı uygulamalar, dijital egemenliğin yalnızca yazılım veya donanım satın almaktan ibaret olmadığını; uzun vadeli vizyon, insan kaynağı ve koordinasyon gerektirdiğini göstermektedir:

- ✓***Estonya:*** Dijital kimlik ve e-Devlet altyapısıyla kamu hizmetlerinin neredeyse tamamını çevrim içi sunmaktadır.
- ✓***Singapur:*** Smart Nation vizyonu ile ileri teknolojiyi, ağları ve büyük veriyi günlük yaşamın ve kentsel yönetimin merkezine yerleştirmiştir.
- ✓***Finlandiya:*** Toplumun tamamına yönelik yapay zekâ ve dijital okuryazarlık eğitimleri açarak doğrudan insan kaynağına yatırım yapmıştır.
- ✓***Avrupa Birliği:*** GAIA-X girişimiyle, küresel teknoloji devlerine bağımlılığı azaltmak adına veri egemenliği ve güvenilir federatif bulut altyapıları konusunda ortak standartlar geliştirmektedir.
- ✓***Ukrayna:*** Savaş koşullarında dahi dijital kamu hizmetlerini sürdürebilmenin ulusal dayanıklılık ve kriz yönetimi açısından ne kadar hayati olduğunu tüm dünyaya kanıtlamıştır.
- ✓***Türkiye:*** Son yirmi yılda dijital dönüşüm alanında önemli bir mesafe kat etmiştir. Bugün milyonlarca vatandaşın aktif olarak kullandığı e-Devlet Kapısı, kamu hizmetlerinin tek noktadan ve güvenli biçimde sunulmasına yönelik başarılı örneklerden biridir. Bunun yanında Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve kurumlar bünyesinde oluşturulan SOME yapılanmaları, ulusal ölçekte siber olayların izlenmesi ve koordinasyonunda önemli bir görev üstlenmektedir. Son yıllarda TEKNOFEST gibi organizasyonlarla gençlerin teknoloji üretimine yönlendirilmesi, savunma sanayisindeki dijital dönüşüm ve yerli yazılım ekosisteminin gelişmesi de dijital egemenliğin yalnızca teknoloji satın almakla değil, insan kaynağı yetiştirmek ve sürdürülebilir bir inovasyon kültürü oluşturmakla mümkün olduğunu göstermektedir. Elbette her ülkenin ihtiyaçları ve ölçeği farklıdır; ancak bu örnekler, KKTC'nin kendi koşullarına uygun bir dijital dönüşüm modeli oluşturması açısından önemli deneyimler sunmaktadır.

***KKTC İçin Yol Haritası ve Fırsatlar***

➢***KKTC'nin Güçlü Yönleri ve Gelişim Alanları***

KKTC, dijital egemenlik açısından düşünüldüğünde önemli avantajlara da

sahiptir. Yüksek internet kullanım oranı, bilişim alanında eğitim veren çok sayıdaki üniversite, genç ve teknolojiye yatkın nüfus, dijital bankacılık uygulamalarının yaygınlığı ve kamu hizmetlerinde devam eden dijitalleşme çalışmaları bu avantajların başında gelmektedir. Özellikle bilişim alanında yetişen insan kaynağı, ülkemizin en değerli stratejik kaynaklarından biridir.

Bununla birlikte, geliştirilmesi gereken alanlar da bulunmaktadır. Kritik altyapılara yönelik ortak güvenlik standartlarının oluşturulması, ulusal ölçekte veri yönetimi politikalarının belirlenmesi, afet ve kriz senaryolarına yönelik yedekli veri merkezlerinin planlanması, kurumlar arası veri paylaşım standartlarının geliştirilmesi, yapay zekâya yönelik ulusal politika belgelerinin hazırlanması ve siber güvenlik alanındaki kurumsal koordinasyonun güçlendirilmesi, dijital egemenliğin sürdürülebilirliği açısından önümüzde duran önemli başlıklardır. Bu eksiklikler bir zafiyet olarak değil, planlı çalışmalarla geliştirilebilecek stratejik fırsatlar olarak değerlendirilmelidir.

Kuzey Kıbrıs Türk Cumhuriyeti özelinde düşündüğümüzde, kamu hizmetlerinin dijitalleşmesi, e-Devlet uygulamalarının yaygınlaşması, üniversitelerin bilişim alanındaki büyümesi ve telekom/fiber optik altyapı yatırımlarının gündeme gelmesi çok önemli stratejik fırsatlar sunmaktadır.

Ancak dijital egemenlik yalnızca sunucu veya yazılım satın almak, güvenlik duvarı kurmaktan ibaret değildir. Doğru mevzuatların hazırlanması, nitelikli mühendislik standartlarının oluşturulması, kurumlar arası koordinasyonun sağlanması, afet ve kriz senaryolarına yönelik yedeklilik politikalarının geliştirilmesi süreçlerin ayrılmaz parçalarıdır.

Bugün herhangi bir kamu kurumunda yaşanabilecek uzun süreli bir siber kesinti yalnızca teknik bir arıza değildir. Sağlık hizmetleri aksayabilir, ekonomik işlemler durabilir, vatandaş-devlet ilişkisi zedelenebilir. Bu nedenle dijital dayanıklılık fiziksel altyapı kadar kritiktir.

Önümüzdeki dönemde dijital egemenlik başlığı altında önceliklendirilmesi gereken temel konular şunlardır:

- Ulusal siber güvenlik stratejisinin hazırlanması.
- Kritik altyapılar için ortak güvenlik standartlarının oluşturulması.
- Veri merkezlerinin ve yedeklilik politikalarının güçlendirilmesi.
- Dijital kimlik ve kişisel verilerin korunmasına yönelik güncel düzenlemeler.
- Yapay zekâ kullanımında etik ve hukuki çerçevenin oluşturulması.
- Üniversite, kamu ve özel sektör iş birliklerinin artırılması.
- Genç mühendislerin ülkede üretim yapmasını destekleyecek ekosistemin geliştirilmesi.
- Dijital okuryazarlığın okul öncesinden başlayarak toplumun tüm kesimlerine yayılması.

***Dijital Egemenlik Kimi İlgilendiriyor?***

Dijital egemenlik yalnızca devlet kurumlarını ilgilendiren teknik bir kavram değildir. Günümüzde dijital dünyanın bir parçası olan herkes bu sürecin doğal paydaşıdır. Bireyler açısından kişisel verilerin korunması, güvenli dijital kimlik kullanımı ve bilinçli internet alışkanlıkları önem taşırken, özel sektör açısından müşteri verilerinin korunması, iş sürekliliği ve rekabet gücü öne çıkmaktadır. Kamu kurumları için güvenilir e-Devlet hizmetleri, kritik altyapıların korunması ve kesintisiz kamu hizmeti temel önceliklerdir. Meslek odaları, üniversiteler ve sivil toplum kuruluşları ise teknik standartların geliştirilmesi, etik ilkelerin oluşturulması, nitelikli insan kaynağının yetiştirilmesi ve toplumsal farkındalığın artırılması noktasında önemli sorumluluklar üstlenmektedir. Dijital egemenlik ancak tüm bu paydaşların ortak katkısıyla güçlenebilir.

***Meslek Örgütlerinin Rolü ve Sorumluluğu***

Bilgisayar mühendisleri bu dönüşümün merkezinde yer almaktadır. Bizler yalnızca yazılım geliştiren veya sistem yöneten profesyoneller değil, aynı zamanda toplumun dijital geleceğini planlayan, riskleri analiz eden mühendisleriz.

KTMMOB Bilgisayar Mühendisleri Odası olarak son yıllarda güvenli internet, siber güvenlik, dijital farkındalık ve bilinçli teknoloji kullanımı konularında öğrencilerden kamu çalışanlarına, belediyelerden 60 yaş üstü bireylere kadar çok geniş bir kesime yönelik eğitimler gerçekleştirdik. Bunun yanında kamu politikalarına katkı sağlayacak teknik görüşler hazırlamaya, karar vericilere yapıcı öneriler sunmaya devam ediyoruz.

Amacımız eleştirmekten ziyade çözüm üretmek ve teknolojiyi toplum yararına kullanacak ortak bir vizyon geliştirmektir.

***Yapay Zekâ Çağına Hazırlık***

Bugün dijital egemenliği konuşurken aslında yarının yapay zekâ çağını da konuşuyoruz. Çünkü yapay zekâ sistemlerinin başarısı, sahip olunan verinin kalitesine, güvenilirliğine ve yönetimine doğrudan bağlıdır. Verisini yönetemeyen toplumlar, gelecekte yapay zekâyı yalnızca tüketen konumda kalacak; verisini güvenli biçimde yöneten toplumlar ise teknolojiyi geliştiren ve yönlendiren ülkeler arasında yer alacaktır. Bu nedenle dijital egemenlik ile yapay zekâ stratejileri birbirinden ayrı düşünülemeyecek kadar güçlü bir ilişki içerisindedir.

***Ortak Bir Vizyon İhtiyacı***

Tüm bu değerlendirmeler ışığında, ülkemizin uzun vadeli hedeflerini ortaya koyacak kapsamlı bir ***"Ulusal Dijital Egemenlik Strateji Belgesi"*** hazırlanmasının faydalı olacağı kanaatindeyim.

Böyle bir belge, siber güvenlikten yapay zekâya, veri yönetiminden dijital kimliğe, fiber optik altyapılardan insan kaynağı planlamasına kadar farklı alanları ortak bir vizyon altında buluşturabilir. Böylece kurumlar birbirinden bağımsız hareket etmek yerine aynı hedef doğrultusunda ilerleyebilir ve ülkemizin dijital geleceği daha planlı, sürdürülebilir ve bütüncül bir yaklaşımla şekillendirilebilir.

***Sonuç ve Geleceğe Bakış***

Dijital egemenlik nihai bir hedef değil, sürekli geliştirilmesi gereken dinamik bir kapasite ve yolculuktur. Unutulmamalıdır ki güçlü toplumlar yalnızca teknolojiyi tüketen değil, teknolojiyi geliştiren, yöneten, denetleyen ve güvenli hâle getiren toplumlardır. Bir ülkenin gerçek bağımsızlığı yalnızca sınır kapılarında değil, veri merkezlerinde, yazılım laboratuvarlarında, mühendislik ofislerinde ve bilgi üreten kurumlarında da şekillenir.

Bu makale ile birlikte BTKıbrıs dergisinde yeni bir yazı dizisine başlıyorum. Önümüzdeki sayılarda, yapay zekânın kamu yönetimine etkileri, veri egemenliği, dijital kimlik, kritik altyapılar, akıllı şehirler, dijital

çocuk hakları, fiber optik altyapılar, siber dayanıklılık ve "KKTC Dijital Gelecek Vizyonu 2035" gibi başlıkları derinlemesine birlikte değerlendireceğiz.

Dijital geleceği inşa etmek yalnızca teknoloji yatırımı yapmakla mümkün değildir; bilim, mühendislik, eğitim, hukuk ve toplumsal bilinç birlikte ilerlemelidir. Bugün atacağımız doğru adımlar, çocuklarımızın ve gelecek nesillerimizin de ortak mirası olacak daha dirençli bir dijital toplumu oluşturacaktır.

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

# Meta'nın yapay zeka faturası kabardı: Nakit akışı yüzde 91 düştü

***Meta'nın gelirleri ve kullanıcı sayısı artmayı sürdürse de yapay zekaya yapılan dev yatırımlar şirketin serbest nakit akışını ciddi şekilde düşürdü. Meta yine de harcama hedefini yükseltti.***

Meta, 2026'nın ikinci çeyreğine ilişkin finansal sonuçlarını açıkladı. Şirketin gelirleri ve kullanıcı sayısı güçlü artışlar yaşamış olsa da yapay zeka altyapısına yapılan milyarlarca dolarlık yatırımlar serbest nakit akışında sert düşüşe neden oldu. Ancak şirket yine de gelecek yıla yönelik sermaye harcaması beklentisini de yukarı yönlü revize etti.


İkinci çeyrek verilerine göre Meta'nın serbest nakit akışı geçen yılın aynı dönemindeki 8,55 milyar dolar seviyesinden yüzde 91 düşerek 784 milyon dolara geriledi. Finansal sonuçların ardından Meta hisseleri, seans sonrası işlemlerde yaklaşık yüzde 10 değer kaybetti.

### Zuckerberg kendinden emin

Meta CEO'su Mark Zuckerberg, şirketin bilgi işlem kapasitesinin önemli bölümünün yapay zeka modellerinin eğitimi, ana faaliyetlerin büyütülmesi, kişisel yapay zeka asistanlarının geliştirilmesi ve yeni ürünlerin oluşturulması için kullanılacağını söyledi.

Zuckerberg ayrıca Meta'nın büyük kurumsal müşterilere yönelik önemli bir yapay zeka işi kurmayı hedeflediğini belirtti. CEO, şirketin bugünkü yüksek harcamalarının, kişisel yapay zeka ajanlarının gelecekte büyük bir tüketici pazarı oluşturacağı beklentisine dayandığını ifade etti.

### AI harcamaları hız kesmiyor

Bu kapsamda Meta'nın AI yatırımları da hız kesmiyor. Şirket, 2026 yılı sermaye harcaması beklentisinin alt sınırını 125 milyar dolardan 130 milyar dolara yükseltti. Üst sınır ise 145 milyar dolar olarak korundu.

Reuters'ın daha önce aktardığı bilgilere göre şirket, toplam bilgi işlem kapasitesini bu yıl 7 gigavata, gelecek yıl ise 14 gigavata çıkarmayı hedefliyor. Meta'nın dünya genelinde faaliyette olan veya inşası süren 32 veri merkezi bulunuyor.

Yüksek yatırım harcamalarına rağmen Meta'nın temel reklam faaliyetleri güçlü performans göstermeyi sürdürdü. Şirketin ikinci çeyrek geliri yıllık bazda yüzde 28 artarak 60,8 milyar dolara yükseldi. Net gelir ise 15,85 milyar dolar oldu.

Meta'nın uygulamalarını kullanan günlük aktif kullanıcı sayısı da yüzde 3 artışla 3,6 milyara ulaştı.

### Hukuki riskler de devam ediyor

Meta, finansal sonuçlarla birlikte devam eden hukuki süreçlere ilişkin uyarılarını yineledi. Şirket, bu ay mahkemeye sunduğu belgelerde ABD'deki dört eyaletin, Facebook ve Instagram'ın genç kullanıcıları bağımlı hale getirdiği ve platformların güvenliği konusunda kamuoyunu yanılttığı iddialarıyla 1,4 trilyon dolarlık ceza talep ettiğini açıkladı. Meta ayrıca Avrupa Birliği ve ABD'de gençlerin sosyal medya kullanımıyla ilgili düzenleyici baskının sürdüğünü belirtti. - Kaynak: donanimhaber.com

# Röportaj: Gençlerle Yapay Zekâ


***Her çağın kendine özgü bir dönüşümü vardır. Günümüzün en büyük dönüşümlerinden biri olan yapay zekâ, özellikle teknolojinin içinde büyüyen gençlerin yaşamını ve geleceğe bakışını şekillendiriyor.***

***Peki gençler yapay zekâ hakkında ne düşünüyor? Onlar için yapay zekâ ne ifade ediyor? Bu soruların cevaplarını bulmak için farklı gençlerle bir araya gelerek yapay zekâ üzerine keyifli bir röportaj gerçekleştirdim. Gelin, yapay zekâyı gençlerin gözünden birlikte keşfedelim.***

**1. Yapay zekâyı tek bir cümleyle nasıl tanımlarsın? Ona bir isim versen ne ad verirdin?**

**Defne Ceylan**
"İnsanın zihnini ve üretkenliğini katlayan ama ruhu olmayan süper hızlı bir iş ortağı." Destekleyiciliği sonsuz ama asıl oyuncu yine insan bu nedenle ona "'Yedek Oyuncu.' Adını verirdim.

**Eray Okuşluğ**
"Gün içinde yanımda bulunan yol arkadaşı. 'AKIL' veya 'YOLDAŞ'.

**Kemal Saygılı**
"Gündelik yaşamı kolaylaştırmak." "'AETHER.' Bilgiyi, yeniliği ve sınırsız gelişimi temsil ettiği için."

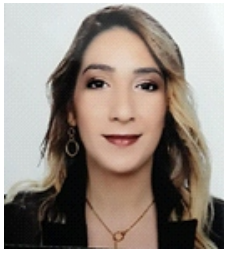
**2. Günlük hayatta yapay zekâyı en çok nerede kullanıyorsun?**

**Defne Ceylan**
"Proje geliştirirken elim ayağım gibi. Beyin fırtınası yapmak istediğimde veya mantık yürütemediğim bir noktada ikinci bir kafa gibi kullanıyorum."

**Eray Okuşluğ**
"Gündelik hayatta en çok yazılım ve teknoloji alanında kullanıyorum."

**Kemal Saygılı**
"Çoğunlukla okul için, bunun dışında merak ettiğim konuları araştırmak için kullanıyorum."

*Gençlerin cevapları, yapay zekânın artık yalnızca geleceğin teknolojisi olmadığını, günlük yaşamın ve eğitimin önemli bir parçası hâline geldiğini gösteriyor. Kimi onu bir "yol arkadaşı", kimi ise üretkenliği artıran bir "düşünme ortağı" olarak görüyor. Ortak nokta ise yapay zekânın hayatı kolaylaştıran güçlü bir yardımcı olduğu düşüncesinde ilerliyor.*



**3. Yapay zekânın insanlardan daha iyi yapabileceği bir şey var mı? Peki insanların daha iyi yapacağı?**

**Defne Ceylan**
"Veriyi saniyeler içinde işlemek, tekrarlayan görevleri hatasız yapmak ve karmaşık algoritmaları çalıştırmakta yapay zekâ çok daha iyi. Ama empati kurmak, özgün duygular hissetmek ve kriz anlarında sezgiyle karar vermekte insanlar her zaman öndedir."

**Eray Okuşluğ**
"Veri analizi ve sayısal işlemlerde yapay zekâ daha başarılı. Yaratıcılık ve duygusal zekâ ise insanların güçlü olduğu alanlar."

**Kemal Saygılı**
"Yapay zekâ hız konusunda öne çıkıyor ve bilgiye hızlı ulaşmayı sağlıyor. Ancak insanlığın önemini kaybetmemesi için kendimizi geliştirmemiz gerekiyor."

**4. Yapay zekâyla ilgili seni en çok heyecanlandıran ve aynı zamanda endişelendiren şey nedir?**

**Defne Ceylan**
*"Beni en çok heyecanlandıran şey, aklımdaki bir fikri ya da tasarımı haftalarca uğraşmadan saatler içinde somut bir hâle dönüştürebilmek. Ancak insanların düşünmeyi bırakıp her şeyi hazır beklemesi, problem çözme becerilerimizin zamanla körelmesi ise beni endişelendiriyor."*

**Eray Okuşluğ**
*"Yapay zekânın her geçen gün daha neler yapabileceğini görmek ve hangi konularda daha fazla yardımcı olacağını keşfetmek beni heyecanlandırıyor. Buna karşılık, arka planda neler olduğunu ve bize açıklanmayan özelliklerin bulunmasını bilmemek ise düşündürücü ve endişe verici geliyor."*

**Kemal Saygılı**
*"Müzikle ilgilenen biri olarak yazdığım şarkı sözlerini yapay zekâ sayesinde sevdiğim tarzda gerçek bir şarkıya dönüştürebilmek beni heyecanlandırıyor. Ancak yapay zekâ ile oluşturulan gerçekçi görsellerin ve videoların insanları yanıltabilecek düzeye ulaşması da en büyük endişelerimden biri."*

*Yapay zekâ söz konusu olduğunda gençlerin bakış açısı tek yönlü değil. Cevaplar, bu teknolojinin sunduğu fırsatların heyecan uyandırdığını; ancak etik sorunlar, bilgi güvenliği ve insanın düşünme becerilerini köreltebileceği endişesinin de göz ardı edilmediğini ortaya koyuyor.*

**5. Yapay zekâya güveniyor musun? Hangi konularda güvenmezsin?**

**Defne Ceylan**
"Teknik konularda güveniyorum. Ancak etik, empati ve doğruluğunu teyit etmediğim bilgiler konusunda asla tamamen güvenmem."

**Eray Okuşluğ**
"Genel olarak güveniyorum ancak özel ve ailevi bilgilerimi paylaşmam."

**Kemal Saygılı**
"Hayatımı kolaylaştırdığı için güveniyorum. Ancak sahte görseller, tehdit ve kötüye kullanım gibi konularda güven kaybı yaşıyorum."

**6. On yıl sonra yapay zekânın hayatımızı nasıl değiştireceğini düşünüyorsun?**

**Defne Ceylan**
"Rutin işleri yapay zekâ üstlenecek, insanlar ise fikir üreten ve yön veren konuma gelecek."

**Eray Okuşluğ**
"Hayatımızı kökten değiştirecek. Özellikle teknoloji ve yazılım alanında değişim çok daha belirgin olacak."

**Kemal Saygılı**
"Hayatımızın büyük bölümünde yapay zekâ yer alacak ve bazı mesleklerin yerini alabilecek."

**7. Yapay zekâyı bilinçli kullanmak için öğrencilere neler öğretilmeli?**

**Defne Ceylan**
"Doğru soru sormayı öğrenmeli ve yapay zekânın bir ödev aracı değil, düşünme ortağı olduğu anlatılmalı."

**Eray Okuşluğ**
"Yapay zekânın nasıl çalıştığı, ürettiği bilgilerin doğrulanması gerektiği ve güvenilir bilgiye ulaşma yöntemleri öğretilmeli."

**Kemal Saygılı**
"Amaca uygun kullanım ve yapay zekâya doğru komut vermenin önemi öğretilmeli."

*Röportaj boyunca verilen cevaplar, gençlerin yapay zekâya ne kayıtsız kaldığını ne de sorgusuz sualsiz teslim olduğunu gösteriyor. Onlar için yapay zekâ; doğru kullanıldığında öğrenmeyi, üretmeyi ve gelişmeyi destekleyen önemli bir araç. Ancak bu gücün bilinçli, etik ve eleştirel bir yaklaşımla kullanılması gerektiği konusunda ortak bir farkındalık da dikkat çekiyor.*

Biz bu çalışma süresince çok keyif aldık umarım sizlerde ayni şekilde keyif almışsınızdır. Görüş ve deneyimlerini samimiyetle paylaşan genç meslektaş adaylarıma en içten teşekkürlerimi sunarım.

*Defne Ceylan - Yakın Doğu Üniversitesi – Yazılım Mühendisliği Bölümü 4.Sınıf*
*Eray Okuşluğ – Yakın Doğu Üniversitesi – Bilgisayar Mühendisliği Bölümü 4.Sınıf*
*Kemal Saygılı - Yakın Doğu Üniversitesi – Yazılım Mühendisliği Bölümü 4.Sınıf*

Teknoloji hızla gelişmeye devam ediyor; ancak onu nasıl şekillendireceğimiz ve hangi amaçlarla kullanacağımız yine biz insanların elinde.
*Bir sonraki yazımızda buluşmak üzere…*

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

# ESTONIA Modeli

***Estonya (e-Estonia), dünya genelinde dijital devlet ve e-devlet dönüşümünün en başarılı örneği ve rol modeli olarak kabul edilir. 1990'ların sonunda "Tiger Leap" (Kaplan Sıçraması) projesiyle altyapısını kuran Estonya, kamu hizmetlerinin %99'unu dijital ortama taşımıştır.***

Estonya e-Devlet modelinin öne çıkan temel özellikleri, mimarisi ve başarı ilkeleri şunlardır:

1. Temel Yapı Taşı: X-Road (Merkeziyetsiz Veri Paylaşımı)

Estonya sisteminin kalbinde X-Road adı verilen omurga yer alır.

* Tüm devlet kurumları ve özel sektör kuruluşları (bankalar, telekom, hastaneler) verilerini tek bir devasa veri tabanında toplamak yerine kendi veritabanlarında tutar.

* X-Road, bu farklı sistemlerin uçtan uca şifreli ve güvenli bir şekilde birbiriyle konuşmasını sağlar.

2. Once-Only İlkesi

Estonya yasalarına göre devlet, vatandaşından aynı bilgiyi ikinci kez isteyemez.

* Örneğin; adresinizi Nüfus Kayıt Sistemi'ne bir kez girdiğinizde; ehliyet başvurusu, vergi dairesi veya sağlık kuruluşu bu adrese X-Road üzerinden otomatik erişir. Vatandaşın tekrar işlem yapmasına gerek kalmaz.

3. Dijital Kimlik (e-ID) ve Dijital İmza

* Her Estonya vatandaşına çipli bir dijital kimlik kartı veya mobil kimlik (Mobile-ID / Smart-ID) verilir.

* Dijital imza, yasal olarak ıslak imza ile %100 eşdeğerdir.

* Estonyalılar vergi beyanı, sözleşme imzalama veya reçete alma gibi tüm işlemleri saniyeler içinde telefonlarından onaylayabilir.

4. Dünyada Bir İlk: e-Residency (e-Oturum / e-Vatandaşlık)

Estonya, fiziki olarak ülkede yaşamayan küresel girişimcilere dijital kimlik sağlayan dünyadaki ilk ülkedir.

* Dünyanın herhangi bir yerinden internet üzerinden dakikalar içinde Avrupa Birliği merkezli şirket kurulabilir.

* Şirket yönetimi, vergilendirme ve bankacılık işlemleri tamamen uzaktan e-Devlet altyapısı ile yürütülür.

5. i-Voting (İnternet Üzerinden Oylama)

* Estonya, 2005 yılında genel ve yerel seçimlerde internet üzerinden oy kullanma sistemini getiren ilk ülkedir.

* Günümüzde genel seçimlerde kullanılan oyların yarıya yakını çevrimiçi olarak evden atılmaktadır.

Dijitalleşemeyen Sadece 2 İşlem Var:

Estonya'da neredeyse her şey çevrimiçi yapılabilir. Dijital olarak yapılamayan yalnızca iki istisna kalmıştır:

* Evlenme / Boşanma

* Gayrimenkul devri/satışı (Belirli noter güvenlik protokolleri nedeniyle)

Sağladığı Faydalar

* Zaman Tasarrufu: Dijital imza ve bürokrasinin kalkması sayesinde her bir vatandaş için yılda ortalama 5 iş günü zaman tasarrufu sağlanır.

* Ekonomik Kazanç: Kağıtsız süreçler ve verimlilik sayesinde ülke her yıl GSYİH'sının yaklaşık %2'si kadar tasarruf eder.

**Bu Bilgilerin (Verilerin) Bozulma veya Kaybolma veya Çalınma Olasılığı Ne?**

Estonya'nın e-Devlet verilerini tamamen kaybetme olasılığı, mühendislik ve uluslararası hukuk standartları açısından sıfıra yakın kabul edilir.

Özellikle 2007 yılında maruz kaldığı kapsamlı siber saldırılardan ders çıkaran Estonya, verilerinin kaybolması veya işlenemez hale gelmesi riskini bertaraf etmek için dünyada eşi benzeri olmayan çok katmanlı bir güvenlik ve yedekleme mimarisi şu katmanlarla kurmuştur:

1. Veri Büyükelçiliği (Data Embassy)

Estonya, fiziki sınırlarına yönelik bir askeri işgal, doğal afet veya devasa bir siber saldırı durumunda devlet yapısının çökmemesini sağlamak amacıyla Lüksemburg'da dünyanın ilk "Veri Büyükelçiliği"ni kurmuştur.

* Diplomatik Dokunulmazlık: Lüksemburg'daki bu yüksek güvenlikli (Tier 4) veri merkezi, diplomatik anlaşmalarla korunan Estonya toprağı statüsündedir. Hiçbir yabancı devlet veya kurum bu sunuculara el koyamaz veya erişemez.

* Canlı Yedekleme (Disaster Recovery):

Nüfus kayıtları, mülk tapuları, şirket sicilleri, mahkeme belgeleri ve kimlik bilgileri gibi kritik devlet verileri bu sunucularda anlık olarak senkronize edilir. Estonya topraklarındaki tüm sunucular yok olsa bile devlet işleyişi Lüksemburg üzerinden uzaktan sürdürülebilir.

2. KSI Blockchain (Veri Bütünlüğü ve Değiştirilemezlik)

*Verilerin kaybolması kadar "fark ettirmeden değiştirilmesi" de hayati bir risktir.* Estonya, verilerin kurcalanmasını önlemek için Guardtime şirketi ile birlikte geliştirilen KSI Blockchain altyapısını kullanır.

* Siteme giren her veri anında blockchain ile zaman damgalanır ve şifrelenir.

* Kötü niyetli bir aktör veya siber korsan veritabanına sızıp bir kaydı silmeye veya değiştirmeye çalışsa bile, blockchain üzerindeki matematiksel doğrulama nedeniyle bu değişiklik anında tespit edilir ve veri orijinal haline döndürülür.

3. X-Road

Estonya'da veriler tek bir devasa veritabanında toplanmaz.

Sağlık verileri ayrı, vergi verileri ayrı, nüfus verileri ayrı sunucularda tutulur. Bu sistem sayesinde, tek bir sunucunun çökmesi veya fiziksel hasar görmesi durumunda tüm sistem zarar görmez; sadece o spesifik birimin yedeği devreye girer.

4. Siber Hijyen ve Uluslararası İttifaklar

* NATO Siber Savunma Merkezi (CCDCOE-Cooperative Cyber Defence Center of Excellence): Merkezi Estonya'nın başkenti Tallinn'dedir. Estonya, küresel siber savunma alanındaki en gelişmiş istihbarat ve teknolojiye doğrudan erişim sahibidir.

* Hybrid ve Cloud Yedekleri: Hassas olmayan veya kamuya açık hizmetlerin yedekleri (örneğin Cumhurbaşkanlığı web sitesi gibi)

uluslararası güvenli Cloud sağlayıcılarında da sanal olarak yedeklenir.
Sistemdeki potansiyel riskler, verinin "kaybolması" değil, "geçici olarak erişilemez hale gelmesi" ile sınırlıdır:
* Global İnternet / Kablo Kesintileri: Ülkeyi dünyaya bağlayan fiber optik denizaltı kablolarının fiziksel olarak kesilmesi durumunda kısa süreli erişim sıkıntıları yaşanabilir.
* Kapsamlı Siber Saldırılar (DDoS): Ağ trafiğini boğmaya yönelik saldırılar e-hizmetleri birkaç saatliğine yavaşlatabilir ancak verileri silemez veya bozamaz.

**Dezavantajları Neler? En Korkunç Senaryo..**
Estonya'nın e-Devlet modeli teknolojik açıdan büyüleyici olsa da kusursuz değildir. Dünyanın En Dijital Ülkesi olmanın getirdiği ciddi riskler, teknolojik bağımlılıklar ve insani/toplumsal dezavantajlar da mevcuttur.
1. %100 Dijital Bağımlılık ve "Tek Noktadan Çöküş" Riski
Sistem her şeyi dijitalleştirdiği için, yaşanacak devasa bir altyapı krizi (fiziksel elektrik kesintileri, küresel internet çöküşü veya stratejik fiber optik kablo kesintileri) ülkeyi tamamen felç edebilir.
* Sonuç: Fiziksel evrak ve bürokratik alternatifler tamamen ortadan kalktığı için sistem durduğunda kağıt üzerinde işlem yapacak geleneksel bir altyapı bulunmaz.
2. Siber Saldırı ve Hybrid Savaş Tehdidi
Estonya, Rusya ile sınır komşusudur ve jeopolitik olarak çok hassas bir konumdadır.
* Kritik Hedef: Devletin tüm damarları internete bağlı olduğu için ülke, geleneksel bir askeri kara harekatından ziyade yıkıcı bir siber saldırıyla (DDoS, fidye yazılımları, kritik altyapı sızmaları) çok daha kolay hedef alınabilir.
* 2007'deki büyük Rus siber saldırısında ülkedeki bankalar, medya ve kamu hizmetleri günlerce kilitlenmişti.
3. Elderly & Tech-Literacy Exclusion
Teknolojiye adapte olmak genç nüfus için kolay olsa da yaşlılar, engelliler veya teknoloji okuryazarlığı düşük bireyler için sistem dışı kalma riski doğurur.
* Fiziksel şubeler ve "yüz yüze" kamu görevlisi sayısı minimuma indirildiği için yardım almak veya teknik sorunları çözmek belirli yaş grupları için oldukça zorlayıcı olabilir.
4. Biyometrik ve Dijital Kimlik Çalınması / Güvenlik Açıkları
Veriler kaybolmasa bile kimlik avı (phishing) ve yazılım açıkları her zaman bir tehdittir.
* 2017 Kimlik Kartı Krizi: Estonya'daki çipli kimlik kartlarının kullandığı bir donanım şifreleme kütüphanesinde küresel bir güvenlik açığı (RSA key hatası) tespit edildi. Devlet, 750.000'den fazla vatandaşın kimlik kartı sertifikasını acilen dondurmak ve yenilemek zorunda kaldı.
* Vatandaşın dijital şifrelerini (PIN1/PIN2) kaptırması durumunda, bir başkası onun adına yasal işlem yapabilir veya şirket kurabilir.
5. Mahremiyet Kaygıları ve "Gözetim Devleti" Algısı
X-Road üzerinde kimin hangi veriye baktığı (örneğin bir doktorun sizin finansal geçmişinizi görememesi gibi) sıkı denetlense ve vatandaşa "Hangi memur benim verime baktı?" izleme yetkisi verilse de:
* Devletin tüm veri akışını ve vatandaş hareketlerini anlık olarak izleyebilme potansiyeli, mahremiyet odaklı bireyler için sürekli bir tedirginlik kaynağıdır.
6. Yüksek Altyapı ve Bakım Maliyeti
Sistemi kurmak kadar onu sürekli güncel tutmak, en son siber güvenlik standartlarıyla yenilemek ve nitelikli yazılımcı/uzman istihdam etmek çok yüksek bir bütçe gerektirir.
Özetle: Estonya bürokrasiyi ve zaman kaybını neredeyse sıfıra indirmiştir; ancak bunun bedeli olarak tüm yumurtaları tek bir dijital sepete koymuş durumdadır. Sistem çalıştığı sürece mükemmel, durduğu sürece ise hayatı durduracak kadar bağımlılık yaratıcıdır.

Kamu Nasıl Yapılandırıldı?
Estonya'nın e-Estonia vizyonunu hayata geçiren kamu yapılanması; bürokrasiyi azaltmak, kurumlar arası veri paylaşımını zorunlu kılmak ve siber güvenliği en üst düzeyde tutmak üzere esnek, yatay ve teknoloji odaklı bir modelle tasarlanmıştır. Klasik devlet yapısındaki "her bakanlığın kendi hantal bilgi işlem dairesini kurması" yerine, Estonya devleti kamu organlarını şu temel sütunlar etrafında yapılandırmıştır:
1. Yasal ve Kurumsal Çerçeve: Ortak Yönetim
Estonya kamu yönetimi, dijitalleşmeyi tek bir kurumun insafına bırakmak yerine yasalarla tüm devlet teşkilatına zorunlu kılmıştır.
* Ekonomi ve İletişim Bakanlığı (MKM): Dijital vizyonun, bilişim politikasının ve stratejilerin ana belirleyicisidir. Devletin genel bilişim mimarisini çizer.
* Devlet Bilgi Sistemleri Kurulu (RIA - Riigi Infosüsteemi Amet): e-Devletin teknik motorudur. X-Road omurgasının işletilmesinden, dijital kimlik (e-ID) altyapısının güvenliğinden ve kamu kurumlarının bilgi sistemlerinin koordinasyonundan sorumludur.
* CERT-EE (Siber Olaylara Müdahale Ekibi): RIA çatısı altında çalışan ve ülkenin kamu dijital altyapısını 7/24 siber saldırılara karşı koruyan uzman birimdir.
2. Mimari Yapılanma: Merkezsiz (Decentralized) Kamu Modeli
Estonya, kamu hizmetlerini tek bir devasa "Süper Bakanlık" veya "Tek Veri Tabanı" üzerinden yürütmez.
* Silo Yok, Bağlantı Var: İçişleri Bakanlığı nüfus verilerini, Adalet Bakanlığı mülk/tapu verilerini, Sosyal İşler Bakanlığı ise sağlık verilerini kendi veritabanında tutar.
* Veri Sahipliği ve Sorumluluk: Her kamu kurumu kendi verisinin doğruluğundan ve güvenliğinden doğrudan sorumludur. Diğer kurumlar bu veriye erişmek istediğinde X-Road protokolü üzerinden anlık izinle erişir. Böylece kamu yapısı hantal bir tek merkez yerine birbirine bağlı esnek bir ağ gibi çalışır.
3. "Digital First" ve Katı Yasal Kurallar
Kamu teşkilatının çalışma prensipleri iki ana kanuni ilke ile şekillendirilmiştir:
* Once-Only Prensibi: Kamu kurumlarının, başka bir kamu kurumunda zaten var olan bir veriyi vatandaştan tekrar istemesi kanunen yasaktır. Bu kural, kurumları kendi aralarında entegre olmaya zorlamıştır.
* Kağıtsız Kamu (Paperless Governance): Bakanlar Kurulu toplantıları da dahil olmak üzere kamu içi süreçlerin %99'u dijital ortamda ve e-imza ile yürütülür. Devlet arşivleri ve belgeler tamamen dijital formatta saklanır.
4. Kamu - Özel Sektör İş Birliği (PPP-Purchasing Power Parity)

Estonya kamusu, tüm teknolojiyi kendi bünyesinde geliştirmek yerine özel sektörle stratejik ortaklıklar kurmuştur:

* Teknoloji Geliştirme: Sistem yazılımları, siber güvenlik ürünleri ve blockchain altyapıları (Guardtime, Cybernetica vb.) Estonya merkezli yerli teknoloji şirketleriyle birlikte geliştirilmiştir.

* Bankalar ve Telekom Operatörleri: Vatandaşların sisteme ilk girişte kullandıkları güvenli kimlik doğrulama altyapıları (Smart-ID, Mobile-ID) özel sektör bankaları ve GSM operatörleriyle ortaklaşa kamu hizmetine entegre edilmiştir.

5. Şeffaflık ve "Vatandaş Odaklı Denetim"

Estonya kamu yapılanmasında vatandaş sadece hizmet alan değil, devleti denetleyen konumdadır:

* Veri İzleme Portalı: Vatandaşlar e-devlet portalına girdiklerinde, hangi kamu görevlisinin (polisin, doktorun, vergi memurunun) hangi tarihte ve ne sebeple kendi kişisel verisine baktığını görebilir.

* Yasadışı Erişim Ceza Sebebidir: Yetkisi veya geçerli bir soruşturma sebebi olmadan bir vatandaşın verisini sorgulayan kamu görevlisi ağır yaptırımlarla ve meslekten ihraçla karşı karşıya kalır.

Yeni Yapılandırmada Mevcut Personele Ne Oldu?

Estonya'nın dijital dönüşüm sürecinde en çok merak edilen konulardan biri, bürokrasinin ve evrak işlerinin ortadan kalkmasıyla "boşa çıkan" kamu personelinin durumu olmuştur. Estonya bu süreci personeli işten çıkarıp sokağa atmak yerine, stratejik bir iş gücü dönüşümü (reskilling & upskilling) ile yönetmiştir.

Teknolojiye uyum sağlayamayan veya manuel iş ihtiyacı biten personelin akıbeti şu ana başlıklar altında gerçekleşmiştir:

1. Manuel Memurluktan "Analistlik ve Müşteri Danışmanlığına" Geçiş

Geleneksel kamu yönetiminde zamanının %80'ini dilekçe kabul etmek, veri girişi yapmak ve evrak mühürlemekle geçiren memurlar, sistemlerin otomatize olmasıyla birlikte katma değerli rollere kaydırılmıştır.

* Veri Kontrolörlüğü: Memurlar artık veri giren değil, sistemin işlediği verileri denetleyen ve istisnai durumları çözen uzmanlar haline geldi.

* Danışmanlık: Vatandaşa "evrak alan" değil, karmaşık durumlarda (örneğin karmaşık hukuki/ticari durumlar) yol gösteren "danışman" rolü üstlendiler.

2. Yoğun Yeniden Eğitme (Reskilling) Programları

Devlet, dijitalleşme hamlesini başlatırken kamu çalışanları için kapsamlı teknoloji ve süreç yönetimi eğitimleri düzenledi.

* Temel bilgisayar kullanımından veri analitiğine, yeni e-Devlet yazılımlarının kullanımından siber güvenlik farkındalığına kadar memurlar sürekli hizmet içi eğitime tabi tutuldu.

* Uyum sağlayan personelin unvanı ve sorumluluk alanı genişletilerek dijital kamu hizmetlerinin yöneticileri olmaları sağlandı.

3. Teknolojiye Uyum Sağlayamayanlar İçin Ne Oldu?

Teknolojiye adapte olmakta zorlanan veya yeni rolü benimseyemeyen personel için birkaç farklı yol izlendi:

* Fiziksel Destek Noktalarına Kaydırma: Sistem %99 dijital olsa da yaşlılar, engelliler veya dijital okuryazarlığı düşük vatandaşlar için "fiziksel hizmet merkezleri" (örneğin Hizmet Binaları / Service Centers) korundu. Teknolojiye ayak uyduramayan veya insan ilişkileri güçlü olan memurlar, bu merkezlerde vatandaşa dijital araçları kullanmayı öğreten "dijital rehberler" olarak görevlendirildi.

* Erken Emeklilik ve Doğal Doğal Eksilme (Natural Attrition): Dijitalleşme bir gecede gerçekleşmediği için (20 yıllık bir süreçtir), emeklilik yaşı gelen personelin yerine yeni geleneksel memurlar alınmadı. Kadrolar zamanla doğal yollarla küçüldü.

* Özel Sektör ve İdari Kadro Transferleri: Kamu bürokrasisi küçülürken, büyüyen teknoloji ve hizmet sektörüne geçiş yapmak isteyen personele kariyer ve oryantasyon desteği verildi.

4. İstihdamın Kaydığı Yeni Alan: Siber Savunma ve Bilişim Teknolojileri

<u>Evrak memurluğu kadroları kapatılırken, kamu sektöründe yepyeni ve devasa bir istihdam alanı doğdu: Bilişim Teknolojileri ve Siber Güvenlik Uzmanlığı.</u>

* *Devlet, geleneksel memur bütçesini azaltarak kaynaklarını veri analistleri, yazılım mühendisleri, siber güvenlik uzmanları ve UX (kullanıcı deneyimi) tasarımcıları istihdam etmeye yönlendirdi.*

Özetle, Estonya modeli, insanları "teknoloji yüzünden işsiz bırakmak" yerine, insan kaynağını "gereksiz amelelikten kurtarıp zihinsel/analitik işlere yönlendirmeyi" başarmıştır.

Bir memurun gün boyu adres beyanı kaydetmesi yerine, o veriyi kullanarak şehir planlaması veya sosyal yardım analizi yapması sağlanmıştır. Uyum sağlayamayan küçük bir kesim ise, sistemin dışında kalan vatandaşlara rehberlik etmek üzere destek rollerinde tutulmuştur.

**Ne Kadar Zamanda Başarıldı?**

Estonya'nın bugünkü e-Estonia vizyonuna ulaşması ve kamunun %99'unu dijitalleştirmesi yaklaşık 25–30 yıllık kademeli ve kararlı bir sürecin sonucudur.

<u>*Estonya'nın Dijitalleşme Zaman Çizelgesi*</u>

1. Hazırlık ve Altyapı Dönemi (1991 – 1997)

* 1991: SSCB'den bağımsızlığın kazanılması. Sıfırdan bir devlet yapısı kurulması gerekiyordu ve geleneksel bürokrasiye ayıracak bütçe yoktu.

* 1996 - Tiigrihüpe (Kaplan Sıçraması): Tüm okullara bilgisayar ve internet erişimi sağlayan devasa bir eğitim projesi başlatıldı. Genç nesil ve toplum dijital çağa hazırlandı.

2. Temellerin Atılması (2000 – 2002)

* 2000: İnternet erişimi yasal bir insan hakkı ilan edildi. İlk kez e-Vergi (e-Tax) sistemi kullanıma sunuldu ve halkın %20'si vergilerini internetten ödedi.

* 2001 (X-Road'un Doğuşu): Kamu ve özel sektörün güvenli veri paylaşmasını sağlayan X-Road omurgası devreye alındı.

* 2002 (Dijital Kimlik): İlk çipli dijital kimlik kartları (e-ID) vatandaşlara dağıtılmaya başlandı.

3. Hizmetlerin Yaygınlaşması (2005 – 2014)

* 2005: Dünyada ilk kez internet üzerinden genel/yerel seçim oylaması (i-Voting) yapıldı.

* 2008: Dijital Sağlık Kayıtları (e-Health) ve e-Reçete sistemine geçildi.

* 2012: Kamu hizmetlerinin %90'ından fazlası artık tamamen dijital ortamdaydı.

4. Küreselleşme ve Veri Güvenliği (2014 – Günümüz)

* 2014: Dünya çapında girişimcileri çekmek

için e-Residency (e-Oturum) programı başlatıldı.
* 2017: Dünyanın ilk Veri Büyükelçiliği (Data Embassy) Lüksemburg'da açıldı.
* Günümüz: Evlenme ve boşanma dışındaki tüm kamu hizmetleri (%99+) dijital olarak yürütülmektedir.
Özetle
* İlk Somut Adımlar - Tam Dijitalleşme: Yaklaşık 25 Yıl (1996 - 2021)
* Kritik Eşik (Temel Altyapıların Oturması): Yaklaşık 10 Yıl (1996 Kaplan Sıçraması'ndan 2005/2008 dijital hizmet patlamasına kadar)
Estonya'nın başarısındaki en büyük etken; siyasi iradenin hükûmetler değişse bile 30 yıl boyunca bu vizyondan taviz vermeden projeyi sürdürmüş olmasıdır.

**Finansal Etki?**
Estonya'nın e-Devlet dönüşümünün yarattığı finansal ve ekonomik etkiler son derece ölçülebilir, doğrudan ve yüksek getirili sonuçlar doğurmuştur. Bu finansal etkiler şu temel başlıklarda toplanmaktadır:
1. GSYİH'de Yıllık %2 Tasarruf
Estonya devletinin resmi verilerine ve OECD analizlerine göre, kağıtsız kamu yönetimi ve dijital imza kullanımı, ülkeye her yıl Gayrisafi Yurtiçi Hasıla'nın (GSYİH) yaklaşık %2'si kadar tasarruf sağlamaktadır.
* Bu oran, ülkenin yıllık savunma bütçesine veya eğitim harcamalarının önemli bir kısmına denk gelen muazzam bir mali kaynaktır.
2. Devasa Zaman ve İş Gücü Maliyeti Kazancı
* Masaüstü İş Gücü Kaybının Önlenmesi: Dijital imzalar, otomatik veri transferleri ve bürokrasinin kalkması sayesinde her bir vatandaş ve çalışan için yılda ortalama 5 iş günü (40 çalışma saati) tasarruf edilir.
* Kamu Bütçesinden Personel Tasarrufu: Manuel evrak onaylayan, veri giren binlerce memur kadrosuna bütçe ayrılması zorunluluğu ortadan kalkmıştır. Kamu personeli giderleri doğrudan katma değerli alanlara (teknoloji, analiz, güvenlik) kaydırılmıştır.
3. "e-Residency" (e-Vatandaşlık) İle Yeni Gelir Modeli
Estonya, dijital altyapısını ülkeye döviz ve vergi girdisi sağlayan bir "ihracat kalemine" dönüştürmüştür.
* Doğrudan Vergi Geliri: Dünyanın dört bir yanından e-Yerleşik (e-Resident) olan 120.000'den fazla girişimci, Estonya'da 39.000'den fazla şirket kurmuştur.
* Bütçe Katkısı: Bu program sayesinde Estonya devleti, sadece e-yerleşik şirketlerin ödediği kurumlar vergisi, gelir vergisi ve harçlardan yıllık 100 milyon Euro'nun üzerinde net devlet geliri elde etmektedir.
* Yatırım Getirisi (ROI): Estonya devleti e-Residency programına harcadığı her 1 Euro karşılığında bütçesine yaklaşık 12 Euro doğrudan gelir elde etmektedir.
4. Yerel Özel Sektöre Ekosistem Geliri
Dijitalleşme sadece devlete değil, özel sektöre de finansal canlılık getirmiştir:
* e-Yerleşiklerin kurduğu on binlerce şirket; Estonya'daki muhasebe, hukuk, yazılım ve danışmanlık firmalarından hizmet almakta, bu da yerel hizmet sektörüne yılda 15 milyon Euro'yu aşkın ek ciro sağlamaktadır.
* Banka ve İşlem Maliyetlerinin Düşmesi: Kağıt baskı, kargo, arşivleme ve fiziksel depolama gibi operasyonel giderler sıfıra yaklaştığı için şirketlerin işletme maliyetleri dramatik şekilde düşmüştür.
5. Veri Doğruluğu ve Kaçakların Önlenmesi
* Vergi Kaybının Önlenmesi: Vergi sisteminin %100 dijitalleşmesi ve banka/ticaret verilerinin eşzamanlı işlenmesi sayesinde vergi kaçırma, kayıt dışı ekonomi ve evrakta sahtecilik oranları minimuma inmiştir.
* Şirket kurulumları ve vergi beyanları saniyeler içinde şeffaf biçimde yapıldığı için devletin vergi toplama maliyeti düşmüş, toplama verimliliği tavan yapmıştır.
*Estonya, teknolojiye yaptığı ilk altyapı yatırımını fazlasıyla geri çıkarmış; e-Devlet altyapısını sadece bir "hizmet aracı" değil, devlete ve ülkeye milyonlarca Euro kazandıran kârlı bir ekonomik model haline getirmiştir*.

**Neden Sadece Estonya?**
Estonya'nın bu kadar uçtan uca ve cesur bir dijitalleşmeyi başarması ve bunu bu dereceye ulaştıran nadir ülkelerden biri olması, tamamen o döneme özgü "tarihsel, ölçeksel ve siyasi" faktörlerin bir araya gelmesiyle ilgilidir.
Başka ülkelerin aynı modeli birebir kopyalamasını veya sıfırdan hayata geçirmesini zorlaştıran temel nedenler şunlardır:
1. SSCB Sonrası "Sıfır Tabula Rasa" (Temiz Sayfa) Fırsatı
* Eski Sistem Yükü Yoktu: 1991'de SSCB dağıldığında Estonya'nın elinde bakımı yapılması gereken hantal, kağıt bazlı, yüzyıllık geleneksel bir bürokrasi altyapısı yoktu.
* Sıfırdan İnşa Etmek Kolaydır: Bir binayı yıkıp yenisini yapmak, eski binayı güçlendirmekten kolaydır. Almanya veya Fransa gibi ülkeler yüz yıllık kağıt arşivlerini ve sistemlerini dijitalleştirmeye çalışırken, Estonya doğrudan dijital altyapıyı "varsayılan" (default) olarak kurdu.
2. Bütçe Yetersizliği ve Zorunluluk
* Bağımsızlığın ilk yıllarında Estonya son derece fakir bir ülkeydi. Geleneksel devlet binaları açmak, binlerce memur istihdam etmek ve fiziksel posta/evrak ağı kurmak için paraları yoktu.
* İnternet ve dijitalleşme, devleti ucuza mal etmenin ve ayakta tutmanın tek çaresi olarak görüldü.
3. Ülke Ölçeği ve Nüfus Avantajı (1.3 Milyon)
* Estonya'nın nüfusu yaklaşık 1,3 milyondur (İstanbul'un bir iki ilçesi kadar).
* Bu ölçekte bir nüfus için veri tabanı entegrasyonu yapmak, çipli kimlik dağıtmak ve test süreçlerini yönetmek; 80 milyonluk Türkiye, 84 milyonluk Almanya veya 330 milyonluk ABD ile kıyaslanmayacak kadar hızlı ve esnektir.
4. Toplumsal Güven ve Kültürel Yapı
* Estonya halkının devlete olan güveni son derece yüksektir. Büyük ülkelerdeki vatandaşlar kişisel verilerinin "devletin elinde toplanmasından" ve gözetlenmekten korkarken (örn. Almanya veya ABD'deki mahremiyet kaygıları), Estonyalılar veriyi şeffaf bir şekilde devlete emanet etme konusunda çok daha rahattı.
5. Siyasi İstikrar ve Devamlılık
* 1990'lardan bu yana Estonya'da hükûmetler, sağ veya sol partiler defalarca değişti. Ancak "Dijital Estonya" bir devlet politikası kabul edildi ve gelen hiçbir hükûmet bu vizyonu geriye sarmadı, aksine üzerine koyarak devam etti.
6. Büyük Ülkelerdeki "Kazanılmış Haklar" ve Lobi Direnci
* Gelişmiş birçok ülkede devasa kamu

bürokrasisi, noterler, posta teşkilatları ve geleneksel hizmet sağlayıcıları güçlü lobilere sahiptir. Süreçlerin tamamen dijitalleşmesi bu kurumların yetkilerini ve gelirlerini azaltacağı için ciddi bir iç direnç oluşur. Estonya'da bu yapılar henüz kemikleşmediği için direnç yaşanmadı.

***Günümüzde Durum Değişiyor mu?***

Aslında Estonya artık yalnız değil, sadece bu işin öncüsü.

Estonya'nın kurduğu X-Road altyapısını bugün:

* Finlandiya aynen alıp kendi sistemine entegre etti (Suomi.fi).
* Ukrayna, Estonya mimarisinden esinlenerek geliştirdiği Diia uygulamasıyla dünyadaki en hızlı dijitalleşen ülkelerden biri haline geldi.
* Singapur, Birleşik Arap Emirlikleri ve Güney Kore gibi ülkeler de benzer yüksek dijitalleşme seviyelerine ulaştı.

Estonya doğru zamanda, doğru ölçekte ve çaresizlikten kaynaklanan doğru bir vizyonla bu adımı attı. Büyük ve köklü ülkeler için ise bu dönüşüm, giden treni hareket halindeyken tamir etmeye benzediği için çok daha yavaş ilerliyor.

**Kıbrıs?**

Evet, Kıbrıs gibi bir adada bu sistem kesinlikle başarılabilir; hatta coğrafi ve demografik açıdan Kıbrıs, Estonya modelini uygulamak için dünyadaki en ideal adaylardan biridir. Ancak uygulamanın başarısı, teknolojinin kendisinden ziyade siyasi, idari ve adadaki mevcut sosyo-politik dinamiklere bağlıdır.

1. Neden Kıbrıs İçin Çok Büyük Bir Fırsat?

* İdeal Nüfus ve Ölçek:

Estonya'nın başarısındaki en büyük etken 1,3 milyonluk nüfusu ve esnek yapısıydı. Kıbrıs adasının toplam nüfusu da bu ölçeğe son derece yakındır. Küçük nüfus; veri tabanı mimarisinin kurulumunu, pilot testleri ve çipli kimlik/e-imza dağıtımını devasa ülkelere kıyasla çok daha hızlı ve ucuz hale getirir.

* Fiziki Ada İzolasyonunu Aşma:

Bir adada yaşamanın getirdiği lojistik ve bürokratik sınırlandırmalar, e-Devlet ile tamamen ortadan kalkar. Evrak göndermek, onay almak veya yurt dışındaki vatandaşların işlemlerini yürütmesi için adaya seyahat etme zorunluluğu biter.

* Ekonomik Çeşitlendirme ve Finansal Dönüşüm:

Kıbrıs (özellikle Kuzey ve Güney yapıları itibarıyla) turizm ve yükseköğretim odaklı ekonomilere sahiptir. Estonya'nın e-Residency (e-Oturum) benzeri bir modeli ada ölçeğinde uygulamak; küresel yazılımcıları, dijital göçebeleri ve uluslararası girişimcileri adaya çekerek ciddi bir vergi ve döviz girdisi yaratabilir.

* Maliyet/Etkinlik Dengesi:

Geleneksel kamu binaları kurmak ve hantal bir memur kadrosu beslemek ada ekonomileri için yük oluşturur. Dijitalleşme, kamu giderlerinde devasa tasarruf sağlar.

2. Kıbrıs'ta Uygulanmasının Önündeki Temel Engeller

Sistemin kurulmasının önündeki engeller teknik değil, yapısal ve politik nedenlerdir:

A. Siyasi ve Hukuki Durum (Bölünmüşlük)

Adanın mevcut siyasi yapısı ve uluslararası tanınabilirlik durumları (KKTC ve Güney Kıbrıs), tek bir entegre omurganın (X-Road benzeri) tüm adada ortak çalışmasını zorlaştırır. Ancak her iki taraf da kendi idari yapısı içinde bu sistemi bağımsız olarak rahatlıkla kurabilir.

B. **Bürokratik Direnç ve Memur Kültürü**

Ada ülkelerinde kamu istihdamı genellikle sosyal ve siyasal bir güvence mekanizması olarak görülür. Estonya'nın başardığı "memurları analist ve rehber kadrolarına dönüştürme" süreci, Kıbrıs'taki mevcut kamu sendikaları ve geleneksel bürokrasi tarafından ilk etapta dirençle karşılanabilir.

C. Altyapı ve Fiber İnternet Bağımlılığı

Estonya bu işe başlamadan önce tüm ülkeyi fiber ağlarla örmüş ve interneti yasal bir hak ilan etmişti. Kıbrıs genelinde kesintisiz ve yüksek hızlı internet altyapısının, veri merkezlerinin (Data Center) ve enerji sürekliliğinin tam olarak güvenceye alınması gerekir.

3. Nasıl Başarılabilir? (Yol Haritası)

Kıbrıs'ta bu dönüşümü başlatmak için Estonya'nın izlediği strateji uygulanabilir:

* Açık Kaynak Altyapı Kullanımı: Estonya, X-Road sistemini açık kaynaklı olarak dünya ile paylaşmıştır (Nordic Institute for Interoperability Solutions aracılığıyla). Kıbrıs sıfırdan sistem yazmak yerine hazır ve denenmiş bu omurgayı kendi mevzuatına uyarlayabilir.
* Eğitimden Başlamak (Kaplan Sıçraması): İlkokullardan itibaren dijital okuryazarlık ve yazılım eğitimine öncelik verilerek toplum dijital süreçlere hazırlanabilir.
* Pilot Alan Tanımlama: İlk olarak vergi beyanları, şirket kurulumları ve e-Reçete/sağlık sistemi gibi vatandaşın günlük hayatına doğrudan dokunan alanlar dijitalleştirilerek güven inşa edilebilir.

Sonuç

Estonya örneği bize gösteriyor ki; dijital devrim yapmak için zengin veya devasa bir ülke olmaya gerek yoktur. Aksine, küçük ve ada boyutundaki coğrafyalar karar alma hızları sayesinde bu dönüşümü çok daha çabuk başarabilir.

Kıbrıs için gerekli olan tek şey; partiler üstü güçlü bir siyasi irade ve kararlı bir teknoloji vizyonudur.

**Süre?**

Kıbrıs gibi bir ölçekte Estonya benzeri uçtan uca bir e-Devlet dönüşümünü tamamlamak, toplamda ortalama 3 ila 5 yıllık planlı bir süreç gerektirir.

Estonya bu yolu 1990'ların teknolojisiyle sıfırdan keşfederek 10-15 yılda yürüdü; ancak bugün teknoloji, hazır altyapılar ve standartlar olgunlaştığı için bu süre çok daha kısadır.

Kıbrıs için aşamalı zaman haritası şu şekilde özetlenebilir:

1. Aşama: Hazırlık, Mevzuat ve Mimari (6 – 12 Ay)

* Siyasi Karar ve Yasal Altyapı: e-İmza, Veri Koruma (KVKK/GDPR uyumu) ve “Once-Only” prensibini zorunlu kılan yasaların çıkarılması.
* Teknik Altyapı: Estonya'nın açık kaynaklı X-Road omurgasının veya benzeri bir veri paylaşım altyapısının kurulması.

2. Aşama: Çekirdek Hizmetler ve Dijital Kimlik (12 – 24 Ay)

* Dijital Kimlik (e-ID / Mobile-ID): Tüm vatandaşlara güvenli e-imza ve dijital kimliklerin (çipli kart veya mobil uygulama) dağıtılması.
* Kritik Veritabanlarının Bağlanması: Nüfus kaydı, vergi dairesi, tapu ve sağlık veritabanlarının X-Road omurgasına entegre

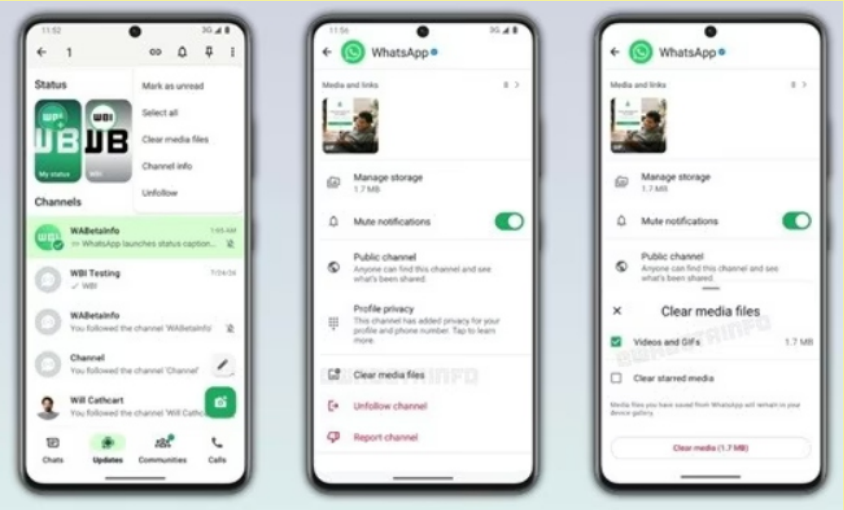
edilmesi.
* İlk Pilot Uygulamalar: e-Vergi, e-Reçete ve şirket kurulumu gibi temel kamu hizmetlerinin dijital ortamda açılması.
3. Aşama: Yaygınlaşma ve Tam Entegrasyon (24 – 36 Ay)
* Kamu hizmetlerinin %70 - %80'inin tamamen dijital ortama taşınması.
* Kağıtsız kamu yönetimine geçiş (kurumlar arası yazışmaların %100 e-imzalı olması).
* Memurların yeni rollere (analistlik, dijital rehberlik) eğitimi.
4. Aşama: İleri Düzey Ekosistem (36 – 60 Ay)
* İnternet üzerinden oylama (i-Voting) altyapısının test edilmesi.
* Yatırımcı ve dijital göçebeleri adaya çekecek e-Residency (e-Oturum) benzeri küresel programların hayata geçirilmesi.
* Kesintisiz veri güvenliği için ülke dışı yedekleme (Veri Büyükelçiliği) veya güvenli bulut mimarilerinin tamamlanması.
*Olası bir senaryoda, Kıbrıs'ta kararlı bir siyasi irade ile 1,5 - 2 yıl içinde günlük hayatı kolaylaştıran hissedilir bir dönüşüm başlar; 3 ila 5 yıl içinde ise ülke, dünya standartlarında tam dijital bir e-Devlet yapısına kavuşabilir.*

**Vasviye Tunaboylu**
Database Specialist

# WhatsApp, kanal medyalarını yönetmeyi kolaylaştırıyor.

***WhatsApp, Android beta sürümünde kanallar için geliştirilen yeni depolama temizleme aracını test etmeye başladı. Özellik, medya yönetimini kolaylaştırırken önemli içerikleri koruyor.***

WhatsApp, Android beta sürümünde kanal depolama temizleme aracı üzerinde yürüttüğü çalışmaları daha geniş bir test aşamasına taşıdı. Android 2.26.30.4 beta sürümüyle bazı kullanıcılara sunulan yeni özellik, kanallardan indirilen medya dosyalarının daha kolay yönetilmesini amaçlıyor. Kullanıcılar artık fotoğraf, video, çıkartma ve sesli not gibi içerikleri türlerine göre filtreleyerek




silebiliyor. Ayrıca yıldızla işaretlenen güncellemelerin temizleme işlemi sırasında korunması da mümkün hale geliyor.

## Yeni araç medya yönetimini daha esnek hale getiriyor

Yeni depolama temizleme aracına ulaşmanın ilk yolu kanal bilgi ekranı üzerinden sağlanıyor. Kullanıcılar ilgili kanalın bilgi sayfasına girdiklerinde cihazlarına kaydedilen medya içeriklerini görüntüleyebiliyor ve bunları fotoğraflar, videolar, çıkartmalar ile sesli notlar gibi kategorilere göre filtreleyebiliyor. Bu yaklaşım, özellikle en fazla depolama alanı tüketen dosya türlerini hızlı şekilde belirlemeyi kolaylaştırıyor. Böylece tüm medya arşivini tek tek incelemek yerine yalnızca ihtiyaç duyulan içerikler üzerinde işlem yapılabiliyor.

WhatsApp, temizleme işlemi sırasında yıldızla işaretlenen güncellemeler için de ek bir koruma mekanizması sunuyor. Kullanıcılar önemli gördükleri kanal paylaşımlarını yıldızlayarak saklamaya devam edebiliyor. Temizleme işlemi başlatıldığında bu içerikler varsayılan olarak korunuyor ve yalnızca kullanıcı açıkça silmeyi tercih ederse kaldırılıyor. Bu yaklaşım, depolama alanı boşaltılırken önemli bilgi veya duyuruların yanlışlıkla kaybedilmesi riskini azaltıyor ve medya yönetimine daha güvenli bir yapı kazandırıyor.

WhatsApp ayrıca temizleme aracına ikinci bir erişim noktası da ekliyor. Güncellemeler sekmesinde kullanıcılar bir kanala uzun basarak açılan menü üzerinden "Medya dosyalarını temizle" seçeneğine ulaşabiliyor. Bu yöntemin en dikkat çekici yönü ise aynı anda birden fazla kanalın seçilebilmesi olarak öne çıkıyor. Çok sayıda aktif kanalı takip eden kullanıcılar, her kanalın bilgi ekranına tek tek girmek yerine toplu temizlik yaparak depolama yönetimini daha kısa sürede tamamlayabiliyor.

# Akılalmaz Bir OPSEC Hatası:
# Gelişmiş Casus Yazılım Şirketinin Büyük İfşası

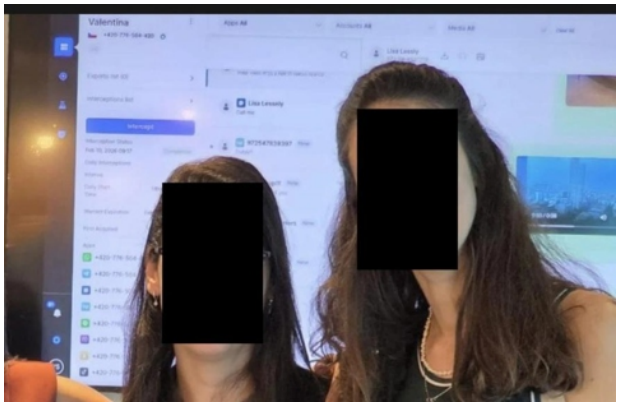
Günümüz dünyasında savaşlar fiziksel dünyada artık topla tüfekle olmaktansa siber dünyaya taşınmış durumda ve bu yeni tür savaşın en büyük araçlarından biri casus yazılımlar oldu. Casus yazılımlar zaman içerisinde devlet destekli operasyonların önemli araçlarından biri haline gelmiştir. Bu alandaki en bilinen üreticilerin önemli bir bölümü İsrail merkezli şirketlerden oluşmaktadır. Daha önce Pegasus yazılımıyla gündeme gelen NSO Group'un ardından, bu araştırmada ele alınacak Paragon Solutions'da İsrail merkezli bir başka casus yazılım şirketidir.

Paragon Solutions şirketi 2019 yılında Ehud Schneorson, Idan Nurick, Igor Bogudlov, Liad Avraham ve Ehud Barak beşlisiyle kurulmuştur. Bu kurucular ekibinin dikkat çeken bir özelliği var. Bu ekipteki kişilerin içerisinde İsrail askeri ve istihbaratı geçmişine sahip isimler bulunmaktadır. Örneğin Ehud Schneorson, İsrail Savunma Kuvvetleri (IDF) bünyesindeki sinyal istihbaratı (SIGINT) alanında faaliyet gösteren Birim 8200'ün (Unit 8200) komutanlığını yapmıştır. Idan Nurick, Igor Bogudlov ve Liad Avraham'ın da daha önceden İsrail İstihbaratı için görev yaptığı belirtilmektedir.

Bu isimler arasında yer alan Ehud Barak ise 1991-2001 yılları arasında İsrail Devletinde sırasıyla Genelkurmay Başkanı, Dışişleri Bakanı, Savunma Bakanı ve Başbakanlık görevlerinde bulunmuştur. Yani bu geçmiş nedeniyle Paragon Solutions, İsrail güvenlik ve istihbarat çevreleriyle bağlantılı bir şirket olarak değerlendirilmektedir.

Graphite, Paragon Solutions şirketinin geliştirdiği bir çeşit gelişmiş casus yazılımdır. NSO Group'un geliştirdiği Pegasus yazılımı gibi, bu yazılım da kurbanın cihazında sıfırıncı gün (zero-day) zafiyetlerden faydalanarak cihazı ele geçirip gizlice izlenmesini sağlayan bir yazılım olarak karşımıza çıkıyor. Peki, bu yazılım ilk ne zaman ve nasıl fark edildi? Bu olayların ilk kırılma noktası 2025 yılında başlıyor. Citizen Lab laboratuvarı bu konu hakkında 2025 yılında ilk analizini yayınlıyor ve analize göre bu olay 2024 Haziran ayına kadar uzanıyor. Paragon Solutions şirketinin açıklamalarına göre terörle mücadele, çocuk istismarı ve insan kaçakçılığını önleme, organize suç örgütlerinin takibi gibi nedenlerle geliştirildiği söylenen Graphite, araştırmalar sonucunda bu amaçlar dışında gazeteciler, aktivistler, insan hakları savunucuları ve sivil toplum kuruluşu çalışanları gibi grupları hedefe aldığı görülmektedir.

En dikkat çekici nokta, bu operasyonların klasik istihbarat hedeflerinden farklı olarak bilgi üreten ve kamuoyu oluşturan kişilere yönelmiş olmasıydı. Bu nedenle Graphite olayı sadece bir siber casusluk vakası değil, aynı zamanda basın özgürlüğü, devlet gözetimi ve ticari casus yazılım endüstrisinin denetlenmesi konusunda uluslararası bir tartışmaya dönüştü. Bu hedeflerden 90 civarı kişi biliniyor ve iki hedefin cihazları incelendiğinde araştırmacılar Graphite yazılımının parmak izine ulaştı. Ancak bu ölçekte operasyonlar gerçekleştiren Paragon Solutions, nasıl büyük bir operasyonel güvenlik (OPSEC) hatası yaptı?



Reut Yamen tarafından paylaşılan fotoğrafın sansürlü hali.

Tarih 11 Şubat 2026, Reut Yamen, Paragon Solutions firmasında Genel Hukuk Danışmanı ve Baş Uyum Yetkilisi. Kendisi LinkedIn hesabı üzerinden Paragon çalışanlarının da bulunduğu bir şirket etkinliğinden bir fotoğraf paylaşıyor. Fotoğraf ilk bakışta normal görünsede fotoğrafı daha detaylı inceleyen araştırmacı Jurre van Bergen, arka planda dikkat çekici bir ayrıntıyı fark etti. Arka planda bir kontrol paneli vardı. Kontrol panelinde Valentina rumuzlu birinin kişisel bilgileri yazıyordu. Bu bilgiler arasında en dikkat çekeni ise telefon numaralarının yanında bulunan uygulama ikonları ve arkada gözüken mesaj içerikleriydi. Yazılım sadece mesajları okumakla kalmıyor üstelik istenilen zamanda müdahale imkanı sunuyordu ve bu kontrol paneli sadece 1 çalışanın dikkatsizliği yüzünden ortaya çıktı. Yani bu kişi operasyonel güvenliğe dikkat etmediği için yılların gizliliği boşuna zarar görmüştü.

Tabi bu olay fark edilince Reut Yamen kısa sürede yayımladığı paylaşımı kaldırıyor ama artık her şey için çok geç kalmıştı, araştırmacılar ekran görüntülerini çoktan yaymaya başlamışlardı. Bu olayda önceden adı geçen Citizen Lab labrotuvarı araştırmacılarından olan John Scott-Railton olayı büyük bir operasyonel güvenlik (OPSEC) hatası olarak değerlendirerek "epic OPSEC fail" ifadesini kullandı. Güvenlik açıklarından yararlanarak gelişmiş gözetim araçları geliştiren bir şirket, bu kez teknik bir saldırıyla değil kendi operasyonel güvenlik hatasıyla gündeme geldi. Bu olayın önemi, herhangi bir exploit veya kaynak kod sızıntısından kaynaklanmıyordu. Graphite'ın saldırı zinciri, zero-day yetenekleri veya teknik altyapısı bu olay ile doğrudan ifşa edilmedi. Ancak bir casus yazılım şirketi için en değerli unsurlardan biri olan gizlilik ve görünmezlik prensibi zarar gördü. Bir güvenlik şirketinin kendi operasyonel disiplinindeki küçük bir hata, yıllarca korunan bir teknolojinin kamuoyunun incelemesine açılmasına neden oldu. Graphite vakası, modern siber güvenlikte önemli bir gerçeği tekrar ortaya koydu. En gelişmiş saldırı araçları bile insan hatasına karşı savunmasızdır.

Güvenlik yalnızca kod, şifreleme veya exploit yeteneklerinden oluşmaz, aynı zamanda çalışanların davranışları, kurum kültürü ve operasyonel disiplin ile şekillenir. Paragon'un hikayesi bu nedenle yalnızca bir casus yazılım hikayesi değildir.

Aynı zamanda teknoloji şirketlerinin sahip olduğu gücün nasıl yönetildiği, devlet destekli siber araçların nasıl denetlendiği ve dijital çağda görünmez kalmaya çalışan aktörlerin kendi hatalarıyla nasıl açığa çıkabileceği üzerine önemli bir örnektir. Sonuç olarak Graphite, teknik açıdan gelişmiş bir gözetim aracının değil, yüksek güvenlik gerektiren bir operasyonun en zayıf halkasının insan olduğunu gösteren bir OPSEC vakasıdır.

**Kaynaklar:**

https://en.wikipedia.org/wiki/Paragon_Solutions
https://tr.wikipedia.org/wiki/Ehud_Barak
https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/
https://www.linkedin.com/in/reut-yamen-885b7b6b/
https://www.linkedin.com/posts/barrotem_on-february-11-2026-someone-at-paragon-activity-7428825040810491904-nxx8
https://x.com/jsrailton/status/2021647308790911384

**Muharrem Öğdü**
Bilgisayar Mühendisliği Öğrencisi
Doğu Akdeniz Üniversitesi 2.Sınıf

**Facebook'ta kişisel verilerinizi korumak için öncelikle Ayarlar ve gizlilik → Ayarlar bölümüne girin. Menü adları telefon veya bilgisayarda küçük farklılıklar gösterebilir.**

Facebook'un Gizlilik Kontrolü aracı; gönderiler, profil bilgileri ve geçmiş paylaşımların hedef kitlesini birlikte gözden geçirmenizi sağlar.

**Hesap güvenliği**

- Facebook'a özel, başka hiçbir yerde kullanmadığınız uzun bir parola belirleyin.
- İki faktörlü kimlik doğrulamayı açın. SMS yerine mümkünse Microsoft Authenticator, Google Authenticator veya benzeri bir doğrulama uygulaması kullanın.
- Tanınmayan giriş uyarılarını etkinleştirin.
- "Giriş yaptığınız yerler" bölümünü kontrol edip tanımadığınız cihazlardan çıkış yapın.
- İki faktörlü doğrulamanın kurtarma kodlarını güvenli ve çevrimdışı bir yerde saklayın.

Facebook, iki faktörlü doğrulamanın yanında tanınmayan giriş uyarılarının kullanılmasını da destekliyor.

**Facebook'un topladığı verileri azaltma**

- **Kişileri sürekli yükleme** özelliğini kapatın; daha önce yüklenen telefon rehberini de silin. Bu ayarı Messenger içinde ayrıca kontrol edin.

**1. Hesaba giriş yapılan cihazları kontrol edin**

**Ayarlar → Hesaplar Merkezi → Parola ve güvenlik → Giriş yaptığın yerler**

- Tanımadığınız telefon, bilgisayar ve konumlardan çıkış yapın.
- Eski telefonlarınızı ve artık kullanmadığınız tarayıcı oturumlarını kapatın.
- Şüpheli bir cihaz görürseniz önce parolanızı değiştirin, ardından diğer oturumları kapatın.

**2. SMS yerine doğrulama uygulaması kullanın**

**Hesaplar Merkezi → Parola ve güvenlik → İki faktörlü kimlik doğrulama**

Önerilen sıralama:

1. Fiziksel güvenlik anahtarı
2. Doğrulama uygulaması
3. SMS

SMS hiç kullanmamaktan iyidir ancak telefon hattı kopyalama saldırılarına karşı doğrulama uygulaması daha güvenlidir. Ayrıca **kurtarma kodlarını** indirip telefon dışında güvenli bir yerde saklayın.

**3. Geçiş anahtarı — Passkey oluşturun**

Bu, az bilinen fakat oldukça önemli bir seçenektir. Telefonunuzun parmak izi, yüz tanıma veya ekran kilidiyle Facebook'a giriş yapmanızı sağlar ve sahte giriş sayfalarına karşı paroladan daha dayanıklıdır.

**Hesaplar Merkezi → Parola ve güvenlik → Geçiş anahtarı/Passkey**

Her cihazda veya hesapta henüz görünmeyebilir.

**4. Hesap kurtarma bilgilerini kontrol edin**

**Hesaplar Merkezi → Kişisel bilgiler → İletişim bilgileri**

- Kullanmadığınız eski telefon numaralarını kaldırın.
- Erişiminiz olmayan eski e-posta adreslerini silin.
- Facebook için güvenli ve düzenli kontrol ettiğiniz bir e-posta adresi kullanın.
- E-posta hesabınızda da iki aşamalı doğrulamayı açın.

Facebook hesabı çoğunlukla bağlı e-posta hesabı ele geçirilerek çalınır.

**5. Profil bilgilerini tek tek gizleyin**

Profilinizdeki Hakkında bölümünü kontrol edin:

- Telefon numarası → Sadece ben
- E-posta adresi → Sadece ben
- Doğum tarihi → Sadece ben veya Arkadaşlar
- Doğum yılı → Sadece ben
- Yaşadığınız şehir → Arkadaşlar
- Aile ve ilişki bilgileri → Arkadaşlar veya Sadece ben
- İş ve okul geçmişi → Gerekmiyorsa kaldırın

Özellikle tam doğum tarihi, telefon ve e-posta bilgileri kimlik doğrulama ve dolandırıcılık girişimlerinde kullanılabilir.

- Telefon ayarlarından Facebook'un **konum iznini** "Asla" veya gerekiyorsa "Yalnızca uygulamayı kullanırken" şeklinde ayarlayın.
- Kamera ve mikrofon izinlerini yalnızca gerektiğinde verin.
- **Uygulamalar ve internet siteleri** bölümünden artık kullanmadığınız bağlantıları kaldırın. Özellikle test, oyun ve "Facebook ile giriş yap" uygulamalarına dikkat edin.
- **Meta teknolojileri dışındaki hareketler** bölümünden geçmiş etkinlik bağlantısını kesin ve gelecekteki etkinliğin kullanılmasını sınırlandırın. Meta dışındaki etkinlikleri yönetme.
- **Reklam tercihleri** bölümünde reklam ortaklarından gelen verilere dayalı kişiselleştirmeyi mümkün olduğunca azaltın.

**Paylaşırken dikkat edilmesi gerekenler**

Kimlik kartı, uçak bileti, ev adresi, telefon numarası, çocukların okul bilgileri, canlı konum, tatil süresi ve banka bilgileri paylaşılmamalıdır. Profil ve kapak fotoğrafları gibi bazı profil bilgilerinin herkese açık olabileceğini de unutmayın.

En hızlı başlangıç için şu dört işlemi yapmanız yeterlidir: **Gizlilik Kontrolü'nü çalıştırın, eski gönderileri sınırlandırın, etiket incelemesini ve iki faktörlü doğrulamayı açın.**

**Önerilen gizlilik ayarları**

| Ayar | Önerilen seçim |
|---|---|
| Gelecekteki gönderileri kim görebilir? | **Arkadaşlar** |
| Hikâyeleri kim görebilir? | **Arkadaşlar** veya **Özel** |
| Eski gönderilerin görünürlüğü | **Geçmiş gönderileri sınırla** |
| Arkadaş listenizi kim görebilir? | **Sadece ben** |
| Telefon, e-posta ve doğum tarihi | **Sadece ben** |
| Arkadaşlık isteği gönderebilenler | **Arkadaşların arkadaşları** |
| Telefon/e-posta üzerinden profil önerisi | Mümkün olan **en dar seçenek** |
| Facebook dışındaki arama motorlarının profilinize bağlantı vermesi | **Kapalı** |
| Başkalarının profilinizde paylaşım yapması | **Sadece ben** |
| Etiketlendiğiniz gönderilerin profilinizde görünmesi | **Önce inceleme açık** |
| Gönderilerinize eklenen etiketleri inceleme | **Açık** |

# Geç Kalıyoruk!

***Aslında istediğimiz şey çok fazla değil, son derece basit, kolay uygulanabilen ve istenirse karşılık görebilen bir şey. Biz bu toplumun ve bu ülkenin içinden yetişmiş gençler olarak toplumumuza gerek özel sektör, gerekse de devlet kurumlarında nitelikli siber güvenlik hizmeti vermek istedik her zaman ve bunun için de bir cyber sem istedik ki bu alanda iyi eğitimli, liyakatli, deneyimli ve kaliteli insan kaynağı oluşturabilelim ve cyber sem sayesinde bu da süreklilik arz eden bir yapıya dönüşsün. Şimdi size biz sibercilerin çektikleri sıkıntıları ve başlarına gelenleri anlatacağım biraz da karşılaştığımız sektör gelişmelerini aktardığım zaman neden cyber sem yapısını istediğimizi anlayabileceksiniz.***

**BU ÜLKEDE SİBERCİ OLMAK İSTEDİĞİNİZ ZAMAN YAŞADIĞINIZ SIKINTILAR:**

Bu ülkede önemli kurum, kuruluş ve şirketler var ve dolayısıyla nasıl ki diğer dünya vatandaşlarının siber güvenliğe gönül verenlerinin hakkıysa gereken hizmet edebilme şansını bularak bu kritik sistemlerle verilerin güvenliğini sağlayabilmek haklarıysa bu bizim de hakkımız diyorsunuz ve bunun için çaba sarf etmeye başlıyorsunuz fakat birazdan aşağıda maddeleyeceğim sıkıntılarla karşı karşıya geliyorsunuz:

**SİBER GÜVENLİK ALANINDA KENDİNİZİ GELİŞTİREREK YETKİNLİK SAHİBİ OLABİLECEĞİNİZ HİÇBİR YER YOK:**

Şimdi diğer ülkeleri incelediğiniz zaman çok çeşitli akademiler, siber güvenlik şirketlerinin açtıkları bootcamp'ler, kendi bünyelerinde öğrencileri personelleri olarak yetiştirmek için sağladıkları eğitimler ve onlara kazandırdıkları sertifikasyonlar + mesleki tecrübe ve deneyimler ve çeşitli devlet kurumlarının bu alan için sağladıkları eğitimlerle sertifikasyonların olduğunu görebilirsiniz. Hatta belirli zamanlarda indirim bile yaparlar bu tarz siber güvenlik sertifikasyon eğitimlerinde çünkü amaçları bu alanda mümkün olduğunca çok sayıda iyi eğitilmiş, liyakatli, tecrübeli ve kaliteli insan kaynağı elde etmektir. Peki bizde durum nedir? Bizde sizin başvurup eğitim alabileceğiniz veya sertifikasyon ihtiyacınızı giderebileceğiniz hiçbir yer yoktur. Hz. Google'la mı akraba olmazsınız? Youtube'la mı içli dışlı olmazsınız? Blogları v.s. mi okumazsınız? Telegram, Discord, Whatsapp v.s. gibi mecralarda ki hacker gruplarıyla internetteki hacker forumlarına üye olup alabileceğiniz kadar bilgi almaya mı çalışmazsınız? Yoksa free online eğitimler mi düşürmeye çalışmazsınız? Bunların hepsini de mecburen yapacaksınız. Çünkü maalesef bu memlekette başka bir şansınız yok. Ancak bu şekilde kendinizi bu alanda geliştirebilirsiniz. Üniversitede öğrenciyim, ben bilgisayar mühendisliği okuyorum bazı arkadaşlarım var MIS okuyorlar. Ders programını iple çekerdim acaba siber güvenlikle alakalı dersim olacak mı ama maalesef olmazdı MIS deki arkadaşlarımsa Security dersleri alıyorlardı hatta sayısından bunalmışlardı, kaç kere dedim yahu hocam ben siber güvenlik uzmanı olmak istiyorum ve benim gibi başka arkadaşlarım da var niye bize de güvenlik dersleri koymuyorsunuz? Fakat maalesef yine tek bir siber güvenlik dersi konmazdı bize sanki biz cezalıydık da bizim hakkımız yoktu siber güvenlikle alakalı ders almaya. Siber güvenlikle alakalı iki gram olsun işlenen derslerimiz genellikle network ve operating systems gibi derslerimiz olduğu için en çok onları iple çekerdim (Gerçi network 2 de siber güvenlikle alakalı açlığımdan dolayı aşırıya kaçtığım için hoca beni dersten kovmuştu bu bir güvenlik dersi değil Cem diyerek.). Allahtan Yazılım Mühendisliği dersini veren hocamız bana kendi yazılım şirketiyle alakalı bir siber güvenlik görevi vermişti. Tabi kolay olmadı epeyi başını şişirmek zorunda kaldım hocanın ama mecburdum. Çünkü bu alanda imkanlar kısır olduğu için bulduğum veya bulabileceğim her fırsatı değerlendirmem gerekiyordu. Sonra laboratuvarlarda cmd üzerinden diğer bilgisayarlarla konuşmaya çalışıyordum, tatil dönemlerinde iş dneyimi edinmek için çalıştığım newtech de yine kendi ısrarlarımla sağolsun genel müdürümüz bana siber güvenlikle alakalı sunumlar yaptırıyor, bilgilendirme toplantısı yapmaya gelen trend micro yetkilisiyle olan toplantıya sokuyor, abilerimin sayesinde fidye virüsüyle ki o zamanlar henüz yeni yeni çıkıyordu mücadele için keşfedilen metodları öğreniyordum hatta cyberoam firewall eğitimini de youtube üzerinde free şekilde almama da vesile olmuşlardı, hatta yine genel müdürümüz bana siber güvenlikle alakalı bir proje yaptırmıştı çok mutlu olmuştum. Yani demek istediğim şey bizde gerek kısıtlı imkanlardan gerekse de var olmasına rağmen size sunulmayabilen imkanlardan dolayı eğer siber güvenlik uzmanı olarak toplumunuza, değerli kurum, kuruluş ve şirketlerin sistemleriyle verilerinin güvenliğini sağlamak isterseniz bir yandan internetten ne öğrenebilirseniz öğreneceksiniz ve fırsatını bulduğunuzda yani bu alanla alakalı ücretsiz ve hatta hem ücretsiz hem de sertifikalı eğitimleri yakaladığınız zaman affetmeyeceksiniz ve aynı zamanda maalesef gerek hocalarınızın gerekse de çalıştığınız yerler varsa oralardaki insanların başlarını şişireceksiniz ki size siber güvenlikle alakalı bir şeyler yaptırsınlar ve en azından ileride çıkıp bende şunları şunları ve bunları bunları yaptım deyebilesiniz. Sadece bu konuda dünyadaki meslektaşlarımızdan kaç sıfır geride başlıyoruz farkında mısınız?

**SİBER GÜVENLİK ALANINDAKİ MEZARCILAR VE YALANCILAR:**

Bazı insanlarla tanışırsınız bu alanda iş yapıyorlardır ama bunu açık etmezler abi benda siberci olacam banada yardımcı olur musun dersiniz ama aksine onlar sizi uzak tutmaya çalışırlar bu işi sadece kendileri yapsınlar diye sanki bana mesleği mezara götürecekler ve mezarda da bu işi yapabilecekler. Halbuki bu yaptıklarıyla aslında kendileri bu mesleğe zarar veriyorlar çünkü böyle yaptıkları için kendilerinden sonra bu işi yapabilecek deneyimli ve tecrübeli insan kaynağı

olamayacağı için bu alanda destek alınabilecek insan olmadığından bir süre sonra bu işi iki gram dahi yaşıyorsa tamamen ölmek zorunda kalır. Bir de yalancılarla uğraşmak zorunda kalabiliyorsunuz. Mesela ben bunlardan birini tanıdım. Kendisi GAÜ de akademisyen di ve CEZERİSGA Etkinliğini düzenleyen kulübün başındaysı o zamanlar hiç unutmam CEZERİSGA'nın kurucusu ki şimdi GAİS Security'nin başındadır sayın Osman Doğan'la etkinliğin bitişinde bir araya geldiğimizde dedim ki bizim sizin gibi kıymetli siber güvenlik uzmanlarından sürekli olarak eğitim alabileceğimiz ve arkasından da sertifika ihtiyacımızı karşılayabileceğimiz bir yere ihtiyacımız var. Tam da o sırada yalancı akademisyenimiz oradan geçerken Osman Doğan seslendi "Bakın öğrenci arkadaşımızın isteği var ben de Osman Doğana dediğimin aynını söyledim ve dedim yani böyle bir yere ihtiyacımız var bu memlekette siber güvenlik uzmanı olabilmemiz için." Yalancı akademisyen de Osman Doğanla benim gözlerimizin içine bakarak "Ya tabii ki hocam siz hiç merak etmeyin zaten biz de şuanda yer bakıyoruz bulacağız ve ayarlayıp halledeceğiz hocam dedi." Osman Doğan da sonra bana dönüp bak duydun takipçisi ol dedi. Peki sonra ne oldu dersiniz? Ben bu yalancıyı takibe aldım sosyal medya hesaplarından ve belli aralıklarla sormaya başladım "Selamlar hocam Cezerisga Etkinliğinde Osman Doğanla bana bir söz vermiştiniz burada bir eğitim merkezi kuracaktınız ne oldu durum nedir?" Aldığım cevap "Henüz gündemimizde yok." Düşünün ki aradan seneler geçti ben üniversiteyibitirdim askere gitmeden önce sordum yine aynı cevap. Askerlik bitti, pandemi geçti v.s. derken 2025 Ekimin'de bir siber güvenlik etkinliğinde tekrardan bu yalancıya rastladım. Kendisi konuşmacıydı etkinlikte, etkinliğin sonunda yanına gittiğimde öğrendim ki kendi siber güvenlik şirketini kurmuş. Dedim ki peki hocam bu şirkette çalışabilir miyim? Bana siz nerdesiniz diye sordu söyledim. Dedi ki çok iyi sizi hem Lefkoşa hem de Girnedeki şubelerimizde değerlendiririz. Yalnız biz yılda sadece 2 kez alım yapıyoruz o da Mart ve Eylül Aylarında Eylülü geçtik dolayısıyla seneye Martta gelin görüşelim. Ben de tamam dedim. Aradan zaman geçti Mart geldi. Dedim ki fazla gecikmeyim Mart'ın ilk haftası gideyim konuşalım. İlk gittiğim gün kapı duvardı bulabildiğim tüm şirket numaralarını aradım ve kendi numarasını da hem normal hem de whatsapp dan defalarca aradım ve mesaj attım fakat ulaşamadım. Dedim ki bu GAÜ de akademisyen di belki de okulunda derstedir okuluna gideyim hop Lefkoşadan ta GAÜ ye gittim. Kendisiyle görüşmek istediğimi söyledim sağolsun güvenlik beni yönlendirdi. Bana tarif edilen yere gittiğim de oradaki bir kadın akademisyen bana "O çoktan bıraktı bizi. Baktı ki yürütemeyyor vazgeçti bu işten. Şimdi sadeceşirketi ve BRT'deki programıyla uğraşıyor dendi." Bir sonraki gün şirketini önce sabah aradım ulaşamadım kimseye, öğleden sonra aradığımda nihayet karşıma bir muhatap çıktı. Dedim ki böyle böyle durum. Aldığım cevap kendisi bir süredir yurt dışında, bizde ekibi olarak arıyoruz ama ona ulaşamıyoruz oldu. Dedim ki sizinle görüşsem olmaz mı? Aldığım Cevap: Benim veya başkasının işe alım yetkisi yok maalesef o yetki sadece patronda var ben kendisine ulaşabildiğimde ileteceğim dedi. Ben de ulaşmaya çalışmaya devam ettim kendisine telefoniyen hem whatsapp hem de normal sms ve aramayla. Martın son günleriydi şirkete gittim nihayet telefonda görüştüğüm muhatabımla fiziksel olarak görüşüp tanıştık, ona bilgisayarımdan cv mi, referanslarımı, rozetlerimi ve sertifikalarımı gösterdim. Maalesef hala gelmedi dedi. Ama gelince mutlaka sizden bahsedeceğim dedi. Mart bitti Nisan a girdik. Arıyorum ulaşamıyorum, yazıyorum dönüş yok. Nisan'ın ortalarına geldik. Radyo programında konuk olarak konuşup adaya yeni döndüğünü söyledi. Ondan sonra bir kaç kere daha hem whatsapp'dan hem de normal SMS ve aramayla ulaşmaya çalıştım ama hiçbir geri dönüş alamadım. Düşünebiliyor musunuz? Onca imkansızlığın ve sıkıntının içinde bir de böyle, etiği etiket olarak gören ama etikle uzaktan yakından alakası olmayan, insanlara yalan söyleyip onlara bu şekillerde kazık atan, kötü ve yalancı insanlarla da uğraşmak zorunda kalıyoruz bu işi yapabilmek için. Halbuki diğer dünya vatandaşlarının hiç böyle dertleri yoktur onlar ne mezarcılarla ne de böyle yalancılarla uğraşmak zorunda kalmadan kendilerine bu alanda iş bulabiliyorlar.

**BURNU BÜYÜKLER:**

Bu alandaki bir diğer sorunumuz bazı şirketler var ki sanki memleket diğer memleketlerin sunduğu tüm şartları sunmuş, ortalık bu alanda kaliteli insan kaynağı kaynıyormuşcasına bir şımarıklık ve burnu büyüklük içindedirler. Siber güvenlikle alakalı münhal açarlar, online olarak cv ni gönder derler, cv ni yollan ve bir yüz yüze görüşmeye dahi çağırmazlar veya çıkar sana siber güvenlik etkinliğinde bu alanda isteyen gelsin beraber çalışalım dersana ama linkedin'den zar zor ulaşın adama bana kendini yani yaptıklarını anlat der sana, sen daha anlatırken yani anlatımını bitirmeden ama sen benim beklediğim seviyede değilsin deyip kestirip atar seni. Halbuki sen daha anlatmanı bitirmedin bile. Belki sonuna kadar beklese farklı olacak ama kestirir atar. Bakın size yemin ederek söylerim ben bu zamana kadar ne yaptıysam hep etik çizgide kalmaya çalıştım her zaman birine ısrar edip ondan izin alarak ne yaptıysam yaptım ve böyle biri olarak çok rahatlıkla söyleyebilirim ki benden daha iyi ve tecrübeli insanların hepsi karanlık tarafdaydılar ve sonradan etik tarafa geçtiler. Buna yemin edebilirim ama ıspatlayamam. Ama şunu da bilirim ki o karanlık yönleri mutlaka karşılarına çıkar kaybolup gitmez. Bunu Bilişim Academy'nin ücretsiz düzenlediği online etkinliklerden birinde bir siber güvenlik uzmanından öğrenmiştim. Bir arkadaşı başlarda karanlık taraftaymış sonra etik tarafa geçmiş ama bir gün iş yaparlarken sen filanca siber suçu işleyen değil misin? Demişler. Aradan o kadar süre geçmiş hatta arkadaşı da unutulmuştur diye düşünürken unutulmadığını anlamış ve bize söylediği karanlık taraftaysanız o karanlık iş bir gün mutlaka karşınıza çıkar ben artık etik oldum rahatım diyemezsiniz oldu. Bu yüzden ben de derim ki benden daha deneyimliler bir zamanlar karanlık tarafta olupta etik hacker'lığa geçenlerdir. Çünkü size paylaştığım deneyimlerime bile baksanız görürsünüz ki insanlara bol bol ısrar etmeden insanlardan izin alabilmeniz mümkün değil. Ancak karanlık taraftaysanız mümkün sonuçta onların amacı zarar vermek olduğu için izine ihtiyaçları yoktur. Bir de böyleleriyle uğraşmak zorunda kalıyoruz.

**BU İŞE GEREKEN ÖNEMİ VERMEYENLER:**

CV'nizi atıp başvurduğunuz bazı yerlerse sizi yüz yüze görüşmeye çağırıyorlar veya bazen telefoniyen görüşüyorsunuz ama ne zaman siber güvenlik alanında kendinizi geliştirdiğinizi ve yetiştirdiğinizi ve bu alandaki bilgilerinize dayanarak bu işi istediğinizi belirtmenize ve başvurduğunuz pozisyonunda siber güvenlikle ilgili

olmasına rağmen siber güvenlik bizim için de önemli ama şeklinde geri dönüşler alabiliyorsunuz. Yani sanki siber güvenliği çok önemsiyormuşlar gibi cümleler kurarlar ama aslında o kadar da önemsemezler.

**SAMAN ALEVİ GİBİ ARADA PARLAYAN AMA UZUN SÜRE YOK OLAN ORGANİZASYONLAR:**

Cypsec'le başlayan siber güvenlik etkinlikleri, CEZERİSGA gibi geçici etkinlikler ve bir keç tane BTVizyon etkinliğinden sonra organizasyonlar aniden bıçak gibi kesildi. Ben askerliğimi bitirdikten sonra 2020'de ansızın televizyonda Kıbrıs'ın Siber Kahramanlarını gördüm ve deneyimlerime dayanarak dedim ki içimden zaten bizde bu tür organizasyonların genelde sürekliliği yok bir başlar ansızın durur şimdi varken girecem ki yararlanabileyim. Nitekim tam organizasyona girdim yani fiziksel oturuma katıldım, online sınava girip geçtim, uygulamalı eğitim kampına katıldım, ctf'de yarıştık v.s. şimdi biz hepimiz beklerik ki proje devam etsin artık ikinci kamp olsun bitsin ve vaad edilen yerine getirilsin yani siber güvenlikle alakalı iş isteyene iş, staj isteyene staj, burs isteyene burs, kurs isteyene kurs. Ne güzel değil mi? Fakat ansızın önce projenin ikinci kısmı değiştirildi, sonra proje devam etmeyip patladı. Ondan sonra adamızda yapılan etkinlik Ekim 2025'te düşünün siber güvenlikle alakalı organizasyonların bile süreklilik arz edemediği saman alevi gibi aniden ortaya çıkıp sonra uzun süre hiçbir şeyin olmadığı bir yerdeyiz maalesef. Öyle ki Lisani Deniz bile genellikle kendisinden sonra organizasyonların devam etmemesinden bıkıp usanmış olacak ki cypsec'le uzun süredir hiçbir organizasyon veya etkinlik gerçekleştirmiyor.

**Sektördeki Meslektaşlarımızın Seslerini Çıkartmayarak Düzenin Devamını Sağlaması:**

Sen Yazılımcı, sen analist-programcı, sen db'ci. Aslında bir anlamda hepiniz yani tüm IT Departmanı Çalışanları, bilerek veya bilmeyerek bize zarar veriyosunuz. Şöyle ki hem her şeyin size yıkılmasından şikayet ediyorsunuz ama hem de siber suçlar meydana geldiğinde aylarca evime gitmedim ben demekle yetiniyorsunuz. Peki o zaman soru şu hiç bu tip bir olayın ardından amirlerinize gidipte şöyle itirazlar yaptınız mı: efendim bu düzende çok yoğunuz ve iş yükümüz fazladır, bunca yükün arasında sizde görüyorsunuz siber güvenliğe gereken zamanı ayıramıyoruz o yüzden bizlere bu konularda destek olabilecek siber güvenlik ekipleri oluşturmalısınız. Hem insanımıza istihdam olur, hem de siber güvenlik için özel olarak bu ekipler uğraşacağından dolayı kurumsal siber güvenlik seviyemiz çok yükselir veya bu yapıda siber tehditlere açık hale geliyoruz ve biz bunlarla başa çıkamıyoruz dolayısıyla lütfen siber güvenlik ekipleri oluşturun ve bu ekiplere gereken alımı yapın ki güvende olalım v.s. Maalesef hepiniz de sadece her şeyin üstünüze yıkıldığını, bu tip olaylarda uzun süre doğru düzgün dinlenemediğinizi söylersiniz ama patron, amir veya müdürlerinize bu konularda ses çıkartmazsınız. Haliyle onlarda derler ki madem bunlar hallerinden memnun hiç gıkları çıkmıyor ben neden siber güvenlik için ekstra masraf yapayım. Dolayısıyla bilmeden/istemeden de olsa bize en çok zararı verenlerden biri de bu pasifliğinizle siz oluyorsunuz. Halbuki tepkinizi verseniz bizlere hizmet etme şansı yaratmış olacağınız gibi kendiniz de; siber güvenlik, bilgi güvenliği, felaket kurtarma ve müdahale/CSIRT senaryolarıyla planları, yama yönetimi ve bu tip süreçlerin yönetilmesiyle, bu süreçlerle ilgili politikaların oluşturulması, uygulanması ve güncellenmesi, personelin bu konularda eğitilmesi ve bilgilendirilmesi, konfigürasyon ayarları, devsecops v.b. konuları bizlere bırakıp belirli alanlarda olsun kendinizi rahatlatma şansı bulacaksınız ama maalesef ki bunu yapmıyorsunuz ve bu da bizi kızdırıyor!

**Geçmişteki Olaylardan Ders Çıkartmamak:**

Geçmişten beri onca başarılı siber saldırı gerçekleşmesine rağmen hala ders çıkartılmıyor. Her olayda acaba bu kez akıllanıpta bizim gibi insanlara gereken imkanlarla hizmet etme fırsatını tanıyacak siber güvenlik ekibi yapılanmasına gidilecek mi diye bakıyorsunuz, bekliyorsunuz, ümit ediyorsunuz ama bir bakıyorsunuz ki ilk başlarda herkes bağırıyor çağırıyor ama sonra da kendi kabuğuna çekiliyor ve olay unutuluyor ne zamana kadar mı? Taa ki yeni bir siber saldırı vakası yaşansın ve ortaya çıkartılsın ama bir süre sonra yine aynı durum yaşanıyor. O zaman sormazlar mı madem ki gerçekte umurunuzda değil niye yaygara yapıyorsunuz? Niye canınız yanmış gibi ortalığı velveleye veriyorsunuz? Niye bas bas bağırıyorsunuz ki? Madem aslında siber güvenlik, bilgi güvenliği v.s. gibi şeyler umurunuzda değil boşuna bu saydıklarımı neden yapıyorsunuz ki?

**Yok Sayılmanız:**

Bu ülkede; Teknisyenin herhangi bir teknik servise veya teknoloji şirketine veya herhangi bir IT Departmanına girme ve orada çalışıp hizmet etme hakkı var, Yazılımcının herhangi bir yazılım şirketine veya teknoloji şirketine veya herhangi bir IT Departmanına girme ve orada çalışıp hizmet etme hakkı var, networkcünün herhangi bir ISP şirketine veya teknoloji şirketine veya herhangi bir IT Departmanına girme ve orada çalışıp hizmet etme hakkı var, DB cinin herhangi bir şirkete veya teknoloji şirketine veya herhangi bir IT Departmanına girip hizmet etme hakkı var, v.s. diye gider ama siz bir siberci olarak herhangi bir şirkette veya teknoloji şirketinde veya IT Departmanında siber güvenlik uzmanı olarak çalışamazsınız. Etkinliklerde bile bu böyledir. Siber Güvenlikle alakalı etkinlikler genelde boş geçer ama başka bişey olsa hurra dolup taşar, Siber Güvenlik alanında çalışmak istediğinizde size yukarılarda bir yerde söylemiş olduğum cümle söylenir; Siber Güvenlik bizim içinde önemli hatta çok önemlidir ama! Anlayacağınız bu ülke için o vakit geldiğinde ne işiniz var ne de siz varsınız demektir. Resmen yok sayılırsınız neden? Çünkü ülkenizin çok önemli şirketleri, kurum ve kuruluşları, sistemleri ve verileri bünyesinde bulundurduğunu ve dolayısıyla onlarında korunması gerektiğini düşünerek siber güvenliğe de gönül veren biri olarak hizmet etmek istediğiniz için cezalandırılırsınız/cezalandırılmanız gerekir de o yüzden. Sonuçta böyle düşünmek suçtur değil mi? Bir insanın ne haddine kendi ülkesindeki önemli yerlerin, önemli sistemlerin ve önemli bilgilerin verilerini koruyacakmış. Ne büyük kabahat değil mi? Aslında idam etmeniz lazım böyle bir şeyi istediğimiz için. Sonuçta diğer ülkelerde yaşayanların böyle bir hakkı olabilir ama burası KKTC dir burada Allah korur o yüzden bizde haddimizi aşıpta bu işe talip olduğumuz için suçluyuz herhalde. Peki ama bir şeyi çok merak ettim Allah bu bizim sibernetik sistemleri ve verileri bir anlamda da önemli yerleri koruyorsa bu siber saldırılar nasıl gerçekleşebildi?

**ÇÖZÜM:**

**CYBER SEM HAYATA GEÇİRİLMELİ:**

CYBER SEM Siber Güvenlik Sürekli Eğitim Merkezidir ve amacı bu toplumun ve

bahsettiğim kritik yerler, sistemler ve verilerin siber güvenlik, bilgi güvenliği, bunların politikaları, diğer alakasız personelin gerektiği kadar bilgilendirilmesiyle eğitilmesi faaliyetleri, felaket kurtarma ve olay müdahale CSIRT planları, senaryoları ve süreçleri, yazılım güvenliği yaşam döngüsü, güvenli yazılım geliştirme, siber tehdit istihbaratı ve siber istihbarat, açık kaynak istihbarat, tehdit modelleme, Güvenlik Operasyonları Merkezi (SOC - Security Operations Center), Mor Takım Görevleri v.s. konularında yetkin, bilgili, deneyimli ve liyakat sahibi insan kaynağını bu topluma kazandırmak için kurulacak özerk ve bağımsız bir kurumdur. Üç tane fonu vardır bunlar; İstihdamı Destekleme Fonu, Personel Fonu ve CYBER SEM Bakım, Onarım, Tamirat Ve Tadilat Fonu.

**İstihdamı Destekleme Fonu:**
CYBER SEM'den yetişen insan kaynağının çeşitli şirket, kurum, kuruluş, özel sektör ve kamu'da istihdam edilebilmesi için kullanılacak fon olup bu insan kaynağının sosyal sigorta primleriyle ihtiyat sandığının %100'ünü karşılarken maaşının da %10'unu karşılayacak ve böylece ilgili yerler bu insan kaynağının sadece normal maaşının %90'ını ödeyecekler.

**Personel Fonu:**
Öğretim görevlileri dahil olmak üzere CYBER SEM'in ihtiyaç duyduğu tüm personelinin hem sosyal sigorta primleriyle ihtiyat sandığının hem de maaşlarının %100'ünü karşılayacak olan fondur.

**CYBER SEM Bakım, Onarım, Tamirat Ve Tadilat Fonu:**
Adından da anlaşılabileceği gibi bu fon tamamen CYBER SEM'in bakım, onarım, tamirat, tadilat ve gereği halinde de gerek teknolojik alt yapı, gerekse de diğer ihtiyaçlarının karşılanması, yenilenmesi veya en çağdaş halde tutulması için gereken tüm ihtiyacını karşılayacağı fondur.

**CYBER SEM'İN GELİRLERİ:**
Eğitim ve Sertifikasyon Sınav harçlarından alınacak olan gelirler.
Denetimler sırasında tespit edilecek usulsüzlüklerden alınacak olan gelirler.
Bu alanda daha sonra kurulacak şirketlerden alınacak CYBER SEM Katkı Payı.
Özel Sektör ve Kamunun takdir etmesi durumunda CYBER SEM e vereceği destek.
İsterseniz bunları açalım:

**Eğitim & Sertifikasyon Sınav Harçlarından Alınacak Olan Gelirler:**
Dünyadaki her örnek gibi CYBER SEM de ilgili siber güvenlik eğitiminin ve onunla ilgili sertifikasyon sınavının standart başvuru harcını alacaktır. Yine her örnek gibi isterse belirli zamanlarda yani özel günlerle tarihlerde mesela bu harçlardan indirim de yapabilir. Ancak yapılacak olan indirim miktarı hiçbir halde Aylık Net Asgari Ücretin %10'undan, başka bir deyişle 10'da bir'inden aşağıda olamaz.

**Denetimler Sırasında Tespit Edilecek Usulsüzlüklerden Alınacak Olan Gelirler:**
Kurum diğer kurum ve kuruluşlardan bağımsız olarak her yeri kullanılan BT Donanımı standartlara uygun mu? Ayarları olması gerektiği gibi yapılandırılmış mı? Siber Güvenlik Ve Bilgi Güvenliği Politikaları Doğru Şekilde Oluşturulup Uygulanıyor mu? Tüm personele SOC Ekibi yani Mor Takım tarafından belirli aralıklarla Siber Güvenlik Ve Bilgi Güvenliği Ve Sosyal Mühendislik Farkındalık Eğitimleri veriliyor mu? Felaket Kurtarma Ve Olay Müdahale (CSIRT) Planlarıyla Senaryoları düzgün oluşturulmuş mu? Bunlarla ilgili belirli periyotlarla tatbikatlar yapılıyor mu? Bu tatbikatlar sırasında yolunda gitmeyen bir şeyler tespit edilmişse gereken yapılıyor mu? İlgili SOC Ekibi olması gerektiği gibi sadece kendi işini mi yapıyor? Yoksa diğer IT Personelleri gibi alakasız işler de mi yaptırılıyor? Bu tür konularda rastgele ve aniden denetimler yapan ve bu konuların birinde, bir kaçında veya tümünde tespit edilecek usulsüzlüklere göre ağır para cezaları uygulayarak bu gelirleri elde eder. Kurum bu incelemelerinde Kıbrıs Türk Bilgisayar Mühendisleri Odasının oluşturduğu Yazılım Standartları, BT Donanım Standartları, Network Standartları, Sistem ve Sistem Odası Standartları, Konfigürasyon Yapılandırma Standartları v.s. Standartların tümünü göz önünde bulundurarak değerlendirmelerini bu standartlarca yapar.

**Bu Alanda Daha Sonra Kurulacak Şirketlerden Alınacak CYBER SEM Katkı Payı:**
CYBER SEM'den yetişen insan kaynağının içinden bazıları illaki dünyaya ve KKTC'deki duruma bakarak belirli siber güvenlik alanlarına odaklanan Siber Güvenlik Şirketleri kuracaklardır. Ama bunu bir yerde CYBER SEM'e de borçludurlar. Bundan dolayı belirlenecek bir miktarı her ay sabit şekilde CYBER SEM Katkı Payı olarak CYBER SEM'e ödeyecekler.

**Özel Sektör Ve Kamunun Takdir Etmesi Durumunda CYBER SEM'E Vereceği Destek:**
Sağladığı bu nitelikli insan kaynağından dolayı eğer özel sektör ve/veya kamu isterse kendi istediği kadar belirlediği bir miktar parayı CYBER SEM'e destek için hibe edebilir. Ama bunun için zorlanamaz.

Bu şekilde hayata geçirilecek bir CYBER SEM yapılanması sayımızı artırır, bizi nitelikli, iyi eğitimli, deneyimli ve liyakatli insan kaynağına dönüştürür, ihtiyaç duyan her yerin ihtiyacını bu kaliteli insan kaynağından karşılaması sağlanır, önemli şirket, kurum, kuruluş, sistemlerle verilerin siber güvenlik ve bilgi güvenliği seviyesi çok yükselir ve ayrıca siber tehdit aktörleriyle siber saldırılara karşı son derece dirençli hale gelir, Felaket Kurtarma Ve Olay Müdahale Süreçleri son derece etkili şekilde yürütülür ve uygulanacak denetimlerle de bu yerlerin ilgili yetenekleri ciddi şekilde yükseltilmiş/artırılmış olur.

**Doğru Düzgün Siber Güvenlik Ve Bilgi Güvenliği Politikaları Hayata Geçirilmeli:**
Herhangi bir yerin siber güvenliğiyle bilgi güvenliği politikalarını realist şekilde hayata geçirebilmek, doğru şekilde uygulayabilmek, güncellenmesi gereken yerlerini güncellemek, değiştirilmesi gereken yerlerini değiştirmek ve eğer gerekiyorsa mevcut politikalarını tümden yürürlükten kaldırıp yenilerini oluşturmak o yerin değerlerinin tümü için siber savunmasıyla bilgi güvenliğini sağlamak yolunda atacağı ilk adımdır. Kesinlikle ütopik, karmaşık, irreal, kompleks v.s. olmamalıdırlar. Uygulanabilir, rasyonel, net, anlaşılır ve rollerle sorumlulukların da net şekilde dağıtıldığı/paylaştırıldığı bir yapıları olmalıdır.

**Doğru Düzgün Felaket Kurtarma Ve Olay Müdahale (CSIRT) Planları Ve Senaryoları Oluşturulmalı:**
Eğer herhangi bir felaket ve/veya olay başınıza gelmişse ve sizin bunlara dair hiçbir hazırlığınız yoksa başı kesik tavuk gibi davranarak işleri daha da içinden çıkılamaz hale getirip siber tehdit aktörlerinin ekmeklerine yağ sürebilirsiniz. Bu durumun önüne geçebilecek tek yol sizin kendi ihtiyaçlarınızı göz önünde tutarak doğru

düzgün oluşturacağınız Felaket Kurtarma Ve Olay Müdahale Planlarıyla Senaryoları oluşturmanızdır. Bunları da belirli periyotlarla tatbikatlar yaparak test etmeli, bu planlarla senaryolarda sorun varsa sorunlu yerler değişmeli, eğer tümden sorunluysa bunlar iptal edilip yenileri hayat geçirilmeli, eğer personellerin bir kaçında/bazılarında/sadece birinde sorun varsa onlar bu konularda ayrıca eğitilip bilinçlendirilerek ilgili Felaket Kurtarma Ve Olay Müdahale Planlarıyla Senaryolarına uyum sağlamaları sağlanmalıdır.

**Standartlar:**

Bu yaşanan olaylar bir kez daha bize gösterdi ki yalnızca EMO Standartlarıyla bu çağda bu işi götürmemiz imkansızdır. Mutlaka aynı şekilde hazırlanıp uygulamaya konacak ve gerekirse de zaman zaman değişiklikler, güncellemeler, yükseltmeler, düzeltmeler v.s. yapılarak içinde olunan çağdaş koşullara adapte edilecek bilişim standartlarına ihtiyacımız vardır. Bunlar; Yazılım Standartları, BT Donanım Standartları, Kablolu Ve Kablosuz Ağ Standartları, Konfigürasyon Yapılandırma Standartları, Sistem Standartları, Sistem Odası Standartları v.s. gibi bilişimle alakalı aklınıza gelebilecek hemen her şeyin bir standardı olmalı ve bu standartlardan ilgili olanı/olanları karşılayamayan hiçbir bilişim teknolojisi kullanılamamalıdır.

Görüldüğü gibi aslında en acili CYBER SEM'dir. CYBER SEM ve ortaya konacak Bilişim Teknolojileri Standartlarıyla çok iyi yerlere gelebilir ve hatta belki bazı ülkeleri geride bile bırakabiliriz.

CYBER SEM bizim yok sayılmamamızı sağlar.

CYBER SEM bizim layıkıyla işimizi yapabilmemizi sağlar.

CYBER SEM dolaylı yoldan yaratacağı insan kaynağının içinden çeşitli konularda bir araya gelecek insanların belirli alanlarda kaliteli Siber Güvenlik Şirketleri kurmasını sağlayarak yurt dışına Siber Güvenlik Hizmetleri ve Teknoloji İhracatı sağlar.

CYBER SEM düzgün bir Siber Güvenlik Ekosisteminin oluşmasını sağlar.

CYBER SEM oluşturacağı insan kaynağıyla e-devlet hizmetlerinin güvenli, güvenilir ve kesintisiz şekilde işletilmesini sağlar.

CYBER SEM bizi burnu büyüklerden, yalancılarla mezarcılardan, yok olmamaya çalışmaktan, ve daha bir çok sıkıntılı ve kötü durumdan kurtarmış olur.

Ayrıca bunların yanında sağladığı mali desteklerle kolayca istihdam olabilmemizi sağlar ve arada uygulayacağı indirimlerle almamız gereken kaliteli eğitimlerle sertifikasyonlardan makul ücretlerle yararlanmamızı sağlar.

Unutmayın:

Biz bitersek kötü niyetli hackerlar'ın insafına kalırsınız ve sizin için çalışsalar bile acaba bizi de başkalarına satıyor mudur? Şeklinde sorular sorarak her günü bıçak sırtı yaşayarak geçirmek zorunda kalırsınız.

Biz bitersek ancak da her başarılı siber saldırıdan sonra ah vah çekmekden başka bir şey yapamazsınız.

Biz bitersek e-devleti yürütemezsiniz.

Biz bitersek siber saldırılardan çok daha kötü durumlara düşersiniz; Çok yüksek maddi ve manevi kayıplara uğramak, olası alt yapılara yapılacak siber sabotaj sorunları v.s. gibi

Yani artık herkesin şunu anlaması lazım:

Siber Güvenlik, Bilgi Güvenliği, Felaket Kurtarma Ve Olay Müdahale gibi süreçleri oluşturup uygulatacak insan kaynağı bir lüks değil zorunluluktur.

Biz bunu yapmak istiyoruz

Bizler konmayan güvenlik derslerinden dolayı hocalarımızla tartışmak istemiyoruz.

Bizler yalancılarla, burnu büyüklerle, bizi görmezden gelenlerle, işimizi değersiz görenlerle v.s. muhatap olmak istemiyoruz.

Bizler senelerce kendimizi geliştirebilmek uğruna free eğitim, sınav, seminer, konferans, panel v.s. tarzı saman alevi gibi yakaladın yakaladın yakalamadın artık olur mu olmaz mı bilinmez tarzında organizasyon şekli istemiyoruz.

Bizler bu işi yapabilmek için Ferhan Şensoyun Şans Kapıyı Kırınca Filminin tersine var olabilmek için kendimizin zorla şansımızın kapısını kırarak şansımızla iş yapabilir hale gelmek istemiyoruz.

Bizler yok olma tehlikesinde olmaktan artık kurtulmak istiyoruz.

Bizler aslında çok şey istemiyoruz. Sadece Dünyadaki herhangi bir meslektaşımızın sahip olduğu haklarla imkanlara sahip olmak istiyoruz.

Lütfen bunu görün artık ve buna göre gerekenleri yapın. Cypsec'te söyledim olmadı, CEZERİSGA'da söyledim olmadı BT Vizyon'da tanık oldum daha sonra söyledim olmadı, Kıymetli Sektör Büyüklerimin olduğu bir gruptayım orada dillendiriyorum hala bir şey yok bir de buradan haykırayım size o zaman **YETER ARTIK BİR AN EVVEL GEREKENİ YAPIN GEÇ KALIYORUK!**

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

# DEEPFAKE ÇAĞI:
# GÖRDÜĞÜMÜZE Mİ, YOKSA GERÇEĞE Mİ İNANACAĞIZ?

Yapay zekâ çağında tehlikeler, doğrulama yöntemleri ve savunma mekanizmaları*hareket etmemize katkı sağlamak.*

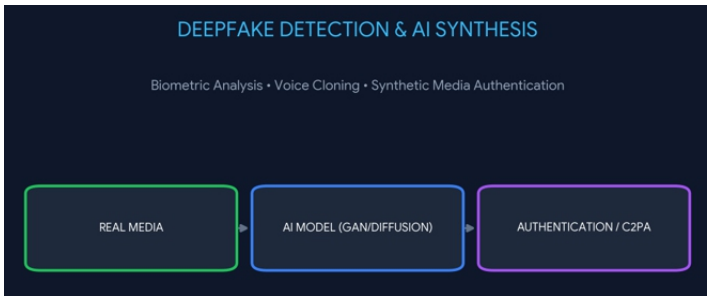
***Telefonunuz çalıyor. Karşınızdaki ses, çalıştığınız kurumun yöneticisine ait. Acil bir ödeme yapılmasını istiyor ve sesi her zamanki kadar gerçek geliyor. Peki gerçekten yöneticinizle mi konuşuyorsunuz, yoksa birkaç saniyelik bir ses kaydından üretilmiş yapay bir sesle mi?***

*Gördüğümüz ve duyduğumuz her şeyin gerçekliğinden emin olmak artık eskisi kadar kolay değil. Bu yazıda, deepfake teknolojisinin nasıl çalıştığını, hangi riskleri taşıdığını ve bireysel ya da kurumsal düzeyde bu içerikleri nasıl doğrulayabileceğimizi ele alacağım. Amacım, dijital dünyada daha bilinçli ve güvenli hareket etmemize katkı sağlamak.*

## 1. DEEPFAKE NEDİR VE NASIL ÇALIŞIR?

Deepfake; bir kişinin yüzünün, sesinin veya hareketlerinin yapay zekâ ve derin öğrenme teknikleriyle ikna edici biçimde sentezlenerek başka bir dijital içeriğe aktarılmasıdır. Teknoloji; sinema, eğitim, erişilebilirlik, tıp ve yaratıcı üretim için önemli imkânlar sağlarken dolandırıcılık, kimlik hırsızlığı ve dezenformasyon risklerini de büyütmektedir.

Üretici çekişmeli ağlar (GAN), bir üretici ve bir ayırt edici modelin karşılıklı öğrenmesine dayanır. Günümüzde bunlara ek olarak difüzyon modelleri, yüz değiştirme sistemleri ve sinir ağı tabanlı metinden konuşmaya dönüştürme modelleri de kullanılmaktadır. Bazı yeni nesil sistemler, birkaç saniyelik ses örneğinden dahi ikna edici ses klonları üretebilmektedir.




Şekil 1. Sentetik medya üretimi ile içerik kökeni doğrulamasının temel bileşenleri.

## 2. RİSKLER VE TEHDİT MATRİSİ

| Risk kategorisi | Açıklama ve örnek senaryo | Etki düzeyi |
|---|---|---|
| Kimlik hırsızlığı | Yüz veya ses verilerinin klonlanarak biyometrik doğrulama ve kimlik kontrol süreçlerinin yanıltılmaya çalışılması. | Yüksek / Kritik |
| Finansal dolandırıcılık | Yönetici kimliğine bürünülerek sahte havale, şifre paylaşımı ya da ödeme talimatı verilmesi. | Çok yüksek / Kritik |
| Sahte haber ve dezenformasyon | Kamuya mal olmuş kişilerin yapay ses veya videolarıyla kamuoyunun manipüle edilmesi. | Kritik |
| Kurumsal itibar kaybı | Kurum sözcülerine atfedilen sahte açıklamalarla kriz yaratılması veya güvenin zedelenmesi. | Yüksek |
| Sosyal mühendislik | Yakınların ya da yöneticilerin sesleri kullanılarak acil durum, şantaj veya para isteme senaryoları kurulması. | Orta / Yüksek |

Deepfake içerikler bireysel güvenlikten kurumsal itibara ve toplumsal güvene kadar uzanan geniş bir tehdit alanı oluşturmaktadır. Aşağıdaki senaryoların ortak özelliği, sesin veya görüntünün tek başına kimlik kanıtı gibi kabul edilmesidir.

## 3. DEEPFAKE İÇERİK NASIL DOĞRULANIR?

Tek bir görsel kusur, otomatik tespit puanı veya sezgi kesin kanıt değildir. Yeni nesil sistemler göz kırpma, dudak eşleşmesi, ışık ve ses tonlaması gibi eski nesil hataları büyük ölçüde azaltabilmektedir. Bu nedenle en güvenilir yaklaşım, içerikten çok kaynağı ve bağlamı doğrulamaktır.

- ***Kaynağı bulun:*** İçeriğin ilk kez nerede, kim tarafından ve hangi tarihte yayımlandığını araştırın. Kırpılmış veya yeniden yüklenmiş kopyalar bağlamı gizleyebilir.
- ***İkinci kaynaktan teyit edin:*** Önemli bir açıklamayı resmî web sitesi, doğrulanmış hesap veya güvenilir haber kuruluşu gibi bağımsız bir kanaldan kontrol edin.
- ***Tersine görsel arama yapın:*** Aynı görüntünün daha eski veya farklı bağlamdaki sürümlerini araştırın.
- ***Ses ve görüntüyle yetinmeyin:*** Finansal veya kritik bir talebi, daha önce kayıtlı telefon numarası ya da yüz yüze doğrulama gibi bağımsız bir kanaldan teyit edin.
- ***İçerik kökenini inceleyin:*** Varsa C2PA/Content Credentials bilgileri, içeriğin kaynağı ve düzenleme geçmişi hakkında doğrulanabilir kayıtlar sunabilir. Bu kayıtlar içeriğin doğru olduğu yönünde tek başına hüküm vermez.
- ***Otomatik araçları yardımcı gösterge sayın:*** Deepfake tespit yazılımları yanlış pozitif veya yanlış negatif sonuç üretebilir; kritik kararlar tek bir araca dayandırılmamalıdır.

Deepfake görsel ve orjinal görselin karşılaştırılması.

Figür 1: Deepfake Figür 2: Orijinal

Şekil 2. Görsel karşılaştırmalar yararlı olabilir; ancak tek başına kesin doğrulama sağlamaz.

## 4. KORUNMA VE SAVUNMA STRATEJİLERİ

*Temel ilke: Kritik bir işlemde hiçbir ses veya görüntü tek başına kimlik kanıtı kabul edilmemelidir.*

### 4.1. Bireysel önlemler

- ***Çok faktörlü kimlik doğrulama:*** Yalnızca yüz veya ses biyometrisine güvenmeyin; doğrulama uygulaması, geçiş anahtarı ya da donanım güvenlik anahtarı kullanın.

*"Dijital dünyada güven, yalnızca teknolojiyle değil; etik davranış, doğru süreç ve bağımsız teyit mekanizmalarıyla kurulur."*

- ***Önceden belirlenmiş güvenlik sorusu:*** Aile içinde acil para taleplerinde kullanılacak, sosyal medyada bulunmayan özel bir kelime veya soru belirleyin.

- ***Dijital ayak izini sınırlama:*** Herkese açık uzun ve temiz ses/video kayıtlarının kötüye kullanılabileceğini göz önünde bulundurun.
- ***Acele baskısına direnme:*** Gizlilik, korku ve aciliyet vurgusu sosyal mühendisliğin klasik işaretleridir; işlemi durdurup bağımsız doğrulama yapın.

**4.2. Kurumsal önlemler**

- ***En az iki kişinin onayı:*** Yüksek tutarlı transfer, hesap değişikliği ve hassas veri paylaşımı tek kişinin sesli veya görüntülü talimatıyla yapılmamalıdır.
- ***Geri arama prosedürü:*** Kritik talep, mesajdaki numaradan değil kurum rehberinde kayıtlı numaradan geri aranarak doğrulanmalıdır.
- ***Farkındalık ve tatbikat:*** Eğitimler ses klonlama, görüntülü görüşme taklidi ve yapay zekâ destekli oltalama senaryolarını içermelidir.
- ***Olay müdahale planı:*** Sahte içerik tespit edildiğinde delilin korunması, hesapların güvenceye alınması, paydaşların bilgilendirilmesi ve kamu açıklaması için sorumlular önceden belirlenmelidir.
- ***İçerik kökeni kayıtları:*** Kurumsal medya üretiminde C2PA/Content Credentials gibi kriptografik olarak bağlanan köken kayıtlarından yararlanılabilir.

## 5. YASAL VE ETİK ÇERÇEVE

Deepfake kullanımı; kişilik hakları, özel hayatın gizliliği, fikrî haklar, dolandırıcılık ve kişisel verilerin korunması gibi birden fazla hukuk alanını ilgilendirir. Bir içeriğin yapay zekâ ile üretilmiş olması, onu otomatik olarak hukuka uygun veya hukuka aykırı kılmaz; amaç, rıza, bağlam ve doğurduğu zarar birlikte değerlendirilmelidir.

- ***Avrupa Birliği Yapay Zekâ Yasası:*** AB AI Act'ın 50. maddesi, deepfake niteliğindeki görüntü, ses veya video içeriğini üreten ya da değiştiren sistemlerin kullanıldığı durumlarda belirli şeffaflık yükümlülükleri öngörür. Sanatsal ve benzeri kullanımlar için özel düzenlemeler bulunduğundan her olay kendi bağlamında değerlendirilmelidir.
- ***Türkiye'de KVKK:*** Yüz ve ses kayıtları, kişiyi benzersiz biçimde tanımlamak amacıyla özel teknik işleme tabi tutulduğunda biyometrik veri niteliği kazanabilir. Biyometrik veriler özel nitelikli kişisel veriler arasındadır ve işleme şartları somut olaya göre değerlendirilir.
- ***KKTC'de yerel çerçeve:*** 89/2007 sayılı Kişisel Verilerin Korunması Yasası kişisel verilerin işlenmesi ve aktarılmasına ilişkin temel kuralları düzenler. Deepfake amacıyla yüz veya ses verisi işleyen kurumların hukuki dayanak, amaçla sınırlılık, güvenlik ve bilgilendirme yükümlülüklerini ayrıca değerlendirmesi gerekir.

## 6. KAYNAKLAR VE İLERİ OKUMA


***1.*** *Avrupa Birliği. Regulation (EU) 2024/1689 (Artificial Intelligence Act), özellikle Madde 50.https://eur-lex.europa.eu/eli/reg/2024/1689/oj*

***2.*** *Coalition for Content Provenance and Authenticity (C2PA). C2PA Technical Specification 2.4 ve açıklayıcı belgeler. https://spec.c2pa.org/specifications/specifications/2.4/*

***3.*** *Kuzey Kıbrıs Türk Cumhuriyeti Kişisel Verileri Koruma Kurulu. 89/2007 sayılı Kişisel Verilerin Korunması Yasası ve ilgili düzenlemeler. https://kvkk.gov.ct.tr/*

***4.*** *T.C. Kişisel Verileri Koruma Kurumu. Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber. https://www.kvkk.gov.tr/*

***5.*** *National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://www.nist.gov/itl/ai-risk-management-framework*

***6.*** *European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends*

***7.*** *Europol Innovation Lab. Facing Reality? Law Enforcement and the Challenge of Deepfakes. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes Stanford Institute for Human-Centered Artificial Intelligence. AI Index Report. https://hai.stanford.edu/ai-index*



**Dr. Eren Küren**
Bilgisayar Mühendisi & Dijital Dönüşüm Uzmanı

# Ergenlik ve Çevrimiçi Sosyal Ağlar


Ergenlik, çocukluktan yetişkinliğe geçişi kapsayan, biyolojik, bilişsel ve sosyal açıdan hızlı dönüşümlerin yaşandığı bir dönemdir. Bu dönemde birey kimliğini sorgular, aileden bağımsızlaşmaya başlar, akran ilişkilerine daha fazla değer atfeder ve toplumsal role dair ilk ciddi denemelerini yapar. Günümüzde bu gelişimsel süreç, büyük ölçüde dijital ortamda, özellikle de çevrimiçi sosyal ağlar aracılığıyla şekillenmektedir. Instagram, TikTok, Snapchat, YouTube ve benzeri platformlar artık ergenlerin günlük yaşamının merkezinde yer almakta; bu durum hem araştırmacılar hem eğitimciler hem de ebeveynler için fırsatlarla birlikte ciddi kaygılar da doğurmaktadır.

Ergenlik döneminde beynin ödül sistemiyle ilişkili bölgeleri, dürtü kontrolünden sorumlu prefrontal korteksten daha hızlı olgunlaşır. Bu asimetrik gelişim, ergenlerin anlık ödüllere karşı yetişkinlere kıyasla daha hassas olmasına yol açar. Sosyal medya platformlarındaki beğeni, yorum ve takipçi bildirimleri gibi anlık geri bildirim mekanizmaları tam da bu ödül sistemini hedef alarak ergenler için güçlü bir çekim yaratır. Aynı zamanda ergenlik, Erikson'ın psikososyal gelişim kuramında da vurgulandığı gibi "kimlik mi rol karmaşası mı" krizinin yaşandığı bir evredir; birey bu dönemde kendini sürekli başkalarıyla kıyaslar. Sosyal medya bu kıyaslama sürecini hem yoğunlaştırır hem de küreselleştirir, çünkü artık ergen yalnızca sınıf arkadaşlarıyla değil, dünyanın dört bir yanından influencer'lar ve akranlarıyla kendini karşılaştırma imkânı bulur. Bunlara ek olarak, ergenlikte akran onayı aile onayından daha belirleyici hâle gelir ve sosyal medya bu ilişkileri 7/24 erişilebilir kılarak sürekli bağlantıda olma baskısı da yaratabilir.

Sosyal medyanın ergenler için bu denli çekici olmasının başlıca nedenleri arasında, beğeni ve bildirimlerin ne zaman geleceğinin belirsiz olmasından kaynaklanan değişken pekiştirme mekanizması, öz-değerin dışsal ölçütlere bağlanmasına yol açabilen sosyal onay arayışı, belirli bir gruba veya trende ait olma hissi, akranların paylaştığı deneyimleri kaçırma korkusu (FOMO) ve gerçek hayatta cesaret edilemeyen kimlik deneyimlerinin çevrimiçi ortamda daha rahat sergilenebilmesi sayılabilir.

Bu platformların ergenlere sunduğu olumlu katkılar da göz ardı edilmemelidir. Coğrafi sınırlamalar olmaksızın benzer ilgi alanına sahip kişilerle bağlantı kurulabilmesi, özellikle sosyal olarak izole ergenler için önemli bir destek kaynağı oluşturur. Müzik, sanat, yazı ve video üretimi yoluyla kendini ifade etme imkânı, özgüven gelişimine ve yaratıcı becerilerin keşfine katkı sağlayabilir. Ruh sağlığı, cinsel sağlık, toplumsal cinsiyet ve iklim krizi gibi konularda okul müfredatının ötesinde bilgiye erişim mümkün hâle gelir. Ayrıca LGBTİ+ ergenler, nadir hastalığa sahip gençler veya göçmen kökenli ergenler gibi gruplar, çevrimiçi topluluklar aracılığıyla kendilerini yalnız hissetmeme ve destek görme fırsatı bulabilir.

Ancak bu faydaların yanı sıra ciddi riskler de mevcuttur. Filtrelenmiş ve düzenlenmiş içeriklere sürekli maruz kalma, gerçekçi olmayan güzellik standartlarının içselleştirilmesine ve özellikle genç kadınlarda beden memnuniyetsizliğine yol açabilir. Anonimlik imkânı ve mesajların hızla yayılabilmesi, mağdurun kaçış alanı bulamadığı, geleneksel zorbalıktan daha yıkıcı olabilen bir çevrimiçi zorbalık türünü ortaya çıkarmıştır. Ekran süresinin, özellikle yatma öncesi kullanımın artması uyku kalitesini düşürebilir, dikkat süresini kısaltabilir ve akademik performansı olumsuz etkileyebilir. Yoğun ve pasif kullanım bazı araştırmalarda kaygı ve depresif belirtilerle ilişkilendirilse de, bu ilişkinin yönü ve büyüklüğü konusunda bilim insanları arasında hâlâ tartışmalar sürmekte, etkiler kişiden kişiye büyük farklılık göstermektedir. Son olarak, kişisel bilgilerin, konum verilerinin veya görsellerin paylaşılması istismar, dolandırıcılık veya çevrimiçi avlanma gibi risklere kapı aralayabilir.

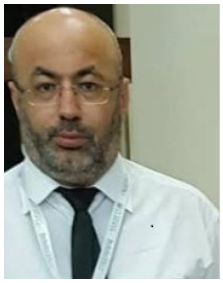
Bu noktada platform tasarımının rolü de önemlidir. Sonsuz kaydırma, otomatik oynatma ve algoritmik öneri sistemleri gibi kullanıcıyı ekranda tutmaya yönelik tasarım stratejileri, öz-düzenleme becerileri henüz tam olgunlaşmamış olan ergenler üzerinde yetişkinlere kıyasla çok daha güçlü bir etki yaratır. Bu durum, bazı platformların ergen hesapları için ekran süresi hatırlatıcıları, gece modu kısıtlamaları ve içerik filtreleme gibi önlemler geliştirmesine de zemin hazırlamıştır. Önceden ruh sağlığı sorunu yaşayan ergenler, sosyal olarak izole olanlar ve erken ergenlik dönemindeki (10-13 yaş) gençler gibi bazı gruplar, bu risklere karşı özellikle savunmasızdır.

Tüm bu tabloda ebeveynlerin ve eğitimcilerin rolü belirleyicidir. Araştırmalar katı yasaklayıcı yaklaşımların çoğunlukla ters etki yarattığını ve ergenin gizli kullanım yollarına yönelmesine neden olduğunu göstermektedir; bunun yerine açık iletişim, ortak kural belirleme ve güven temelli bir rehberlik yaklaşımı çok daha etkili sonuçlar verir. Ergenlere algoritmaların nasıl çalıştığı, içeriklerin nasıl manipüle edilebileceği ve çevrimiçi kaynakların nasıl sorgulanacağı öğretilmelidir. Ekran süresini tamamen yasaklamak yerine birlikte belirlenen makul sınırlar ve ekransız zaman dilimleri daha sürdürülebilir bir denge sağlar. Aynı zamanda ergenlerin çevrimiçi yaşadıkları olumsuz deneyimleri yargılanma korkusu olmadan paylaşabilecekleri bir ortam sağlamak, erken müdahale açısından kritik önem taşır.

Sonuç olarak, çevrimiçi sosyal ağlar günümüz ergenliğinin ayrılmaz bir parçası hâline gelmiştir ve bu olguyu yalnızca iyi veya kötü olarak nitelendirmek konunun karmaşıklığını göz ardı etmek anlamına gelir. Belirleyici olan; kullanım süresi, içeriğin niteliği, kullanım biçimi ve ergenin bireysel psikolojik durumudur. Ebeveynlerin, eğitimcilerin ve platform geliştiricilerin ortak sorumluluğu, ergenlerin bu dijital ortamdan en az zararla en çok faydayı sağlayabilecekleri dengeli bir çerçeve oluşturmaktır. Bu denge sağlandığında sosyal medya, ergenler için zararlı bir tuzak olmaktan çıkıp kimlik gelişimine, sosyal bağlara ve yaratıcı ifadeye katkı sunan değerli bir araca dönüşebilir.

**Uzm. Psk. Eşmen Tatlıcalı**

# Yapay Zekâ ve Dijital İkizler: Gerçek Dünyanın Sanal Kopyaları Geleceği Nasıl Şekillendiriyor?



***Dijital dönüşüm çağında yapay zekâ (YZ), yalnızca verileri analiz eden bir teknoloji olmaktan çıkarak karar verme, tahmin üretme ve karmaşık sistemleri optimize etme yetenekleriyle hayatın her alanında etkisini göstermektedir. Bu dönüşümün merkezinde yer alan teknolojilerden biri de dijital ikiz (Digital Twin) kavramıdır. Dijital ikiz, fiziksel bir nesnenin, sistemin veya sürecin gerçek zamanlı verilerle sürekli güncellenen sanal temsilidir. Sensörler aracılığıyla elde edilen veriler yapay zekâ algoritmaları tarafından analiz edilerek sistemlerin performansı izlenebilmekte, arızalar önceden tahmin edilebilmekte ve geleceğe yönelik senaryolar oluşturulabilmektedir.***

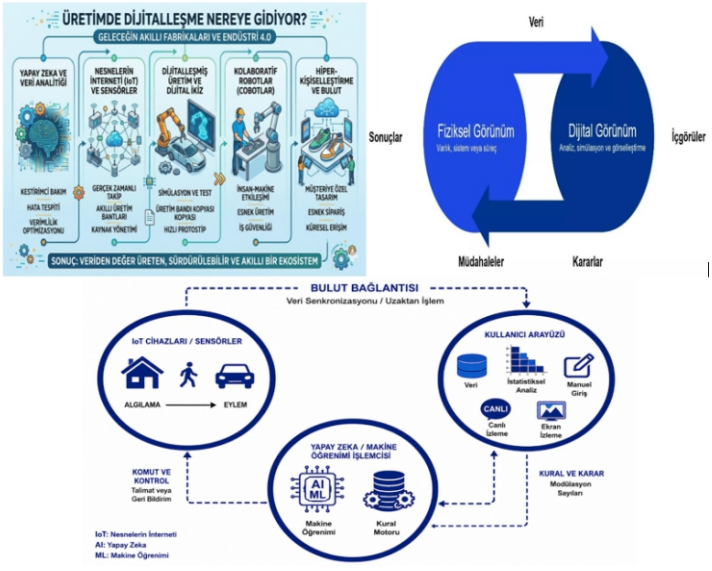
***Günümüzde enerji şebekelerinden akıllı şehirlere, otonom araçlardan sağlık sistemlerine kadar birçok alanda dijital ikiz teknolojileri kullanılmaktadır. Yapay zekâ ile birleşen dijital ikizler, yalnızca mevcut durumu gösteren sanal modeller değil; aynı zamanda öğrenebilen, öngörebilen ve karar destek sağlayabilen akıllı sistemler hâline gelmiştir. Bu yazıda dijital ikiz teknolojisinin temel prensipleri, yapay zekâ ile ilişkisi, kullanım alanları ve gelecekteki potansiyeli ele alınmaktadır.***

### 1. Geleceğin Teknolojisi Neden Dijital İkizler?

Sanayi Devrimi'nden günümüze kadar insanlık birçok teknolojik sıçrama yaşadı. Buhar makinesi üretim süreçlerini değiştirdi, elektrik sanayileşmeyi hızlandırdı, bilgisayarlar bilgi çağını başlattı ve internet dünyayı birbirine bağladı. Günümüzde ise yapay zekâ ve dijital ikiz teknolojileri yeni bir dönüşümün öncüsü olarak görülmektedir.

Bir fabrikanın, bir otomobilin, bir hastanenin hatta bir şehrin dijital ortamda birebir kopyasının oluşturulabildiğini düşünün. Bu sanal model yalnızca görüntüden ibaret değildir; gerçek sistemden sürekli veri alır, onun davranışlarını öğrenir ve gelecekte yaşanabilecek olayları tahmin eder. İşte bu teknolojiye **dijital ikiz** adı verilmektedir.

Dijital ikizler sayesinde gerçek sistemler üzerinde riskli veya maliyetli deneyler yapmadan önce tüm senaryolar sanal ortamda test edilebilmektedir. Bu durum işletmelere hem zaman hem de maliyet avantajı sağlamaktadır.




**Şekil 1: Fiziksel sistemler ile dijital kopyaları arasındaki gerçek zamanlı veri akışı ve yapay zekâ destekli karar mekanizması.**

### Dijital Dönüşümün Yeni Yüzü

Dijital ikiz teknolojisi ilk kez 2000'li yılların başında NASA tarafından karmaşık uzay sistemlerinin izlenmesi amacıyla gündeme getirilmiştir. Günümüzde ise Siemens, Microsoft, IBM, NVIDIA, Tesla ve General Electric gibi teknoloji devleri bu teknolojiyi aktif olarak kullanmaktadır.

Örneğin modern bir rüzgâr türbininde yüzlerce sensör bulunmaktadır. Bu sensörler sıcaklık, titreşim, rüzgâr hızı ve enerji üretimi gibi verileri sürekli toplar. Toplanan bilgiler dijital ikiz modeline aktarılır ve yapay zekâ tarafından analiz edilir. Eğer türbinin belirli bir parçasında gelecekte arıza oluşma ihtimali varsa sistem bunu günler hatta haftalar öncesinden tespit edebilir.

Benzer şekilde otomotiv sektöründe de araçların sanal kopyaları oluşturularak performans testleri yapılmakta, bakım ihtiyaçları belirlenmekte ve sürüş güvenliği artırılmaktadır.

**Tablo 1.** Geleneksel Sistemler ve Dijital İkiz Yaklaşımının Karşılaştırılması

| Özellik | Geleneksel Yaklaşım | Dijital İkiz Yaklaşımı |
|---|---|---|
| Veri Kullanımı | Sınırlı | Gerçek Zamanlı |
| Arıza Tespiti | Arıza sonrası | Arıza öncesi tahmin |
| Karar Verme | İnsan odaklı | Yapay zekâ destekli |
| Maliyet | Yüksek bakım maliyeti | Daha düşük işletme maliyeti |
| Simülasyon Yeteneği | Kısıtlı | Gelişmiş senaryo analizi |
| Verimlilik | Orta düzey | Yüksek düzey |

### Dijital İkizler Neden Bu Kadar Önemli?

Dünya genelinde işletmeler her yıl milyarlarca dolarlık bakım, arıza ve üretim kaybı maliyetleriyle karşı karşıya kalmaktadır. Dijital ikiz teknolojisi bu kayıpların azaltılmasına yardımcı olmaktadır.

Başlıca avantajları şunlardır:

- Arızaları önceden tahmin eder.
- Bakım maliyetlerini azaltır.
- Enerji verimliliğini artırır.
- Üretim süreçlerini optimize eder.
- İnsan hatalarını azaltır.
- Daha güvenli çalışma ortamları oluşturur.
- Karar verme süreçlerini hızlandırır.

Bu nedenle Gartner, McKinsey ve Deloitte gibi uluslararası araştırma kuruluşları dijital ikizleri geleceğin en stratejik teknolojileri arasında göstermektedir.

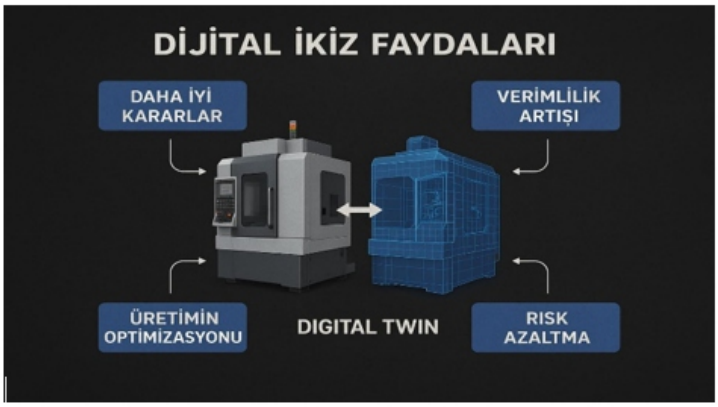
### Yapay Zekâ Bu Hikâyenin Neresinde?

Bir dijital ikiz, tek başına yalnızca veri toplayan ve görselleştiren bir modeldir. Onu gerçekten "akıllı" yapan unsur ise yapay zekâdır. Sensörlerden gelen milyonlarca veri noktası yapay zekâ algoritmaları tarafından analiz edilir. Bu sayede sistem;

- Geçmiş verilerden öğrenebilir,
- Gelecekte oluşabilecek arızaları tahmin edebilir,
- Farklı senaryoları karşılaştırabilir,
- En uygun çözümü önerebilir.

Örneğin bir elektrik dağıtım şebekesinde meydana gelebilecek aşırı yüklenmeler, yapay zekâ destekli dijital ikizler sayesinde önceden belirlenebilir. Böylece olası enerji kesintileri gerçekleşmeden gerekli

önlemler alınabilir. Bu özellik, dijital ikizleri yalnızca bir izleme sistemi olmaktan çıkarıp geleceği öngörebilen akıllı sistemlere dönüştürmektedir.




Şekil 2: Dijital ikiz teknolojisinin işletmeler için sunduğu temel operasyonel ve finansal avantajlar.

**2. Dijital İkiz Nedir Ve Nasıl Çalışır?**

Bugün kullandığımız akıllı telefonlar, otomobiller, üretim tesisleri ve hatta şehirler her saniye milyonlarca veri üretmektedir. Bu veriler uzun yıllar yalnızca kayıt altına alınırken, günümüzde yapay zekâ sayesinde anlamlı bilgilere dönüştürülebilmektedir. Ancak bu verilerin en verimli şekilde kullanılmasını sağlayan teknolojilerden biri **dijital ikiz (Digital Twin)** yaklaşımıdır.

En basit tanımıyla dijital ikiz; fiziksel bir nesnenin, sistemin veya sürecin gerçek zamanlı veriler kullanılarak oluşturulan **dinamik sanal kopyasıdır**. Buradaki en önemli nokta, dijital ikizin yalnızca üç boyutlu bir model olmamasıdır. Sensörlerden sürekli veri alan, bu verileri analiz eden, geçmiş deneyimlerden öğrenen ve gelecekte oluşabilecek durumları tahmin edebilen yaşayan bir dijital modeldir. Örneğin bir elektrikli otomobili ele alalım. Araç üzerinde bulunan yüzlerce sensör; batarya sıcaklığını, motor devrini, fren sistemini, lastik basıncını ve enerji tüketimini sürekli ölçmektedir. Bu bilgiler internet üzerinden dijital ikize aktarılır. Yapay zekâ ise bu verileri analiz ederek bataryanın ömrünü tahmin edebilir, enerji tüketimini optimize edebilir veya olası bir arızayı sürücü fark etmeden önce tespit edebilir. Benzer şekilde bir rüzgâr türbini, yüksek hızlı tren, akıllı bina veya üretim hattı da kendi dijital ikizine sahip olabilir. Böylece gerçek sistem üzerinde risk oluşturmadan farklı senaryolar güvenli bir şekilde test edilebilir.

**Dijital İkiz Nasıl Çalışır?**

Bir dijital ikiz sistemi beş temel aşamadan oluşur.

**1. Veri Toplama**

Sistemin ilk aşaması sensörlerden veri toplamaktır. Sıcaklık, titreşim, basınç, enerji tüketimi, hız, konum ve çevresel koşullar gibi bilgiler gerçek zamanlı olarak ölçülür.

**2. Veri İletimi**

Toplanan bilgiler 5G, Wi-Fi, Ethernet, LoRaWAN veya diğer haberleşme teknolojileri kullanılarak bulut ya da uç bilişim (Edge Computing) altyapısına aktarılır.

**3. Veri İşleme**

Aktarılan veriler temizlenir, filtrelenir ve analiz için hazırlanır. Büyük veri teknolojileri sayesinde saniyede milyonlarca veri işlenebilir.

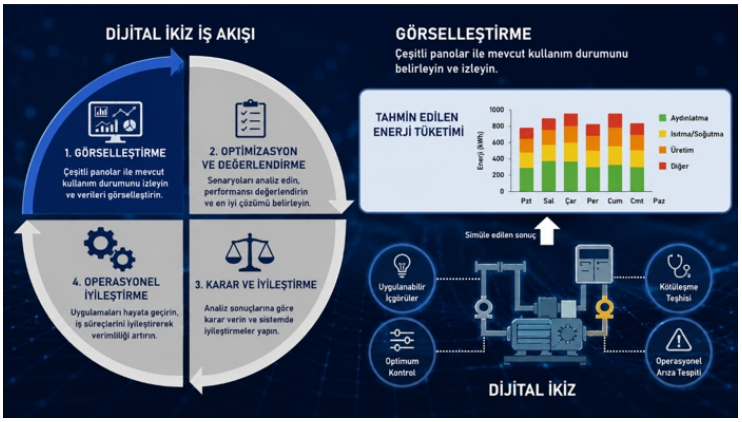
**4. Yapay Zekâ Analizi**

Makine öğrenmesi ve derin öğrenme algoritmaları sistemi analiz ederek;

- Performans değişimlerini belirler,
- Arıza ihtimallerini hesaplar,
- Bakım zamanını tahmin eder,
- Enerji tüketimini optimize eder,
- Farklı senaryolar oluşturur.

**5. Dijital İkiz Modeli**

İşlenen bütün bilgiler sanal modele aktarılır. Böylece sistemin güncel durumu izlenebilir, gelecekte oluşabilecek olaylar tahmin edilebilir ve yöneticilere karar desteği sağlanır.




**Şekil 3:** Veri toplama aşamasından operasyonel iyileştirmeye kadar uzanan döngüsel dijital ikiz iş akışı.

| Bileşen | Görevi | Örnek Teknolojiler |
|---|---|---|
| Sensörler | Fiziksel ortamdan veri toplar | Sıcaklık, titreşim, kamera, GPS |
| Haberleşme Altyapısı | Verileri güvenli şekilde iletir | 5G, Wi-Fi, LoRaWAN, Ethernet |
| Bulut / Uç Bilişim | Verileri depolar ve işler | Microsoft Azure, AWS, Edge Sunucular |
| Yapay Zekâ | Tahmin ve analiz yapar | Makine Öğrenmesi, Derin Öğrenme |
| Dijital İkiz Modeli | Sanal sistemi oluşturur | 3B Modelleme, Simülasyon Yazılımları |
| Karar Destek Sistemi | Sonuçları kullanıcıya sunar | Kontrol Panelleri, Mobil Uygulamalar |

**Tablo 2.** Dijital İkiz Sisteminin Temel Bileşenleri

**Dijital İkizi Akıllı Yapan Nedir?**

Dijital ikiz teknolojisinin başarısındaki en kritik unsur **yapay zekâdır**. Eğer sistem yalnızca sensörlerden veri toplayıp ekranda gösteriyorsa bu bir izleme sistemidir. Ancak yapay zekâ devreye girdiğinde sistem öğrenmeye başlar. Örneğin bir üretim tesisindeki motorların son üç yıllık çalışma verileri incelendiğinde, belirli titreşim değerlerinden sonra arıza oluştuğu görülebilir. Yapay zekâ bu ilişkiyi öğrenerek aynı belirtiler tekrar ortaya çıktığında bakım ekibini önceden uyarabilir. Böylece plansız duruşlar azaltılır, bakım maliyetleri düşer ve üretim sürekliliği sağlanır. Bu yaklaşım yalnızca sanayide değil; hastanelerde hasta takibi, akıllı şehirlerde trafik yönetimi, enerji şebekelerinde yük dengeleme ve tarımda sulama optimizasyonu gibi çok farklı alanlarda da kullanılmaktadır.

**Dijital İkizler Hakkında İlginç Bir Bilgi**

Bir yolcu uçağında bulunan motorlar uçuş sırasında saniyede binlerce veri üretmektedir. Bu veriler dijital ikiz modeli üzerinde analiz edilerek bakım ihtiyacı daha uçak yere inmeden belirlenebilmektedir. Böylece hem güvenlik artmakta hem de bakım maliyetleri önemli ölçüde azalmaktadır. Dijital ikiz teknolojisi, fiziksel sistemlerin yalnızca sanal bir kopyasını oluşturmakla kalmaz; yapay zekâ sayesinde bu sistemleri analiz eden, öğrenen ve geleceğe yönelik tahminler üreten akıllı bir platforma dönüştürür. Sensörler, haberleşme altyapısı, bulut bilişim

ve yapay zekânın birlikte çalışmasıyla oluşturulan bu yapı, geleceğin akıllı fabrikalarının, şehirlerinin ve ulaşım sistemlerinin temelini oluşturmaktadır.

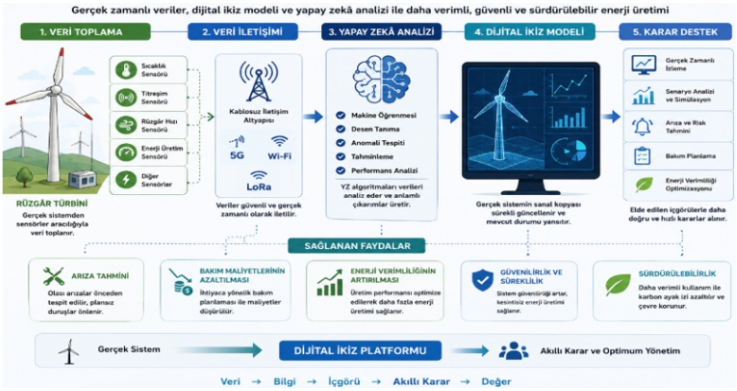
### 3. Yapay Zekâ ve Dijital İkizlerin Günlük Hayattaki Kullanım Alanları

Yapay zekâ destekli dijital ikizler, günümüzde yalnızca büyük teknoloji şirketlerinin kullandığı özel sistemler olmaktan çıkmış; enerji üretiminden ulaşıma, sağlıktan şehir planlamasına kadar birçok alanda yaygın olarak kullanılmaya başlanmıştır. Dijital ikizler sayesinde fiziksel sistemlerin davranışları anlık olarak izlenebilmekte, olası arızalar önceden tahmin edilebilmekte ve en uygun çalışma senaryoları belirlenebilmektedir. Böylece hem işletme maliyetleri azalmakta hem de sistemlerin güvenilirliği ve verimliliği önemli ölçüde artmaktadır.

Aşağıda dijital ikiz teknolojisinin en dikkat çekici uygulama alanları ele alınmıştır.

### 3.1 Enerji Sistemlerinde Dijital İkiz Teknolojisi

Enerji sektörü, dijital ikizlerin en hızlı yaygınlaştığı alanlardan biridir. Elektrik üretim tesisleri, rüzgâr türbinleri, güneş enerji santralleri ve elektrik iletim şebekeleri milyonlarca veriyi sürekli üretmektedir. Bu verilerin yapay zekâ ile analiz edilmesi sayesinde enerji sistemleri daha güvenli, daha verimli ve daha sürdürülebilir hâle gelmektedir. Örneğin bir rüzgâr türbininin dijital ikizi oluşturulduğunda; rüzgâr hızı, kanat titreşimleri, jeneratör sıcaklığı ve enerji üretimi gibi bilgiler anlık olarak izlenebilir. Yapay zekâ algoritmaları bu verileri değerlendirerek bakım ihtiyacını önceden belirleyebilir ve beklenmeyen arızaların önüne geçebilir. Benzer şekilde akıllı elektrik şebekelerinde dijital ikizler, enerji talebini tahmin ederek yük dengesini optimize edebilir. Böylece enerji kayıpları azalırken yenilenebilir enerji kaynaklarının sisteme entegrasyonu da kolaylaşmaktadır.




**Şekil 4.** Enerji üretiminde yapay zekâ destekli dijital ikiz ve kestirimci bakım

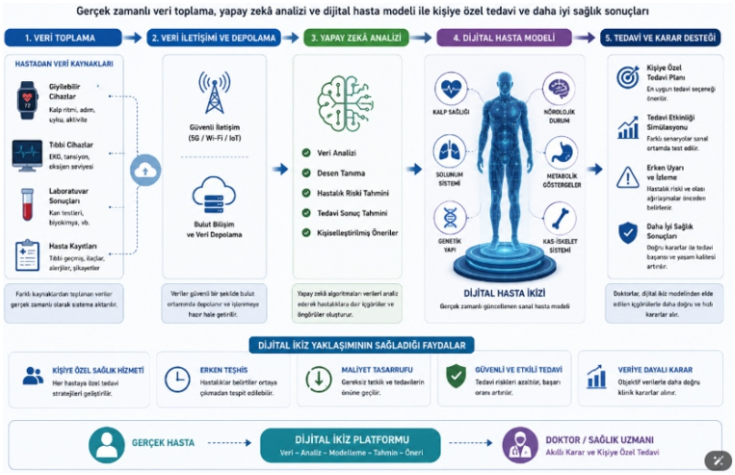
### 3.2 Sağlık Sektöründe Dijital İkizler

Sağlık alanında dijital ikiz teknolojisi, kişiye özel tedavi yaklaşımlarının geliştirilmesinde önemli rol oynamaktadır. Hastaların kalp ritmi, tansiyon, kan şekeri ve diğer biyometrik verileri kullanılarak dijital hasta modelleri oluşturulabilmektedir.

Bu modeller sayesinde doktorlar farklı tedavi seçeneklerini önce sanal ortamda değerlendirebilir ve en uygun yöntemi belirleyebilir. Ayrıca yapay zekâ destekli analizler, hastalıkların erken teşhis edilmesine katkı sağlayarak tedavi süreçlerini daha etkili hâle getirmektedir.

### 3.3 Otomotiv ve Akıllı Ulaşım Sistemleri

Otomotiv sektörü, dijital ikiz teknolojisinin en yoğun kullanıldığı




**Şekil 5:** Biyometrik verilerin analiziyle oluşturulan "Dijital Hasta İkizi" ve kişiye özel tedavi modeli.

alanlardan biridir. Günümüzde modern araçlarda bulunan yüzlerce sensör sayesinde motor performansı, batarya durumu, yakıt tüketimi ve sürüş davranışları sürekli izlenmektedir.

Elektrikli araçlarda dijital ikizler özellikle batarya yönetim sistemlerinde önemli avantaj sağlamaktadır. Yapay zekâ algoritmaları batarya hücrelerini analiz ederek kullanım ömrünü tahmin edebilmekte ve enerji tüketimini optimize edebilmektedir.

Otonom araç teknolojilerinde ise dijital ikizler milyonlarca kilometrelik sanal sürüş senaryoları oluşturarak gerçek trafik ortamında karşılaşılabilecek risklerin önceden değerlendirilmesini sağlamaktadır.

| Alan | Dijital İkiz Uygulaması | Sağladığı Fayda |
|---|---|---|
| Enerji | Elektrik şebekeleri, rüzgâr türbinleri | Arıza tahmini, enerji verimliliği |
| Sağlık | Dijital hasta modeli | Erken teşhis, kişiye özel tedavi |
| Otomotiv | Elektrikli araçlar, otonom sürüş | Batarya yönetimi, güvenlik |
| Üretim | Akıllı fabrikalar | Üretim optimizasyonu |
| Akıllı Şehirler | Trafik, enerji ve su yönetimi | Kaynakların verimli kullanımı |

**Tablo 3.** Dijital İkiz Teknolojisinin Başlıca Kullanım Alanları.

### 3.4 Akıllı Şehirlerin Dijital İkizleri

Geleceğin şehirleri yalnızca daha fazla teknoloji kullanan yerleşim alanları değil; aynı zamanda kendi verilerini analiz ederek öğrenebilen ve gelişebilen sistemler olacaktır.

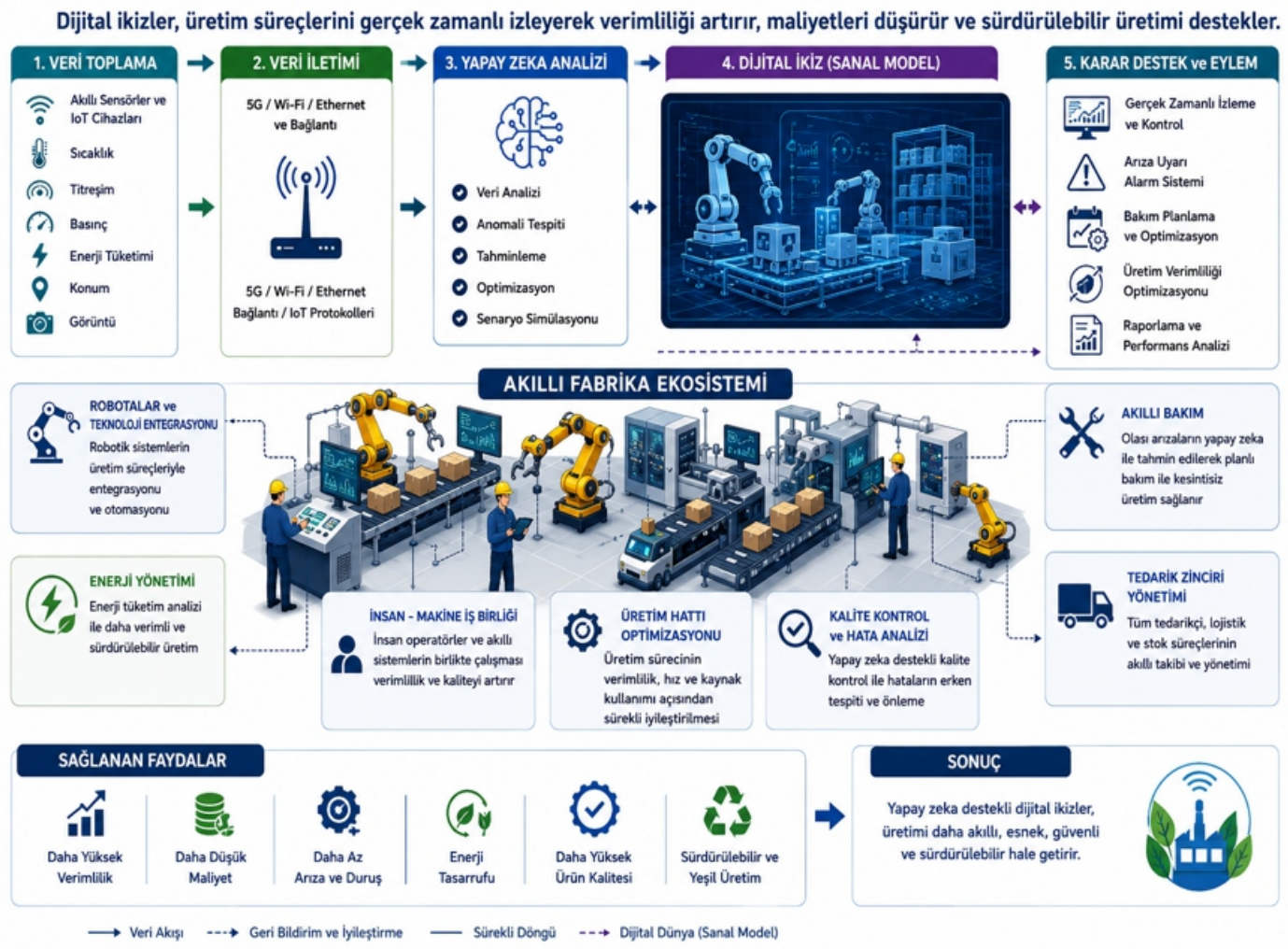
Akıllı şehirlerde oluşturulan dijital ikizler sayesinde;

- Trafik yoğunluğu gerçek zamanlı olarak analiz edilebilir,
- Toplu taşıma sistemleri optimize edilebilir,
- Enerji ve su tüketimi dengelenebilir,
- Hava kalitesi sürekli izlenebilir,
- Afet durumlarında tahliye senaryoları önceden test edilebilir.

Bu sayede şehir yönetimleri daha doğru kararlar alabilirken vatandaşlara daha güvenli ve sürdürülebilir yaşam alanları sunulabilir.

Enerji, sağlık, otomotiv ve akıllı şehir uygulamaları incelendiğinde dijital ikiz teknolojisinin yalnızca sanal modelleme aracı olmadığı; yapay zekâ ile birleşerek karar destek sağlayan, riskleri azaltan ve kaynak kullanımını optimize eden stratejik bir teknoloji olduğu görülmektedir. Önümüzdeki yıllarda bu yaklaşımın Endüstri 5.0, akıllı ulaşım sistemleri ve sürdürülebilir şehircilik projelerinde daha yaygın kullanılması beklenmektedir.


**Şekil 6:** Akıllı şehir ekosisteminde ulaşım, enerji ve altyapı yönetiminin dijital ikiz üzerinden optimizasyonu




**Şekil 7:** Endüstri 5.0 kapsamında insan, robot ve dijital ikiz iş birliğine dayalı akıllı fabrika modeli.

**4. Geleceğin Dünyasında Dijital İkizler: Türkiye ve KKTC İçin Fırsatlar**

Yapay zekâ destekli dijital ikiz teknolojileri, yalnızca bugünün ihtiyaçlarına çözüm sunmakla kalmayıp geleceğin şehirlerini, sanayisini ve yaşam biçimini şekillendirecek stratejik teknolojiler arasında gösterilmektedir. Uluslararası araştırmalar, önümüzdeki yıllarda dijital ikiz kullanımının enerji, sağlık, üretim, ulaştırma ve kamu hizmetleri gibi birçok sektörde hızla yaygınlaşacağını ortaya koymaktadır.

Gelişmiş ülkeler, dijital ikizleri yalnızca teknolojik bir yenilik olarak değil, ekonomik büyüme, sürdürülebilir kalkınma ve dijital dönüşümün temel bileşenlerinden biri olarak değerlendirmektedir. Yapay zekâ ile desteklenen bu sistemler sayesinde gerçek dünyada meydana gelebilecek birçok olay önceden tahmin edilerek zaman, maliyet ve kaynak tasarrufu sağlanabilmektedir. Bu nedenle dijital ikiz teknolojisinin gelecekte yalnızca büyük sanayi kuruluşlarında değil; belediyelerde, üniversitelerde, hastanelerde, enerji şirketlerinde ve ulaşım altyapılarında da yaygın olarak kullanılması beklenmektedir.

**4.1 Akıllı Fabrikaların Yeni Beyni**

Endüstri 4.0 ile başlayan dijital dönüşüm süreci, günümüzde Endüstri 5.0 anlayışıyla daha ileri bir noktaya taşınmaktadır. Endüstri 5.0'ın temel amacı yalnızca üretimi otomatikleştirmek değil; insan, robot ve yapay zekâyı aynı üretim ortamında birlikte çalıştırmaktır.

Bu dönüşümün merkezinde ise dijital ikiz teknolojisi bulunmaktadır. Bir üretim hattının dijital ikizi oluşturulduğunda;

- ✓ Makinelerin çalışma performansı sürekli izlenebilir,
- ✓ Üretim kapasitesi analiz edilebilir,
- ✓ Enerji tüketimi optimize edilebilir,
- ✓ Kalite kontrol süreçleri geliştirilebilir,
- ✓ Olası arızalar üretimi durdurmadan önce belirlenebilir.

Böylece fabrikalar yalnızca daha hızlı değil, aynı zamanda daha güvenli ve daha sürdürülebilir üretim yapabilir.

**4.2 Türkiye ve KKTC İçin Yeni Fırsatlar**

Türkiye son yıllarda akıllı şehirler, savunma sanayii, elektrikli araç teknolojileri ve yenilenebilir enerji yatırımlarıyla dijital dönüşüm sürecini hızlandırmaktadır. Benzer şekilde Kuzey Kıbrıs Türk Cumhuriyeti de üniversiteleri, teknoloji merkezleri ve gelişen bilişim altyapısıyla bu dönüşümden önemli kazanımlar elde edebilecek potansiyele sahiptir.

Özellikle aşağıdaki alanlarda dijital ikiz teknolojisinin önemli katkılar sağlayabileceği düşünülmektedir:

- ❖ Akıllı elektrik şebekelerinin geliştirilmesi
- ❖ Güneş enerji santrallerinin verimliliğinin artırılması
- ❖ Üniversite kampüslerinin dijital yönetimi
- ❖ Akıllı ulaşım sistemleri
- ❖ Su kaynaklarının etkin yönetimi
- ❖ Hastanelerde dijital sağlık uygulamaları
- ❖ Turizm bölgelerinde akıllı şehir çözümleri

KKTC gibi ada ülkelerinde enerji kaynaklarının etkin kullanılması büyük önem taşımaktadır. Dijital ikiz teknolojileri sayesinde enerji üretimi ve tüketimi daha doğru planlanabilir, yenilenebilir enerji kaynaklarının şebekeye entegrasyonu daha güvenli hâle getirilebilir (Tao & Zhang, 2017).

- ❖ **2030 Yılında Bizi Neler Bekliyor?**

Uzmanlar, önümüzdeki yıllarda dijital ikiz teknolojisinin günlük yaşamın birçok alanına entegre olacağını öngörmektedir.

| Alan | Beklenen Katkı |
|---|---|
| Enerji | Daha verimli üretim ve daha düşük enerji kayıpları |
| Sağlık | Kişiye özel tedavi ve erken teşhis |
| Otomotiv | Daha güvenli ve verimli otonom araçlar |
| Üretim | Akıllı fabrikalar ve düşük bakım maliyetleri |
| Akıllı Şehirler | Trafik, enerji ve çevre yönetiminde optimizasyon |
| Eğitim | Uygulamalı dijital laboratuvarlar ve sanal eğitim ortamları |

**Tablo 4.** Dijital İkiz Teknolojisinin Gelecekte Sağlayacağı Kazanımlar

Yakın gelecekte;

- ✓ Her elektrikli aracın bir dijital ikizi olacak.
- ✓ Hastanelerde dijital hasta modelleri yaygınlaşacak.
- ✓ Büyük şehirlerin dijital kopyaları oluşturulacak.
- ✓ Elektrik şebekeleri yapay zekâ tarafından yönetilecek.
- ✓ Fabrikalarda üretim süreçleri büyük ölçüde dijital ikizler üzerinden optimize edilecek.

Bu gelişmeler, yalnızca teknolojik ilerlemeyi değil; aynı zamanda daha sürdürülebilir, güvenli ve verimli bir yaşamın kapılarını aralayacaktır.

Dijital ikiz teknolojisi, yapay zekâ ile birleştiğinde fiziksel sistemlerin yalnızca izlenmesini değil; aynı zamanda öğrenmesini, tahmin üretmesini ve karar vermesini mümkün kılan güçlü bir platform hâline gelmektedir. Önümüzdeki yıllarda bu teknolojinin sanayiden sağlığa, enerjiden akıllı şehirlere kadar pek çok alanda yaygınlaşması beklenmektedir. Türkiye ve KKTC'nin bu dönüşüme zamanında uyum sağlaması, dijital ekonomide rekabet gücünü artıracak önemli adımlardan biri olacaktır.

**5. Sonuç: Dijital İkizler Geleceğin Sessiz Kahramanları mı?**

Sanayi devrimlerinden dijital çağa uzanan teknolojik dönüşüm, yaşamın her alanını değiştirmiştir. Günümüzde bu dönüşümün en dikkat çekici bileşenlerinden biri ise yapay zekâ ile bütünleşen dijital ikiz teknolojisidir (Grieves & Vickers, 2017). Bir zamanlar bilim kurgu filmlerinde görülen gerçek dünyanın sanal kopyaları, bugün enerji sistemlerinden hastanelere, fabrikalardan akıllı şehirlere kadar pek çok alanda kullanılmaktadır. Dijital ikizler yalnızca mevcut durumu yansıtan modeller değildir; gerçek zamanlı verileri analiz eden, olası sorunları önceden tahmin eden ve karar verme süreçlerini destekleyen akıllı sistemlerdir (Fuller ve ark., 2020). Bu sayede enerji verimliliği artırılmakta, bakım maliyetleri azaltılmakta ve kaynaklar daha etkin kullanılmaktadır. Yakın gelecekte dijital ikizlerin sağlık, ulaşım, üretim, eğitim ve şehir yönetimi gibi birçok alanda daha yaygın hâle gelmesi beklenmektedir. Türkiye ve Kuzey Kıbrıs Türk Cumhuriyeti için ise bu teknoloji; akıllı şehirler, yenilenebilir enerji, dijital sağlık ve üniversite-sanayi iş birlikleri açısından önemli fırsatlar sunmaktadır (Alasmary ve ark., 2022). Sonuç olarak dijital ikiz teknolojisi, yapay zekâ ile birlikte yalnızca dijital dönüşümün değil, daha güvenli, verimli ve sürdürülebilir bir geleceğin de temel yapı taşlarından biri olmaya adaydır. **Belki de yakın gelecekte dijital ikizler, bugün internetin olduğu kadar doğal ve vazgeçilmez bir teknolojik altyapı olarak yaşamımızın her alanında yer alacaktır (Tao ve ark., 2022).**


**Şekil 8:** Yapay zekâ, IoT, Büyük Veri ve Dijital İkiz teknolojilerinin

**Dijital İkizler Hakkında 10 Çarpıcı Gerçek**

✓ Dijital ikizler gerçek sistemlerden anlık veri alarak sürekli güncellenir.

✓ Yapay zekâ sayesinde gelecekte oluşabilecek arızaları önceden tahmin edebilir.

✓ Akıllı şehirlerde trafik ve enerji yönetimini optimize edebilir.

✓ Elektrikli araçların batarya ömrünü analiz ederek bakım planlamasını destekler.

✓ Hastaların dijital modelleri üzerinden kişiye özel tedavi seçenekleri geliştirilebilir.

✓ Fabrikalarda plansız üretim duruşlarını azaltmaya yardımcı olur.

✓ Yenilenebilir enerji santrallerinde verimlilik artışı sağlayabilir.

✓ Büyük altyapı projelerinin güvenliğini ve performansını artırabilir.

✓ Doğru uygulandığında enerji tüketimini ve işletme maliyetlerini azaltabilir.

✓ Yapay zekâ ile birlikte geleceğin en önemli dijital dönüşüm teknolojileri arasında gösterilmektedir.

## 6. Dijital İkiz Teknolojisinin Önündeki Zorluklar

Her yeni teknolojide olduğu gibi dijital ikizlerin de bazı önemli zorlukları bulunmaktadır. Bu sistemler büyük miktarda veriyle çalıştığı için **siber güvenlik**, **veri gizliliği** ve **yapay zekâ kararlarının güvenilirliği** en çok dikkat edilmesi gereken konuların başında gelmektedir. Örneğin bir enerji santralinin veya hastanenin dijital ikizine yönelik olası bir siber saldırı, yalnızca dijital sistemi değil gerçek dünyadaki operasyonları da etkileyebilir (Rasheed ve ark., 2020). Benzer şekilde eksik veya hatalı verilerle eğitilen yapay zekâ modelleri yanlış tahminler üretebilir (Jones ve ark., 2020). Bu nedenle dijital ikiz teknolojisinin başarısı yalnızca güçlü algoritmalara değil; güvenli altyapılara, doğru verilere ve insan denetimine de bağlıdır (Ferko ve ark., 2022). Teknoloji geliştikçe etik ilkelerin ve veri güvenliği standartlarının da aynı hızla gelişmesi büyük önem taşımaktadır.

| Fırsatlar | Zorluklar |
|---|---|
| Erken arıza tahmini | Siber güvenlik |
| Enerji verimliliği | Veri gizliliği |
| Düşük bakım maliyeti | Yüksek yatırım maliyeti |
| Akıllı karar desteği | Uzman personel ihtiyacı |

**Tablo 5.** Dijital İkizlerde Fırsatlar ve Zorluklar

## 7. Geleceğe Bakış: Dijital İkizlerle Akıllı Bir Dünya

Yakın gelecekte dijital ikizlerin yalnızca fabrikalarda değil; evlerde, hastanelerde, şehirlerde ve ulaşım sistemlerinde de yaygın olarak kullanılması beklenmektedir (Kritzinger ve ark., 2018). Yapay zekâ ile birlikte çalışan bu sistemler, enerji tüketimini optimize edecek, trafik akışını düzenleyecek, sağlık hizmetlerini kişiselleştirecek ve üretim süreçlerini daha verimli hâle getirecektir (Negri ve ark., 2017).Türkiye ve KKTC açısından bu teknoloji; akıllı şehir projeleri, yenilenebilir enerji sistemleri, üniversite-sanayi iş birlikleri ve dijital sağlık uygulamaları için önemli fırsatlar sunmaktadır. Bu potansiyelin değerlendirilebilmesi ise teknolojiye yatırım yapılmasının yanı sıra, nitelikli insan kaynağının yetiştirilmesine de bağlıdır. Dijital ikizler artık yalnızca geleceğin değil, bugünün de teknolojisidir. Yapay zekâ ile birlikte gelişmeye devam eden bu sistemler, önümüzdeki yıllarda daha akıllı, daha güvenli ve daha sürdürülebilir bir dünyanın oluşturulmasında önemli bir rol oynayacaktır.

**Kaynaklar**


1. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). *Digital Twin: Enabling Technologies, Challenges and Open Research*. **IEEE Access, 8**, 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358
2. Tao, F., & Zhang, M. (2017). *Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing*. **IEEE Access, 5**, 20418–20427. https://doi.org/10.1109/ACCESS.2017.2756069
3. Tao, F., Xiao, B., Qi, Q., Cheng, J., & Ji, P. (2022). *Digital Twin Modeling*. **Journal of Manufacturing Systems, 64**, 372–389. https://doi.org/10.1016/j.jmsy.2022.06.015
4. Alasmary, W., et al. (2022). *Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects*. **IEEE Communications Surveys & Tutorials, 24**(4), 2255–2291. https://doi.org/10.1109/COMST.2022.3208773
5. Ferko, E., Bucaioni, A., & Behnam, M. (2022). *Architecting Digital Twins*. **IEEE Access, 10**, 50335–50350. https://doi.org/10.1109/ACCESS.2022.3172964
6. Rasheed, A., San, O., & Kvamsdal, T. (2020). *Digital Twin: Values, Challenges and Enablers From a Modeling Perspective*. **Computational Geosciences, 24**(3), 1253–1274. https://doi.org/10.1007/s10596-019-09887-4
7. Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). *Characterising the Digital Twin: A Systematic Literature Review*. **CIRP Journal of Manufacturing Science and Technology, 29**, 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002
8. Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). *Digital Twin in Manufacturing: A Categorical Literature Review and Classification*. **IFAC-PapersOnLine, 51**(11), 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474
9. Negri, E., Fumagalli, L., & Macchi, M. (2017). *A Review of the Roles of Digital Twin in CPS-Based Production Systems*. **Procedia Manufacturing, 11**, 939–948. https://doi.org/10.1016/j.promfg.2017.07.198
10. Grieves, M., & Vickers, J. (2017). *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*. In F-J. Kahlen, S. Flumerfelt, & A. Alves (Eds.), **Transdisciplinary Perspectives on Complex Systems** (pp. 85–113). Springer. https://doi.org/10.1007/978-3-319-38756-7_4


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

# Gereğinden Az Kullandığımız 5 İleri C# Özelliği

Modern C# yalnızca daha az kod yazmamızı sağlayan bir dil değil değildir. Aynı zamanda niyetimizi daha açık ifade etmemize, tür güvenliğini artırmamıza ve gerektiğinde gereksiz bellek işlemlerinden kaçınmamıza yardımcı olan güçlü araçlar sunuyor. Her yeni C# sürümüyle birlikte yeni söz dizimleri, API'ler ve derleyici özellikleri geliyor. Ancak bir özelliğin gerçek değerini anlamak için yalnızca nasıl kullanıldığını bilmek yeterli değil. Arka planda nasıl çalıştığını ve hangi maliyetleri beraberinde getirdiğini de anlamak gerekiyor.

Günde milyonlarca kez çalışan bir ayrıştırıcı yazıyorsanız, başka ekiplerin kullanacağı bir kütüphane geliştiriyorsanız veya okunabilirliği korurken performansı artırmak istiyorsanız küçük ayrıntılar büyük önem kazanır.

Bu yazıda modern C#'ın çok konuşulmayan fakat doğru yerde kullanıldığında ciddi fark yaratan beş özelliğine yakından bakacağız.

**1. RANGE (..) VE INDEX (^) OPERATÖRLERİ**

Range ve Index operatörlerinden önce bir dizinin veya metnin son bölümünü almak için başlangıç konumunu elle hesaplamak gerekiyordu.

Örneğin bir dosya adının son üç karakterini almak için şu kod yazılabilir:

```
string fileName = "annual-report.pdf";
string extension =
   fileName.Substring(fileName.Length - 3);
```

Bu kod teknik olarak doğrudur. Ancak okuyucu önce fileName.Length - 3 ifadesinin ne anlama geldiğini hesaplamak zorundadır.

Index operatörü olan ^, sondan saymayı doğrudan ifade eder:

```
string fileName = "annual-report.pdf";
string extension = fileName[^3..];
```

Buradaki ifade açıkça şunu söyler:

“Sondan üç karakter önce başla ve metnin sonuna kadar devam et.”

Aynı yaklaşım dizilerde de kullanılabilir:

```
int[] numbers = { 10, 20, 30, 40, 50, 60 };

int[] middle = numbers[1..4];
```

Bu kod 1 numaralı indisten başlar ve 4 numaralı indise gelmeden durur. Sonuç şu olur:

20, 30, 40

Range operatörünün en önemli avantajı daha az karakter yazmak değildir. Asıl avantaj, başlangıç ve uzunluk hesaplarını ortadan kaldırarak kodun niyetini daha açık hale getirmesidir.

Fakat burada önemli bir ayrıntı vardır: Dilimleme işleminin maliyeti kullanılan türe göre değişir.

Bir array veya string üzerinde alınan dilim çoğunlukla yeni bir nesne oluşturur ve ilgili veriyi kopyalar.

Buna karşılık Span<T> veya ReadOnlySpan<T> üzerinde alınan dilim aynı belleğe açılan başka bir görünümden ibarettir:

```
Span<int> values =
   stackalloc[] { 1, 2, 3, 4, 5 };
Span<int> firstThree = values[..3];
```

Bu örnekte yeni bir dizi oluşturulmaz. firstThree, values tarafından kullanılan belleğin ilk üç elemanına bakar.

Kısacası Range operatörü tek başına “allocation-free” değildir. Bellek tahsisi yapılıp yapılmayacağını, dilimlediğiniz türün bu işlemi nasıl uyguladığı belirler.

**2. KOLEKSİYON KARŞILAŞTIRMASINDA SEQUENCEEQUAL()**

Döngünün nasıl çalıştığını değil, cevaplamak istediğiniz soruyu ifade edin.

İki diziyi eleman eleman karşılaştırmak için aşağıdaki gibi bir metot yazılabilir:

```
public static bool AreEqual(
   int[] first,
   int[] second)
{
   if (first.Length != second.Length)
      return false;
   for (int i = 0; i < first.Length; i++)
   {
      if (first[i] != second[i])
         return false;
   }
   return true;
}
```

Bu kod açık, doğru ve verimlidir. İlk farklı elemanda karşılaştırmayı durdurur.

Fakat döngünün tek amacı “Bu iki sıralı koleksiyon birbirine eşit mi?” sorusunu yanıtlamaksa aynı davranışı kendimiz yazmak zorunda değiliz.

.NET temel kütüphanesinde bunun için SequenceEqual() bulunur:

```
bool areEqual =
   first.SequenceEqual(second);
```

Bu kodun en önemli avantajı kısa olması değildir. Asıl avantaj, niyeti doğrudan ifade etmesidir.

Artık iki dizinin nasıl karşılaştırılacağını anlatmıyoruz. Yalnızca iki sıranın eşit olup olmadığını soruyoruz.

SequenceEqual() sıra duyarlıdır. Aşağıdaki iki koleksiyon aynı elemanlara sahip olmasına rağmen eşit değildir:

```
int[] first  = { 1, 2, 3 };
int[] second = { 3, 2, 1 };

bool result =
   first.SequenceEqual(second); // false
```

Eleman sayısı, elemanların sırası ve kullanılan eşitlik karşılaştırıcısı sonucu belirler.

Özel bir karşılaştırma kuralı gerekiyorsa uygun bir IEqualityComparer<T> de sağlanabilir:

```
bool areEqual =
   first.SequenceEqual(second, comparer);
```

Ancak her karşılaştırma işlemi basit eşitlik değildir.

Şu durumlarda özel bir döngü yazmak daha doğru olabilir:

- Ondalık sayılarda tolerans uygulanacaksa
- Elemanların sırası önemli değilse

- Uyuşmayan elemanın konumu bulunacaksa
- Özel iş kuralları çalıştırılacaksa
- Karşılaştırmanın neden başarısız olduğu raporlanacaksa

Pratik kural şudur:
Döngünüz yalnızca "Bu iki sıra aynı mı?" sorusunu yanıtlıyorsa SequenceEqual() kullanın. Döngü başka iş kuralları da yürütüyorsa özel karşılaştırma kodu yazın.

**3. STATIC YEREL FONKSİYONLAR**

Küçük yardımcı mantığı kullanıldığı yerde tutun ve dış bağlama olan bağımlılığı kapatın.
Yerel fonksiyonlar, yalnızca belirli bir metodun ihtiyaç duyduğu yardımcı işlemleri sınıf seviyesine taşımadan aynı metodun içinde tanımlamamızı sağlar.

```
public void ProcessNumbers()
{
   int Square(int value)
   {
      return value * value;
   }
   Console.WriteLine(Square(5));
}
```

Bu yaklaşım, yardımcı metodun yalnızca ProcessNumbers() içinde kullanılacağını açıkça gösterir.
Yerel fonksiyon çevresindeki değişkenlere ihtiyaç duymuyorsa static olarak işaretlenebilir:

```
public void ProcessNumbers()
{
   static int Square(int value)
   {
      return value * value;
   }
```

static anahtar sözcüğü, yerel fonksiyonun çevresindeki değişkenleri yakalamasını engeller.
Örneğin aşağıdaki kod derlenmez:

```
int multiplier = 2;
static int Multiply(int value)
{
   return value * multiplier;
}   Console.WriteLine(Square(5));
}
```

Çünkü multiplier, yerel fonksiyonun dışındaki bir değişkendir.
Bu derleme hatası aslında yararlıdır. Fonksiyonun görünmeyen bağımlılıklar edinmesini engeller ve fonksiyonun yalnızca kendisine verilen parametrelerle çalıştığını garanti eder.
Değişken yakalama işlemleri bazı durumlarda derleyicinin closure yapıları oluşturmasına neden olabilir. Bu durum özellikle fonksiyon bir delegate'e dönüştürüldüğünde veya normal yaşam alanının dışına taşındığında ek maliyetler oluşturabilir.
Ancak burada dikkatli olmak gerekir.
Bir yerel fonksiyona static eklemek her durumda heap allocation ortadan kaldırıldığı anlamına gelmez. Derleyici bazı yerel fonksiyon çağrılarını zaten verimli şekilde düzenleyebilir.
Bu özelliğin en sağlam avantajı performanstan önce tasarımdır:

- Fonksiyonun bağımlılıkları açık hale gelir.
- İstenmeyen değişken yakalamaları engellenir.
- Yeniden düzenleme sırasında fonksiyonun davranışı daha kolay korunur.
- Derleyici, dış bağlama erişim girişimlerini hata olarak bildirir.

Performans açısından kritik kodlarda gerçek kazanç BenchmarkDotNet veya bir profiler ile ölçülmelidir.

**4. UNMANAGED GENERIC KISITI**

Bir türün yalnızca değer türü olmasını değil, içinde yönetilen referans taşımamasını isteyin.
Generic kısıtlarda en sık class, struct ve new() kullanılır. Daha az kullanılan unmanaged kısıtı ise özellikle native API, binary veri ve ham bellek işlemlerinde önemli bir güvence sağlar.
struct kısıtı yalnızca türün bir değer türü olduğunu garanti eder:

```
public static void Print<T>(T value)
   where T : struct
{
   Console.WriteLine(value);
}
```

Fakat bir türün struct olması, içinde managed referans bulunmadığı anlamına gelmez.
Örneğin:

```
public struct Employee
{
   public int Id;
   public string Name;
}
```

Employee bir değer türüdür ve where T : struct kısıtını karşılar.
Ancak içindeki string alanı managed heap üzerindeki bir nesneye referans taşır. Bu nedenle Employee, ham bellek işlemleri için unmanaged bir tür değildir.
unmanaged kısıtı daha güçlü bir garanti verir:

```
public static unsafe int SizeOf<T>()
   where T : unmanaged
{
   return sizeof(T);
}
```

Bu kısıt, T türünün ve içindeki bütün alanların unmanaged türlerden oluşmasını ister.
Aşağıdaki yapı uygundur:

```
public struct Point
{
   public int X;
   public int Y;
}
```

Fakat içinde string, object, array veya başka bir managed referans bulunan yapılar kabul edilmez.
Bu güvence ham bayt işlemleri yapan metotlarda kullanılabilir:

```
public static unsafe void Write<T>(
   Stream stream,
   T value)
   where T : unmanaged
{
   Span<byte> buffer =
      stackalloc byte[sizeof(T)];
   MemoryMarshal.Write(buffer, in value);
   stream.Write(buffer);
}
```

Derleyici, T içinde yönetilen nesne referansı bulunmasını engeller.

- Böylece yanlışlıkla bir nesne referansını anlamlı binary veriymiş gibi yazma riski azaltılır.

Ancak unmanaged kısıtı otomatik olarak taşınabilir bir dosya biçimi sağlamaz.
Aşağıdaki konular hâlâ geliştiricinin sorumluluğundadır:

- Struct alanlarının bellekteki sırası
- Alanlar arasındaki padding boşlukları
- İşlemcinin byte sırası
- Platform farklılıkları
- Türün ilerleyen sürümlerde değişmesi
- Dosya veya protokol sürümlemesi

Bu nedenle uzun süre saklanacak verilerde veya farklı sistemler arasında taşınacak binary protokollerde açık bir veri biçimi ve sabit byte sırası kullanmak genellikle daha güvenlidir.
unmanaged kısıtı özellikle şu alanlarda değerlidir:

- Native API entegrasyonları
- Binary protokoller
- Özel serileştiriciler
- Oyun motorları
- Yüksek performanslı veri işleme
- Ham bellek kullanan kütüphaneler

Sıradan CRUD uygulamalarında ise çoğu zaman gerekli değildir.

**5. MEMORYMARSHAL.CAST() İLE KOPYASIZ YENİDEN YORUMLAMA**

Bu API veriyi dönüştürmez. Aynı belleğe farklı bir türün gözünden bakar.
Elinizde aşağıdaki gibi sekiz baytlık bir veri bulunduğunu düşünün:

```
byte[] data =
{
   1, 0, 0, 0,
   2, 0, 0, 0
};
```

Bu baytları iki adet int değeri olarak görmek isteyebiliriz.
MemoryMarshal.Cast() yeni bir dizi oluşturmaz ve baytları başka bir alana kopyalamaz:

```
Span<byte> bytes = data;

Span<int> values =
   MemoryMarshal.Cast<byte, int>(bytes);

Console.WriteLine(values[0]);
Console.WriteLine(values[1]);
```

Aynı bellek bölgesi bu kez Span<int> olarak yorumlanır.
Little-endian bir sistemde şu baytlar:
01 00 00 00
int olarak 1 değerini temsil eder.
Bellekteki veri değişmemiştir. Yalnızca veriye bakış biçimi değişmiştir.
İki span aynı belleğe baktığı için bir görünüm üzerinden yapılan değişiklik diğer görünümde de görülür:

```
Span<byte> bytes =
   stackalloc byte[4];

Span<int> numbers =
   MemoryMarshal.Cast<byte, int>(bytes);

numbers[0] = 42;
Console.WriteLine(bytes[0]);
```

Burada herhangi bir kopyalama işlemi yapılmaz. 42 değeri doğrudan asıl byte buffer üzerine yazılır.
Bu yöntem binary dosyalar, ağ paketleri veya büyük veri blokları üzerinde çalışırken gereksiz geçici dizileri ve bellek kopyalamalarını ortadan kaldırabilir.
Fakat MemoryMarshal.Cast() kullanırken bazı önemli riskler bulunur:

- Kaynak ve hedef türlerin boyutları bilinmelidir.
- Kaynak uzunluğu hedef türün boyutuna uygun olmalıdır.
- İşlemcinin byte sırası hesaba katılmalıdır.
- Bellek yerleşiminin platforma bağlı olabileceği unutulmamalıdır.
- Managed referans içeren türler kullanılmamalıdır.
- Aynı belleğe bakan görünümlerin birbirini etkilediği bilinmelidir.

Harici bir protokol okunuyorsa platformun byte sırasına güvenmek yerine BinaryPrimitives gibi açık endian işlemleri sağlayan API'ler daha güvenli olabilir.
Örneğin:

```
int value =
   BinaryPrimitives.ReadInt32LittleEndian(bytes);
```

Bu kod, verinin little-endian olduğunu açıkça belirtir ve farklı platformlarda daha tahmin edilebilir davranır.
MemoryMarshal.Cast() özellikle şu alanlarda değerlidir:

- Ağ paketlerinin işlenmesi
- Görüntü ve ses işleme
- Binary dosya biçimleri
- Oyun motorları
- Native bellek işlemleri
- Büyük veri bloklarının işlenmesi
- Ölçümle doğrulanmış performans darboğazları

Buna karşılık sıradan iş mantığı veya CRUD kodlarında okunabilirlik çoğu zaman birkaç bellek kopyasından daha değerlidir.

C#'ın gelişimi çoğu zaman büyük ve devrimsel değişikliklerden değil, günlük kodun sürtünmesini azaltan dikkatli iyileştirmelerden oluşuyor.
Range ve Index operatörleri indis aritmetiğini daha açık bir niyete dönüştürüyor.
SequenceEqual, uzun karşılaştırma döngülerini semantik bir soruya indiriyor.
Static yerel fonksiyonlar görünmeyen bağımlılıkları engelliyor.
Unmanaged kısıtı, tür sistemini ham bellek güvenliğinin bir parçası haline getiriyor.
MemoryMarshal.Cast ise doğru problemde gereksiz bellek kopyalarını ortadan kaldırıyor.
Bu özelliklerin hiçbiri, her yerde kullanılmak için tasarlanmadı. İyi C# kodu, en ileri API'leri kullanan kod değildir. Kullandığı özelliğin davranışını ve maliyetini bilen, onu doğru bağlamda tercih eden koddur.
Önce niyetinizi açıkça yazın. Ardından özelliğin çalışma zamanındaki davranışını anlayın. Performans gerçekten önemliyse tahmin etmek yerine ölçün.

Modern C#'ın gerçek gücü tam olarak bu dengede yatıyor.

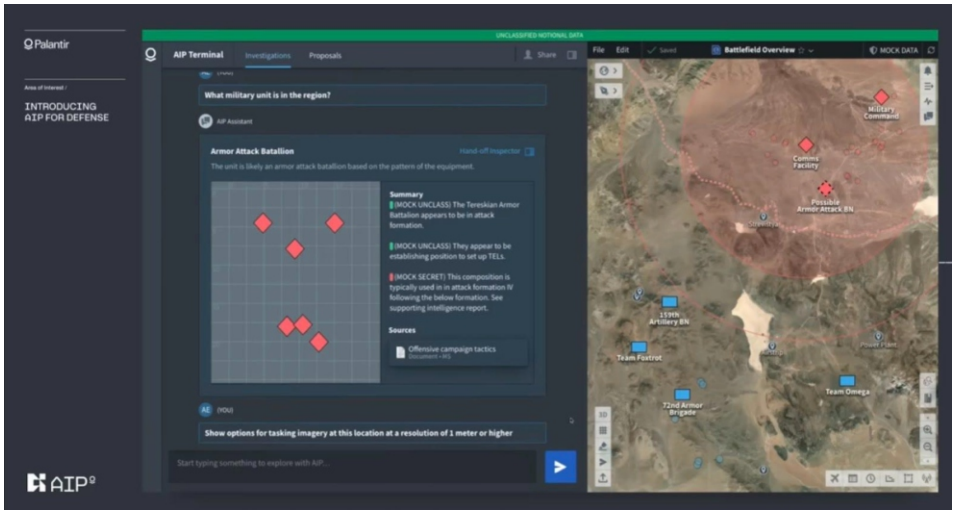
**Erkan Coşkun**
Bilgisayar Mühendisi

# VERİ YENİ PETROL MÜ?

## Savaş Alanından Hastanelere Palantir'in Görünmeyen Gücü

Bir yazılım düşünün: Bir hastanede yatak ve personel planlamasına yardım ederken, başka bir ülkede uydu görüntülerini, drone verilerini ve istihbarat raporlarını aynı ekranda bir araya getiriyor. Peki veri karara, karar da silaha dönüştüğünde son söz gerçekten insanda mı kalıyor?

"Veri yeni petroldür" sözünü artık




Palantir AIP for Defense platformunun temsili savaş alanı arayüzü. Görseldeki bilgiler gerçek bir operasyona değil, "unclassified notional data" olarak belirtilen örnek bir senaryoya aittir.(https://newsletter.safe.ai/p/ai-safety-newsletter-4)

neredeyse her yerde duyuyoruz. Bu benzetme ilk kez 2006 yılında İngiliz veri bilimci Clive Humby tarafından ortaya atılmıştı. Humby'nin asıl anlatmak istediği şuydu: Ham petrol nasıl işlenmeden pek işe yaramıyorsa veri de analiz edilmeden tek başına fazla değer taşımaz. Fakat arada önemli bir fark var. Petrol kullanıldıkça tükenir; veri ise kopyalanabilir, tekrar tekrar işlenebilir ve başka verilerle birleştirildiğinde yeni anlamlar kazanabilir.[12] Bugün asıl güç, en fazla veriye sahip olmaktan çok, o veriyi en hızlı biçimde karara dönüştürebilmekte yatıyor. Palantir de tam olarak bu noktada karşımıza çıkıyor. Palantir Technologies, 2003 yılında kuruldu. Şirketin ABD Menkul Kıymetler ve Borsa Komisyonuna sunduğu belgelerde, ilk yazılımlarını ABD istihbarat kurumlarının terörle mücadele çalışmalarına yardımcı olmak amacıyla geliştirdiği açıkça belirtiliyor.[1] Burada sık yapılan bir yanlışı da düzeltmek gerekiyor: **Palantir'i CIA kurmadı.** Ancak CIA'nın teknoloji yatırımları için oluşturduğu In-Q-Tel, şirketin ilk dönem yatırımcılarından biri oldu. Paradan belki daha önemlisi, In-Q-Tel Palantir ekibini Amerikan istihbarat analistleriyle bir araya getirdi. Böylece yazılım, yıllarca gerçek kullanıcıların ihtiyaçlarına göre geliştirildi.[2, 3] In-Q-Tel'in kendisi de 1999 yılında CIA'nın hızla gelişen bilgi teknolojilerinin gerisinde kalmaması amacıyla kurulmuştu.

Peki Palantir aslında ne yapıyor?

En basit hâliyle farklı yerlerde bulunan verileri birbirine bağlıyor. Uydu görüntüleri bir sistemde, konum bilgileri başka bir sistemde, personel kayıtları başka bir yerde, istihbarat raporları ise bambaşka bir veri tabanında bulunabilir. İnsanların bütün bunları tek tek inceleyip aralarındaki bağlantıları kurması saatler, hatta günler sürebilir. Palantir'in Gotham platformu daha çok savunma, güvenlik ve istihbarat alanına odaklanıyor. Foundry şirketlerde, fabrikalarda ve sağlık kurumlarında kullanılan operasyonel veri platformu olarak öne çıkıyor. AIP, yani Artificial Intelligence Platform ise büyük dil modellerini ve diğer yapay zekâ sistemlerini kurumların kendi verileri ve iş süreçleriyle buluşturuyor. Şirketin tanımına göre AIP; yapay zekâyı yalnızca soru cevaplayan bir sohbet robotu olmaktan çıkarıp gerçek operasyonlar içinde çalışan, kayıt altına alınabilir bir araca dönüştürmeyi amaçlıyor.[4] Kısacası Palantir çoğu zaman silah üretmiyor. Fakat silahın, personelin, uydunun, sensörün ve karar vericinin aynı dijital tablo üzerinde buluşmasını sağlıyor. İşin asıl çarpıcı kısmı da burada başlıyor.

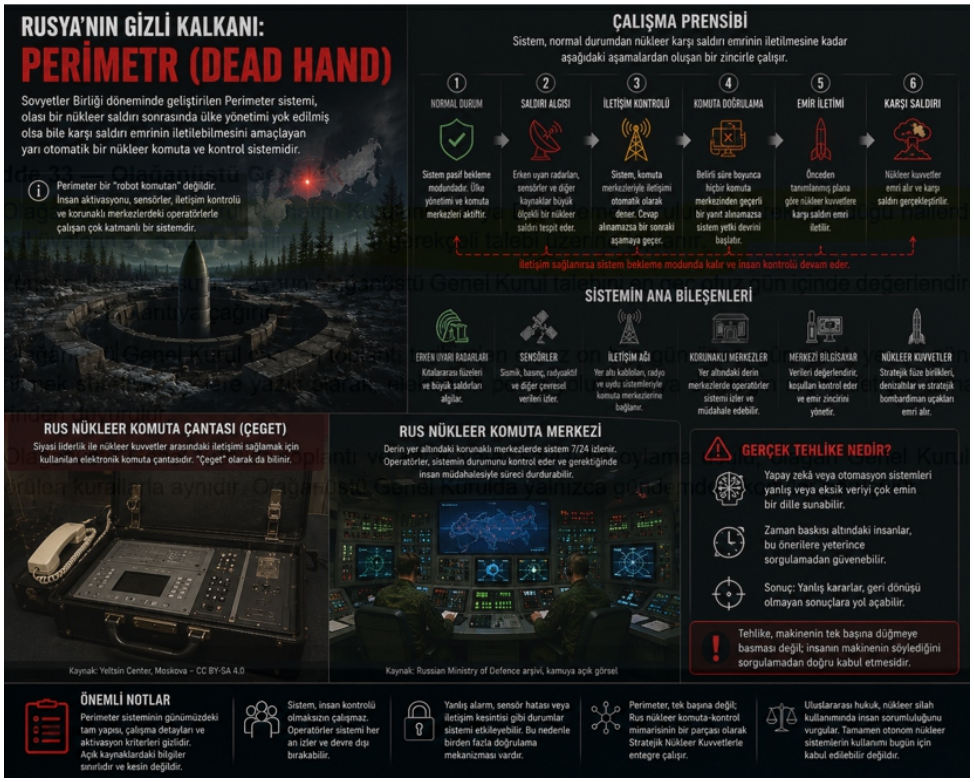
### Bir hastane ile savaş alanının ortak noktası

İlk bakışta bir hastane ile savaş alanı arasında hiçbir benzerlik yokmuş gibi görünebilir. Ancak ikisinde de zaman kritiktir, kaynaklar sınırlıdır ve yanlış kararların bedeli insan hayatıdır. Bir hastanede hangi hastanın hangi yatağa yerleştirileceği, kaç hemşirenin görev yapacağı ve ameliyathanenin ne zaman kullanılacağı hesaplanır. Savaş alanında ise hangi birliğin nerede olduğu, mühimmatın ne kadar kaldığı, hava koşullarının nasıl değiştiği ve bir görüntüdeki cismin gerçekten askerî hedef olup olmadığı değerlendirilebilir. Palantir'in kendi yayımladığı verilere göre Tampa General Hospital'da Foundry kullanımı sonrasında hasta yerleştirme süresinde ve ameliyat sonrası bekleme sürelerinde düşüş sağlandı. Ancak burada dikkatli olmak gerekiyor: Bu rakamlar şirket ve müşterisi tarafından açıklanan sonuçlardır; bağımsız bilimsel deneyler gibi değerlendirilmemelidir. Yine de aynı veri işleme mantığının sağlık alanından savunmaya kadar ne kadar farklı yerlerde kullanılabildiğini göstermesi bakımından önemlidir.[7]

Bu zincir günümüz savaşlarında teoriden


ibaret değil. ABD Savunma Bakanlığı, Palantir'e 2024 yılında Maven Smart System için 480 milyon dolarlık bir sözleşme verdi. 2025 yılında aynı sözleşmeye 795 milyon dolarlık ilave yapıldı. Project Maven'ın temel amacı, çok büyük miktardaki görüntü ve sensör verisinin yapay zekâ yardımıyla analiz edilmesi ve askerî personelin daha hızlı bir ortak operasyon resmi oluşturabilmesidir.[5] Palantir'in savaş alanındaki en belirgin örneklerinden biri ise Ukrayna'dır. Şirketin CEO'su Alex Karp, 2023 yılında Ukrayna ordusunun Palantir yazılımlarını Rus

kuvvetlerine karşı kullandığını açıkça söyledi. Mayıs 2026'da Reuters'ın aktardığı bilgilere göre Ukrayna ve Palantir, savaş boyunca toplanan verileri kullanarak Rus insansız hava araçlarının tespit ve önlenmesine yardımcı olacak yapay zekâ modelleri geliştirmek için Brave1 Dataroom projesinde iş birliğini genişletti. Ukraynalı yetkililer ayrıca Palantir teknolojilerinin hava saldırılarının analizi, büyük miktarda istihbaratın işlenmesi ve uzun menzilli operasyonların planlanmasında kullanıldığını açıkladı.[6] Şunu açıkça belirtmek gerekir: Yazılımın ekranda bir hedef göstermesi, o hedefi kendi başına vurduğu anlamına gelmez. Fakat sistem; hangi verinin öne çıkarılacağını, hangi hareketin şüpheli sayılacağını ve karar vericinin önce neye bakacağını belirliyorsa sonuç üzerinde ciddi bir etkisi vardır. Bir sistem tetiği çekmeyebilir. Ama hedefi seçen göz hâline geliyorsa, gerçekten yalnızca "yardımcı araç" mıdır?




### Hız arttıkça düşünmek için kalan süre azalıyor

Yapay zekânın askerî alandaki en büyük avantajı hızdır. Aynı zamanda en büyük tehlikesi de bu olabilir. Bir insan yüzlerce uydu görüntüsünü birkaç saniyede inceleyemez. Yapay zekâ ise binlerce görüntüyü tarayıp şüpheli gördüğü noktaları işaretleyebilir. Fakat bir sistemin hızlı olması, doğru olduğu anlamına gelmez. Kötü hava koşulları, eksik veriler, yanıltıcı görüntüler, sensör arızaları veya eğitim verilerindeki hatalar yanlış sonuçlara yol açabilir. Üstelik insanlar, bilgisayarın verdiği cevabı sorgulamadan kabul etmeye yatkın olabilir. Buna "otomasyon yanlılığı" deniyor. Ekranda "yüzde 92 askerî hedef" yazdığını düşünelim. Operatör, bu oranın nasıl hesaplandığını bilmiyorsa yine de sistemi sorgulayabilecek mi? Yoksa zaman baskısı altında, "Bilgisayar böyle söylediyse doğrudur" diyerek onay mı verecek? NATO'nun yapay zekâ stratejisinde hukuka uygunluk, hesap verebilirlik, açıklanabilirlik, güvenilirlik, yönetilebilirlik ve önyargıların azaltılması özellikle vurgulanıyor. Bu ilkeler güzel görünüyor. Fakat gerçek bir savaş ortamında hız, korku ve baskı devreye girdiğinde bunların ne kadar uygulanabileceği hâlâ büyük bir soru işaretidir.[8]

### Eminim ki herkesin aklında olan soru: Yapay zekâ nükleer düğmeye basar mı?

Yapay zekâ ve savaş konusu açıldığında akla gelen en ürkütücü soru budur. Önce gerçeği şehir efsanesinden ayırmak gerekiyor: Palantir'in doğrudan bir ülkenin nükleer silahlarını fırlatma yetkisine sahip olduğuna dair kamuya açık, güvenilir bir kanıt bulunmuyor. Ayrıca Amerika Birleşik Devletleri, nükleer silahların kullanılması veya kullanımının sonlandırılmasıyla ilgili kritik işlemlerde insanın karar zincirinde tutulacağını resmî olarak açıklamıştır.[10] Ancak mesele yalnızca son düğmeye kimin bastığı değildir. Bir yapay zekâ radar verisini incelerse, yaklaşan cismin füze olduğuna karar verirse, tehdit seviyesini hesaplar ve devlet başkanının önüne seçenekler koyarsa, son kararı veren insan olsa bile kararın çerçevesini makine çizmiş olabilir. 2024 yılında Stanford bağlantılı araştırmacıların gerçekleştirdiği bir savaş oyunu çalışmasında beş farklı büyük dil modeli, sekiz kurgusal ülkenin karar vericileri olarak kullanıldı. Araştırmada modellerin tamamı bazı senaryolarda öngörülmesi zor biçimde gerilimi artırdı; silahlanma yarışları oluştu ve nadir bazı denemelerde nükleer silah kullanımına kadar gidildi. Bu deney gerçek bir nükleer sistem değildi ve "her yapay zekâ kesinlikle nükleer savaş başlatır" anlamına gelmiyor. Fakat kritik kararların otonom dil modellerine bırakılmasının ne kadar riskli olabileceğini gösteriyor.[9] Rusya konusunda da sıkça yanlış bilgiler dolaşıyor. Sovyetler Birliği döneminde geliştirilen **Perimeter**, Batı'da bilinen adıyla "Dead Hand", olası bir nükleer saldırı sonrasında ülke yönetimi yok edilmiş olsa bile karşı saldırı emrinin iletilebilmesini amaçlayan yarı otomatik bir sistemdi. Fakat bunu günümüzdeki üretken yapay zekâlarla çalışan bağımsız bir "robot komutan" gibi anlatmak doğru değildir. Kamuya açık bilgiler sistemin insan aktivasyonu, sensörler, iletişim kontrolü ve korunaklı merkezlerdeki operatörlerle ilişkili olduğunu gösteriyor; günümüzdeki tam durumu ise şeffaf değildir.[11] Yani korkmamız gereken şey yalnızca bir gün kötü niyetli bir robotun nükleer düğmeye basması değildir. Daha gerçekçi tehlike; yanlış veya eksik veriyi çok emin bir dille sunan sistemlere, karar vermek için yalnızca birkaç dakikası bulunan insanların gereğinden fazla güvenmesidir.

### Son söz gerçekten insanda mı?

Palantir gibi sistemler doğru kullanıldığında hastanelerin kaynaklarını daha iyi yönetebilir, afetlerde ekiplerin yönlendirilmesine yardım edebilir, kayıp kişilerin bulunmasını kolaylaştırabilir ve askerlerin tehlikeli bölgelere gönderilmeden önce daha fazla bilgi edinmesini sağlayabilir. Fakat aynı teknoloji gözetim, hedef belirleme, sınır kontrolü ve savaş planlaması için de kullanılabilir. Teknoloji kendi başına iyi veya kötü değildir

demek kolaydır. Ancak bence bu cümle artık yeterli değil. Çünkü kullanılan sistem yalnızca verilen emri yerine getirmiyor; hangi seçeneklerin görüleceğini, hangi verinin önemli sayılacağını ve hangi riskin kabul edilebilir olduğunu da şekillendiriyor. Bir algoritma vicdan azabı duymaz. Bir koordinatın okul, hastane veya ev olduğunu kendi başına önemsemez. Ona hangi veriler verilmişse ve hangi hedef tanımlanmışsa buna göre hesap yapar. İnsanlığın önündeki asıl soru, yapay zekânın bizden daha hızlı karar verip veremeyeceği değildir. Bunun cevabını zaten biliyoruz: Verebilir.

Asıl soru şudur: **Daha hızlı olmak uğruna, verdiğimiz kararın ne kadarını bir makineye bırakmaya razıyız?**

Sanayi Devrimi'nin gücü makinelerdi. Petrol çağının gücü enerjiydi. Bugünün gücü ise veri, işlem kapasitesi ve bu ikisini gerçek dünyadaki kararlara dönüştürebilen sistemlerdir. Palantir bu yeni dönemin tek şirketi değil. Fakat bize geleceğin nasıl görünebileceğine dair oldukça açık bir pencere sunuyor. Belki geleceğin savaşlarını en fazla tanka sahip ülkeler kazanmayacak. Belki en fazla veriyi, en kısa sürede, en etkili karara dönüştürebilen ülkeler kazanacak. Fakat o gün geldiğinde sorulması gereken son soru şu olacak:

**Kararı biz mi verdik, yoksa bize yalnızca onaylamak mı kaldı?**

**KAYNAKÇA**


1. Palantir Technologies, **2022 Form 10-K**, şirketin kuruluşu ve ABD istihbarat topluluğuyla ilk çalışmaları.
Bağlantı: https://www.sec.gov/Archives/edgar/data/1321655/000132165523000011/pltr-20221231.htm

2. In-Q-Tel, **Our Milestones**; In-Q-Tel'in kuruluş amacı ve istihbarat teknolojileri yatırımları.
Bağlantı: https://www.iqt.org/about/our-milestones

3. Wired, **Palantir Technologies Spots Patterns to Solve Crimes and Track Terrorists**; Palantir–In-Q-Tel ilişkisinin ilk yılları.
Bağlantı: https://www.wired.com/story/joining-the-dots

4. Palantir Technologies, **AIP Overview ve AIP for Defense**; platformun veri, yapay zekâ ve operasyonları birleştirme özellikleri.
Bağlantı: https://www.palantir.com/docs/foundry/aip

5. ABD Savunma Bakanlığı, **Maven Smart System sözleşmeleri**, 2024 ve 2025.
2024 sözleşmesi: https://www.defense.gov/News/Contracts/Contract/Article/3790490/ | 2025 sözleşme ilavesi: https://www.defense.gov/News/Contracts/Contract/Article/4194643/

6. Reuters, **Zelenskiy Meets Palantir CEO as Ukraine Expands Use of AI in War**, 12 Mayıs 2026.
Bağlantı: https://www.reuters.com/world/europe/zelenskiy-meets-palantir-ceo-ukraine-expands-use-ai-war-2026-05-12/

7. Palantir Technologies, **Tampa General Hospital Impact Study**. Sonuçlar şirket ve müşteri tarafından açıklanmıştır.
Bağlantı: https://www.palantir.com/impact/tampa-general-hospital

8. NATO, **Summary of NATO's Revised Artificial Intelligence Strategy**, 10 Temmuz 2024.
Bağlantı: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

9. Rivera ve diğerleri, **Escalation Risks from Language Models in Military and Diplomatic Decision-Making**, ACM FAccT 2024.
Bağlantı: https://arxiv.org/abs/2401.03408

10. ABD Savunma Bakanlığı, **The State of AI in the Department of Defense**; nükleer karar zincirinde insan kontrolüne ilişkin açıklama.
Bağlantı: https://www.defense.gov/News/Speeches/Speech/Article/3578046/remarks-by-deputy-secretary-of-defense-kathleen-h-hicks-on-the-state-of-ai-in-t/

11. Cambridge University Press, **Delegating Destruction: Coercive Threats and Automated Nuclear Systems**; Sovyet Perimeter sistemi ve otomatik nükleer sistemler.
Bağlantı: https://www.cambridge.org/core/journals/international-organization/article/delegating-destruction-coercive-threats-and-automated-nuclear-systems/B8ED249483153AF331F2C998730F7716

Olhede ve Rodrigues, **Why Data Is Not a Commodity**, Oxford Academic; "veri yeni petroldür" benzetmesinin sınırları.
Bağlantı: https://academic.oup.com/jrssig/article/14/5/10/7029251


**Ata Ateş**
Yapay Zeka Mühendisliği
DAÜ 2. sınıf öğrencisi

# Kayıplar Olmasaydı, Bugün Neredeydik?

*Geçen sayıda, modelle çıktığımız yolda modeli kaybettiğimizi yazmıştım; Necdet İcil hocam da o yıllarda yapılanları kendi kaleminden kayıt altına almış, benim anlatmaya çalıştığım birlikteliğin kronolojisini çok daha yetkin biçimde ortaya koymuştu. Bu ay kaldığım yerden devam etmek istiyorum; ama bu kez geriye değil, hiç yaşanmamış bir bugüne bakarak. Bir düşünce egzersizi yapalım: Ya o masa dağılmasaydı? Ya kurumsal hafıza kaybedilmeseydi? Bugün neredeydik? Bu soruyu hayıflanmak için sormuyorum; kaybettiğimizin envanterini çıkarmadan yeniden başlayacağımız yeri bilemeyiz. Kayıp, ancak adı konduğunda telafi edilebilir hale gelir.*

**Model güncellenirdi**

Yol devam etseydi ilk iş modeli güncellemek olurdu; çünkü o model bir fotoğraf değil, Lizbon Stratejisi'ni ve ardından Avrupa Dijital gündemini izleyen, dünyanın en iyi örneklerini kendi ölçeğimize göre harmanlayan bir yöntemdi. O yöntem yaşasaydı model de dünyayla birlikte nefes alacak; veri korumada, dijital kimlikte, siber güvenlikte ve yapay zekâda baştan aşağı yenilenen dünyaya uyarlanmış olacaktı. Modelin bugüne uyarlanmış hali nasıl olabilirdi sorusunun cevabını ilerleyen sayılara bırakalım. Çünkü yol devam etseydi ikinci iş çok daha yakıcı olurdu ve bu yazının asıl konusu odur: Yarım bıraktığımız yasaları tamamlamak, yasalaşanları ise bugünün dünyasına göre elden geçirmek. Hatırlayalım; Meclis'e gitmek için sırasını bekleyen bir mevzuat ailesi vardı. O ailenin bir kısmı Meclis'e hiç ulaşamadı, bir kısmı bir süre sonra ortak akıldan ve kaybolan modelden ayrıştırılarak ulaştı, kimi yasalar hiç doğmadı, doğanlar ise bir daha elden geçirilmedi.

**Kopuk mevzuat bugünü hazırladı**

Bugünkü tabloyu tek cümleyle özetlemek mümkün: Her kurum kendi yasasını kendi dar penceresinden güncelledi, olmayan yasalar ise hiç yapılmadı. Ortaya bütünleşik bir devlet değil, ayrı mevzuat adaları çıktı. Oysa vatandaş adalarla değil, tek bir devletle muhatap olmak ister; adaların arasında kalınca aynı bilgi tekrar tekrar istenir, hizmetler birbiriyle konuşmaz, bir sorun çıktığında sorumluluğun kimde olduğu bulanıklaşır. Bunun teoride kalmadığını iki sayı önce Bilişim Suçları Yasası üzerinden anlatmıştım: Büyük resimden kopuk yazılan o metin, siber güvenlikle içerik denetimini aynı torbaya koyduğu için sonunda iki alanın da hakkını veremedi. Kopuk mevzuat bugünkü dağınıklığın zemini oldu; eksik mevzuat ise o zeminin üzerine bir şey inşa edilememesine yol açtı.

**Yeni yasa, eski alışkanlık: 2023 deneyimi**

Kopukluğun en güncel örneğine de değinmek isterim. 2023'ün aralık ayında Meclis'ten oybirliğiyle geçen Dijital Dönüşüm ve Elektronik Devlet Kurumu Yasası, önce hakkı teslim edilmesi gereken bir adımdır: Dijital dönüşümü sahiplenecek bir kurumun nihayet yasal kimliğe kavuşması başlı başına bir kazanımdır. Hazırlık sürecinde bizden ve birçok kesimden görüş alındı; ben de görüş verenlerdendim. Bu yüzden bu bölümü bir yergi olarak değil, o gün anlatmaya çalıştıklarımın kaydı olarak okumanızı isterim.

O gün anlattığımız şuydu: Yola merkezileşmeyle değil, birlikte çalışabilirlikle çıkılmalıdır. Önce veriyi kaynağında tutan, kurumlar arasında güvenli bir değişim katmanıyla paylaşan yapı kurulmalı; veri tekrarları ayıklanıp gerçek bir servis modeli oturduktan sonra merkezileşme, yapıyı sadeleştiren bir optimizasyon olarak kademe kademe artırılmalıdır. Bazı yapılar ise — hızlı ve yerinde erişim isteyen alanlar — en yedekli altyapıda bile ancak kısmen merkeze yaklaşabilir. Yasanın bu kademeli yolculuğu planlamasını beklerdim; bunu yazılı olarak da iletmiştik. Metin ise bütün kamu verisinin tek bir entegre veri merkezinde toplanmasını ve yalnızca orada tutulmasını esas aldı, bütün kamu sistemlerine de iki yıl içinde taşınma ödevi verdi.

Bunu yasayı yermek için değil, dünyanın gittiği yöne baktığım için söylüyorum. Elektrik önce birkaç merkezde üretilip dağıtıldı; bugün evlerin kendi enerjisini üretip şebekeye kattığı modellere geri dönüyoruz. Haberleşme de tek merkezli yıldız yapılardan, 5G ile düğümlerin birbirine atladığı örgü yapılara evriliyor. Teknolojinin yönü tek merkez değil; birbiriyle konuşan, yedekli, sürekliliği kendi içinde taşıyan yapılardır. Bizim modelimiz, Estonya dersini daha 2000'lerde çalışmış bir ekibin elinde tam da bunu söylüyordu. Bir kurum yasasında kadrolar elbette olacaktır; ama dönüşüm kadroyla değil, mimariyle ve mevzuat ailesinin bütünüyle olur. Kopukluk bitmedi, biçim değiştirdi: Dün yasalar hiç yapılmadığı için kopuktuk; bugün yasa, ailenin geri kalanı olmadan tek başına yapıldığı için kopuğuz.

**Eksik olanlar: devletin çatısı hâlâ açık**

Yol devam etseydi bugün elimizde olacak, ama hâlâ olmayan yasaların başında bir çatı yasa geliyor: dijital devletin, kamu verisinin ve dijital katılımın ortak ilkelerini kuran temel yasa. Vatandaşın dijital hizmet hakkını, devletin zaten bildiği bilgiyi bir daha istememesini, güvenli ve kayıtlı veri paylaşımını, açık veriyi ve geçen sayıda anlattığım katılım araçlarını tek tek kurum yasalarıyla kuramazsınız. Bu yasanın doğal yürütücüsü de elbette 2023'te kurulan Kurumdur; eksik olan yeni bir kurum değil, elimizdeki Kuruma koordine edeceği bütünün hukuki tarifini verecek yasadır. En acil eksiğimiz budur; çünkü diğer her şeyin üzerine oturacağı zemin burasıdır.
İkincisi, ulusal bir siber güvenlik merkezidir. Fidye yazılımı mağduriyetlerinin ülkemizde ulaştığı boyuta rağmen bu olayların kaydını bile tutmuyoruz; ölçmediğimiz tehdide karşı tedbir alınmaz. Kamunun kritik sistemlerini izleyecek, olayları koordine edecek ve kurumlara rehberlik edecek küçük ama uzman bir teknik merkez, devasa bir teşkilat kurmadan da mümkündür; yeter ki adli kolluk değil, teknik koordinasyon otoritesi olarak tanımlansın.

Üçüncüsü, çevrimiçi içerik ve dijital hizmetleri düzenleyen ayrı bir yasadır. Bilişim Suçları Yasası'ndan çıkarılması gereken içerik hükümlerinin gidebileceği bir ev olmadıkça, o hükümler olduğu yerde sorun üretmeye devam eder. İçerik alanı elbette düzenlenebilir; ama kendi

yasasında, bildirim ve itiraz mekanizmalarıyla, mahkeme güvencesi ve ölçülülük esasıyla.

Dördüncüsü, kamuda yapay zekâ ve otomatik karar sistemleridir. Yapay zekâ kamu hizmetine zaten girmektedir; mesele yasaklamak değil, kayıt altına almak, riskine göre sınıflandırmak ve vatandaşı etkileyen kararlarda insan denetimini, itiraz hakkını ve açıklanabilirliği güvence altına almaktır. Bu yasanın yürütücüsü de doğal olarak yine aynı Kurumdur; yani çatı yasa da yapay zekâ yasası da Kuruma rakip yaratmaz, tersine elini güçlendirir ve görevini tarif eder.

Bu iki yasayı birbirine bağlayan bir gerçek daha var: Yazılım dünyası, kodun giderek artan bölümünün yapay zekâ ajanları tarafından yazılacağı bir döneme giriyor. Bu, korkulacak değil, hazırlanılacak bir gelecektir ve hazırlığın ilk adımı açık standart ile açık kaynaktır; çünkü kodu kapalı, sahibi belirsiz bir yazılımı ne bir ajan devralabilir ne de başka bir kurum yeniden kullanabilir. Bugünden ilkelerimizi koymazsak, tekrarlanan veri hastalığının yazılımdaki karşılığını yaşarız: her kurumun aynı işi gören kodu yeniden yazdırdığı, bakımını kimsenin üstlenmediği bir yazılım yığını. Üstelik yapay zekâ, kural konmadığı yerde bu yığını el emeğinden çok daha hızlı büyütür. Oysa kamu kod envanteri, ortak kod deposu ve yapay zekâ destekli geliştirmenin denetim kuralları bu yasalara bugünden yazılırsa, aynı hız bu kez bizim lehimize işler. Fark, teknolojide değil, hazırlıkta olacaktır.

**Eskiyenler: geçen yasalar da yerinde durmuyor**

Eksikler kadar önemli bir başlık da elimizdeki yasaların bugünkü hali. Kişisel Verilerin Korunması Yasası'nı 2007'de çıkardığımızda bölgemizde öncülerdendik; bugün o metin, veri ihlali bildirimi, otomatik kararlara itiraz, çocuk verisi ve biyometrik veri gibi günümüzün gündelik meselelerine karşılık veremiyor. Kötü olduğu için değil, on dokuz yıldır kimse elini sürmediği için eskidi; kurumsal hafıza kaybının mevzuattaki karşılığı tam da budur. Elektronik İmza Yasası da benzer bir kaderi paylaşıyor: İmza yalnızca bir araçtır; asıl mesele güvenli dijital kimlik ve mühürden zaman damgasına bütün güven hizmetleridir. Bu genişleme yapılmadıkça geçen sayıda anlattığım katılım araçları da havada kalır; çünkü görüşü alınacak vatandaşın önce güvenle tanınması gerekir. Liste uzuyor: Elektronik Haberleşme Yasası, BTHK'yı asıl alanında, yani altyapıda tutacak şekilde; Bilişim Suçları Yasası, gerçek siber suç çekirdeğine dönecek şekilde; yayıncılık mevzuatı ise interneti değil yayıncılığı düzenlediği açıkça yazılacak şekilde elden geçirilmelidir. 2023 yasası da — yukarıda anlattığım gerekçelerle — henüz çok genç olmasına rağmen bu listeye girmek zorundadır; çünkü bir yasayı eskiten yalnızca zaman değil, doğduğu andaki mimari tercihleridir. Ve bir yasa daha var ki bu yazının konusuyla hüzünlü bir ironi oluşturuyor: Milli Arşiv mevzuatı. Kurumsal hafızayı kaybetmekten yakındığımız bir ülkede, devletin hafızasını düzenleyen yasanın da güncellenmeyi bekliyor olması, söylenebilecek her şeyi kendi başına söylüyor. Bu yasaların her birinde nelerin değişmesi gerektiğini ise ilerleyen sayılarda tek tek ele alacağım; bu yazının amacı madde yazmak değil, harita çıkarmaktır.

**Sınır çizmek, duvar örmek değildir**

Peki bütün bu yasalar tamamlansa iş biter mi? Bitmez. Çünkü asıl mesele, her yasanın kurumuna neyi yapma yetkisi verdiği kadar, neyi yapmayacağını da açıkça yazmasıdır. Yasalarımız görev sayar ama sınır çizmez; sınır çizilmeyince her kurum zamanla alanını genişletir ve adalar birbirinin kıyısına duvar örmeye başlar. Oysa model tersini söylüyordu: Teknik omurgayı işleten kurum koordine eder ama verinin sahibi gibi davranmaz. Kişisel veri otoritesi bağımsız denetçidir; gerektiğinde en büyük kamu projesini bile durdurabilmelidir. Haberleşme regülatörü altyapının kurumudur; içerik polisi değildir. Siber güvenlik merkezi teknik koordinatördür; kolluk değildir. Arşiv otoritesi belgenin standardını belirler. Yayın kurumu yayıncılığın kurumudur; internetin tamamının değil. Bu cümlelerin hiçbiri bir kurumu küçültmez; çünkü sınırı belli olan kurum, alanında derinleşebilen kurumdur. Birlikte çalışabilirlik de bu sınırların üzerine kurulur. Yarın bir dijital kimlik projesi başlatsak, en az beş kurumun birbirinin alanına girmeden aynı projede çalışması gerekir; geçen sayıda çalışma ahlakı dediğim şeyin mevzuata tercümesi işte budur. Bunun için her kurumun, kendi yasasına dokunduğu her an kendine tek bir soru sorması yeterlidir: Bu değişiklik bütünün hangi katmanına hizmet ediyor ve diğer kurumların görev alanıyla nasıl ilişkileniyor? Bu soru sorulmadan yapılan her tadilat, iyi niyetli bile olsa, adalara bir ada daha ekler.

**Envanter belli, sıra niyette**

Bu yazıda saydıklarım bir hayal listesi değil; bir zamanlar başlanmış, önceliklendirilmiş ve yarım bırakılmış bir işin kaldığı yerden dökümüdür. Yol devam etseydi bugün hangi yasanın eksik olduğunu değil, hangi hizmetin daha iyi çalıştığını konuşuyor olacaktık. Ama geçmişin şartlı cümleleri, ancak geleceğin planına dönüştüğünde bir işe yarar. Soru, geçen sayıda da yazdığım gibi, artık "kurulabilir mi" değil; niyet edilir mi sorusudur. Önümüzdeki sayılarda bu envanterin üzerine koymaya devam edeceğim; yasalarda nelerin değişmesi gerektiğini ve kaybettiğimiz modelin bugüne nasıl uyarlanabileceğini anlatacağım. Çünkü kaybettiğimiz şey bir belge değildi; bir çalışma ahlakı, bir birliktelik ve bir alışkanlıktı. Belgeler yeniden yazılabilir. Alışkanlık ise ancak niyet edilirse geri gelir.

***Eralp Curcioğlu***
*Elektrik ve Elektronik Mühendisi*
*EMI Technologies Ltd. Direktörü*

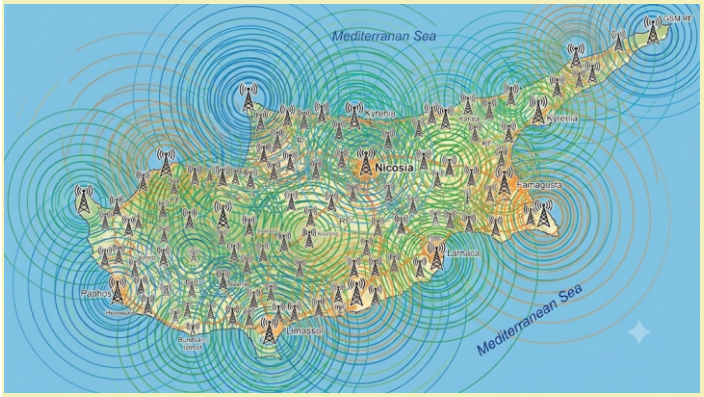
# Havadaki RF sinyalleri zararlı mı?

Havadaki radyo frekansı (RF) elektromanyetik alanlarının (EMA) insan sağlığı üzerindeki etkilerine dair hazırlanan yukarıdaki metne, akademik ve kurumsal düzeyde kabul gören **uluslararası profesyonel referanslar** aşağıda listelenmiştir.
Bu referanslar, elektromanyetik güvenlik standartlarını belirleyen, epidemiyolojik verileri analiz eden ve küresel sağlık politikalarını yöneten en üst düzey otoritelerden derlenmiştir.

**Uluslararası Kurumsal ve Akademik Referanslar**

1. **ICNIRP (International Commission on Non-Ionizing Radiation Protection)**
   - **Referans Döküman:** *Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz).* Health Physics, 118(5): 483–524, 2020.
   - **Önemi:** Dünya genelinde cep telefonları, baz istasyonları ve Wi-Fi cihazları için geçerli olan yasal SAR (Özgül Soğurma Oranı) ve güç yoğunluğu limitlerini belirleyen temel küresel kılavuzdur. 2020 güncellemesi, 5G teknolojilerini de kapsamaktadır.
2. **WHO (World Health Organization) - Dünya Sağlık Örgütü**
   - **Referans Döküman:** *Electromagnetic fields and public health: mobile phones (Fact Sheet No: 193).* WHO, 2014.
   - **Önemi:** DSÖ, bugüne kadar yapılmış binlerce bilimsel çalışmayı konsolide ederek, uluslararası sınır değerlerin altında kalan RF maruziyetinin insan sağlığı üzerinde kanıtlanmış herhangi bir olumsuz etkisi olmadığını resmi olarak deklare etmiştir.
3. **IARC (International Agency for Research on Cancer)**
   - **Referans Döküman:** *IARC Monographs on the Evaluation of Carcinogenic Risks to Humans, Volume 102: Non-Ionizing Radiation, Part 2: Radiofrequency Electromagnetic Fields.* Lyon, France, 2013.
   - **Önemi:** RF sinyallerini "Grup 2B" (İnsanlar için olası kanserojen) olarak sınıflandıran resmi monografttır. Metindeki "kanıtların yetersiz ancak dışlanamaz olduğu" tespiti bu epidemiyolojik rapora dayanmaktadır.
4. **SCENIHR (Avrupa Komisyonu Gelişmekte Olan ve Yeni Belirlenen Sağlık Riskleri Bilimsel Komitesi)**
   - **Referans Döküman:** *Potential health effects of exposure to electromagnetic fields (EMF).* European Commission, 2015.
   - **Önemi:** Avrupa Birliği adına hazırlanan bu kapsamlı bağımsız analitik raporda, cep telefonları ve kablosuz ağlardan (Wi-Fi) yayılan RF sinyallerinin, mevcut AB limitleri dahilinde kalındığı sürece ne kanser riskini ne de nörolojik hastalık riskini artırmadığı sonucuna varılmıştır.
5. **IEEE ICES (International Committee on Electromagnetic Safety)**
   - **Referans Döküman:** *IEEE Std C95.1-2019: IEEE Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz.* IEEE, 2019.
   - **Önemi:** Mühendislik perspektifinden elektromanyetik güvenliği tanımlayan, özellikle ABD standardizasyon enstitüleri (ANSI) tarafından referans alınan en temel küresel mühendislik standardıdır.
6. **COSMOS (Cohort Study on Mobile Phone Use and Health)**
   - **Referans Döküman:** *Schüz, J., et al. (2011 + güncel kohort takipleri). "The COSMOS Cohort Study: Mobile Phone Use and Health." Cancer Epidemiology, Biomarkers & Prevention.*
   - **Önemi:** Birleşik Krallık, İsveç, Finlandiya ve Hollanda dahil olmak üzere Avrupa genelinde yüz binlerce cep telefonu kullanıcısını uzun yıllar boyunca takip eden, RF maruziyeti konusundaki en büyük ve en prestijli prospektif epidemiyolojik çalışmalardan biridir.

**BT Kıbrıs**



# Siber Devriye Temelinde; Siber Vatan Mı, Dijital Gözetim Mi?

KKTC'de saldırı tespiti, zararlı alan adı bildirimi, tehdit istihbaratı paylaşımı, kamu sistemlerinin korunması ve izinli zafiyet taraması yapan savunma amaçlı bir Siber Devriye ya da Ulusal SOME/CSIRT modeli kurulabilir. Ancak Türkiye'den yönetilen, KKTC'deki bütün kullanıcıların internet trafiğini sürekli izleyen, içerik analiz eden, derin paket incelemesi (DPI) uygulayan veya izinsiz port taraması yapan bir sistemin mevcut KKTC mevzuatında açık ve yeterli bir hukuki dayanağı yoktur. Böyle bir yapı; haberleşmenin gizliliği, kişisel verilerin korunması, yargı kararı gerekliliği ve yetkisiz bilişim sistemi izleme hükümleriyle ciddi biçimde çatışabilir.
Bu yazı bağlayıcı bir hukuk mütalaası değil, kamuya açık mevzuat ve belgeler üzerinden yapılmış bir mevzuat ve kamu politikası analizidir.

**1. Türkiye'deki düzenlemeler neyi kapsıyor? 5651, 7253 ve 7418**

| Düzenleme | Temel konusu | Siber Devriye bakımından anlamı |
|---|---|---|
| **5651 sayılı Kanun** | İnternet yayınları, içerik–yer–erişim sağlayıcı yükümlülükleri, trafik bilgileri, erişimin engellenmesi ve içeriğin çıkarılması | Esasen internet aracılarının sorumluluğunu düzenler; genel ve sınırsız bir haberleşme dinleme kanunu değildir. |
| **7253 sayılı Kanun** | 2020'de 5651'i değiştirdi; sosyal ağ sağlayıcılarına Türkiye'de temsilci, başvurulara cevap, raporlama ve bazı veri yükümlülükleri getirdi; trafik bilgisine port bilgisini de ekledi | Platform ve sağlayıcı yönetişimini güçlendirdi. Kitlesel trafik dinleme veya yabancı ülkede tarama yetkisi vermez. |
| **7418 sayılı Kanun** | 2022'de Basın Kanunu, internet haber siteleri, sosyal ağ sağlayıcıları ve TCK'da değişiklik yaptı; "halkı yanıltıcı bilgiyi alenen yayma" suçunu getirdi | İçerik ve dezenformasyon düzenlemesidir. Teknik siber saldırı tespiti veya iletişim dinleme yetkisinin dayanağı olarak kullanılamaz. |
| **7545 sayılı Siber Güvenlik Kanunu** | 2025'te Türkiye'nin siber güvenlik teşkilatını, Siber Güvenlik Başkanlığını, kritik altyapıları ve olay müdahalesini düzenledi | "Siber Devriye" fikrine 5651'den daha yakın bir modeldir; fakat Türkiye makamlarına KKTC kullanıcıları üzerinde kendiliğinden yetki vermez. |

**nedir?**
5651 sayılı Kanun; internet yayınları ile içerik, yer ve erişim sağlayıcıların yükümlülüklerini, trafik bilgilerini, erişimin engellenmesini ve içeriğin çıkarılmasını düzenler. 7253 sayılı Kanun, 2020'de 5651'i değiştirerek sosyal ağ sağlayıcılarına temsilci, başvurulara cevap, raporlama ve bazı veri yükümlülükleri getirmiş; trafik bilgisi tanımına port bilgisini de eklemiştir. 7418 sayılı Kanun ise 2022'de basın, internet haber siteleri, sosyal ağlar ve "halkı yanıltıcı bilgiyi alenen yayma" suçu üzerinde yoğunlaşmıştır. Bu düzenlemelerin hiçbiri genel, sınırsız ve sınır ötesi haberleşme dinleme ya da yabancı bir ülkedeki sistemleri tarama yetkisi vermez.

Siber Devriye fikrine daha yakın karşılaştırma, Türkiye'nin 2025 tarihli 7545 sayılı Siber Güvenlik Kanunu'dur. Bu yasa ulusal siber güvenlik politikası, kritik altyapılar, olay müdahalesi ve Siber Güvenlik Başkanlığını düzenler; istihbarat ve adli kolluk faaliyetlerini ise ilgili özel mevzuata bırakır. Dolayısıyla "siber güvenlik" kavramı tek başına haberleşmeyi dinleme yetkisi anlamına gelmez. Ayrıca güncel değerlendirme, kanunların ilk yayımlanan metinlerinden değil, Anayasa Mahkemesi kararları sonrasındaki yürürlükteki birleştirilmiş hâllerinden yapılmalıdır.

**2. KKTC'de mevcut hukuki çerçeve**
**Anayasa ve özel hayatın korunması**

KKTC Anayasası'nda özel hayat ile haberleşmenin gizliliği temel haklardır. Haberleşme içeriğinin öğrenilmesi veya iletişimin izlenmesi, sıradan bir idari karar ya da bakanlık protokolüyle sınırsız biçimde yapılamaz; müdahalenin kanunla öngörülmesi, belirli ve ölçülü olması ve yargısal denetime tabi tutulması gerekir. 32/2014 Özel Hayatın ve Hayatın Gizli Alanının Korunması Yasası, ilgililerin rızası olmadan haberleşmenin öğrenilmesini veya kaydedilmesini ve kişisel verilerin hukuka aykırı elde edilmesi ya da aktarılmasını cezai sorumluluk konusu yapar.

**Kişisel veriler ve elektronik haberleşme**
89/2007 Kişisel Verileri Koruma Yasası uyarınca veri işleme; rıza, yasal yükümlülük, kamu görevi, sözleşme veya başka bir kanuni işleme şartına dayanmalıdır. KKTC'den başka bir ülkeye kişisel veri aktarımı bakımından Kişisel Verileri Koruma Kurulunun aktarım izni sistemi vardır. Kamu yararı veya kurumlar arası iş birliği, sürekli ve sınırsız trafik aktarımını kendiliğinden hukuka uygun hâle getirmez; IP, port, zaman damgası, DNS sorgusu, cihaz bilgisi ve içerik gibi veri türleri amaç ve gereklilik bakımından ayrı ayrı değerlendirilmelidir.

6/2012 Elektronik Haberleşme Yasası şebeke ve hizmet güvenliğini düzenlerken haberleşmenin kullanıcılar dışındaki kişilerce dinlenmesini, kaydedilmesini veya engellenmesini kural olarak yasaklar. Trafik verileri hizmetin tamamlanmasından sonra silinmeli veya anonimleştirilmeli; faturalandırma, hizmet sunumu ya da açık rıza gibi sınırlı amaçlarla tutulmalıdır. BTHK güvenlik, gizlilik ve veri ihlallerini denetleyebilir; ancak düzenleyici rolü onu ceza soruşturması veya istihbarat dinleme makamına dönüştürmez.

**Bilişim suçları ve kamu sistemlerinin güvenliği**
32/2020 Bilişim Suçları Yasası; bilişim sistemine yetkisiz erişmeyi, erişmeye teşebbüs etmeyi, buna yardım etmeyi ve kamuya açık olmayan verileri teknik yöntemlerle yetkisiz biçimde izlemeyi suç kapsamına alabilir. Bilgisayar veya veri araması, şifre çözme ve adli kopya alma gibi işlemler kural olarak mahkeme kararına bağlıdır. İnternet hizmet sağlayıcılarına bütün içerikleri sürekli izleme yükümlülüğü verilmemiş; trafik verilerinin iki yıl KKTC'deki sunucularda saklanması ve erişimin mahkeme kararı, açık yasal görev veya hizmet zorunluluğu gibi şartlara bağlanması öngörülmüştür.

76/2023 KKTC Başbakanlık Dijital Dönüşüm ve Elektronik Devlet Kurumu Yasası altında Bilgi Güvenliği, Ağ Yönetimi ve Siber Güvenlik Merkezi kurulabilir; kamu kurumları için standart belirleme, zafiyet araştırma, saldırı tespiti ve olay müdahalesi yapılabilir. Ancak bu yetki esas olarak kamu sistemlerine yöneliktir ve bütün toplumun internet trafiğini sürekli izleme

yetkisi şeklinde genişletilemez.

**3. KKTC–Türkiye iş birliği ve USOM meselesi**

BTHK'nın 2025 faaliyet raporuna göre KKTC'deki siber tehditler Türkiye BTK bünyesindeki USOM tarafından analiz edilmekte, Ağustos 2021'den beri zafiyet bildirimleri yapılmakta ve 2025 yılında 129 tespit BTHK'ya iletilmektedir. Bu durum belirli bir tehdit istihbaratı ve zafiyet bildirim modelinin zaten bulunduğunu gösterir. Ancak kamuya açık rapor, USOM'un bütün KKTC kullanıcılarının ham paketlerini topladığı veya haberleşme içeriklerini dinlediği anlamına gelmez. Tehdit göstergesi analizi ile ülke çapında tam trafik gözetimi hukuken ve teknik olarak farklı işlemlerdir.

Ulaştırma Bakanı Erhan Arıklı'nın 1 Ağustos 2026 tarihli açıklamasında Siber Devriye'nin dolandırıcılık, kimlik hırsızlığı, zararlı yazılım, çocuk istismarı, yasa dışı bahis, terör ve organize suçlarla mücadele amacı taşıdığı ve gerekli yasal-teknik altyapıdan sonra kurulmasının düşünüldüğü belirtilmiştir. Kamuya açık alanda henüz ayrıntılı yasa tasarısı, teknik mimari, veri koruma etki analizi veya sınır aşan veri protokolü bulunmadığından proje şimdilik politika niyeti düzeyindedir.

**4. Mevcut yasalarla kurulabilecek ve kurulamayacak model**

Mevcut hukukla; kamuya açık kaynaklarda sahte site ve zararlı alan adı araştırması, zararlı IP/alan adı/dosya özeti paylaşımı, DDoS ve botnet olaylarında koordinasyon, yazılı izinli sistemlerde zafiyet taraması, vatandaş ihbar merkezi, kamu kurumları için 7/24 SOC/SOME-CSIRT, delil koruma taleplerinin polis-savcılık-mahkeme kanalıyla yürütülmesi ve hizmet sağlayıcılara güvenlik/olay bildirim yükümlülüğü getirilmesi mümkündür. Burada amaç kullanıcı içeriğini okumak değil, saldırı göstergelerini ve teknik kötüye kullanım belirtilerini tespit etmektir.

Buna karşılık bütün KKTC trafiğinin ham kopyasının Türkiye'ye aktarılması, mahkeme kararı olmadan içerik dinlenmesi, ülke çapında sürekli DPI, şifreli trafiğe araya girme, vatandaşlar için DNS-IP-SNI-sosyal medya profili oluşturulması, Türkiye'deki bir kurumun bağımsız hedef seçmesi, gerçek zamanlı kişi/cihaz takibi, habersiz aktif zafiyet veya exploit taraması ve siyasi eleştirinin "siber güvenlik" faaliyeti olarak izlenmesi mevcut hukukta açıkça mümkün değildir veya son derece yüksek hukuki risk taşır.

**5. Hangi yeni düzenlemeler gerekiyor?**

Öncelikle bir Siber Güvenlik ve Kritik Altyapılar Yasası çıkarılarak ulusal SOME/CSIRT'nin statüsü, kritik altyapı sektörleri, zorunlu olay bildirimi, asgari güvenlik standartları, izinli taramanın koşulları, acil durum yetkileri ve bağımsız denetim açıkça düzenlenmelidir. İkinci olarak Haberleşmenin Adli Amaçla Denetlenmesi Yasası; hangi ağır suçlarda, hangi makamın başvurusu ve hangi mahkemenin kararıyla izleme yapılabileceğini; hedef, süre, uzatma, içerik-trafik ayrımı, mesleki sırların korunması, silme, bildirim, tazminat ve şeffaflık güvenceleriyle belirlemelidir.

KKTC–Türkiye iş birliği sıradan bir kurumlar arası mutabakatla değil, Meclis onaylı bir protokol veya yasayla kurulmalıdır. Aktarılabilecek veri türleri, ham trafik yasağı veya istisnası, KKTC makamının veri sorumlusu ve karar verici olarak kalması, Türkiye'deki kurumun yalnızca teknik hizmet sağlayıcı rolü, saklama süresi, erişim kayıtları, veri ihlali, imha, delil zinciri, uygulanacak hukuk ve KVK Kurulu denetimi açıkça yazılmalıdır.

Ayrıca 32/2020 Yasasında pasif tehdit istihbaratı, port taraması, banner/sürüm tespiti, zafiyet doğrulaması, exploit, yetkisiz erişim teşebbüsü, trafik toplama ve içerik yakalama birbirinden ayrılmalıdır. 89/2007 Yasası ise veri koruma etki değerlendirmesi, tasarımdan itibaren mahremiyet, ihlal bildirimi, profil çıkarma, kolluk verileri, biyometrik ve trafik verileri, yurt dışı aktarım denetimi, Kurul bağımsızlığı ve etkili yaptırımlar bakımından güncellenmelidir.

**6. Türk Telekom geçidi ve iki hukuk düzeni**

KKTC'nin uluslararası internet erişiminin Türk Telekom POP'u ve Türkiye'ye uzanan fiber bağlantılar üzerinden sağlanması, işletmeciye trafiği sınırsız inceleme yetkisi vermez. Yönlendirme, kapasite ölçümü ve saldırı göstergesi/DDoS tespiti; uygun sözleşme, veri minimizasyonu ve denetimle hizmet güvenliği kapsamında kalabilir. Abone bazlı profil, tam paket kaydı, içerik dinleme ve şifre çözme ise açık kanun, belirli amaç, yargı kararı ve bağımsız denetim gerektirir.

Türkiye'deki kanunlar bir Türk kamu kurumuna KKTC'deki kişiler üzerinde kendiliğinden yetki sağlamaz. Türkiye tarafından işletilen bir gözetim sistemi, KKTC iç hukukunun yanı sıra uluslararası insan hakları sorumluluğu, yurt dışı veri aktarımı ve delillerin geçerliliği sorunlarını da doğurabilir. Türkiye'de toplanan verinin KKTC mahkemelerinde kullanılabilmesi için toplama yetkisi, zaman senkronizasyonu, hash, erişim kayıtları, personel yetkisi ve delil zinciri doğrulanmalıdır. Aksi hâlde hukuka aykırılık ve bütünlük itirazları gündeme gelebilir.

7. Port taraması neden özel olarak düzenlenmeli?

Portun açık olup olmadığını kontrol etmek, servis başlığı ve sürümü almak, zafiyet eklentisi çalıştırmak, kimlik doğrulamayı aşmaya çalışmak ve exploit göndererek zafiyeti doğrulamak aynı ağırlıkta değildir. 32/2020 Yasası erişim teşebbüsünü ve teknik yöntemle yetkisiz izlemeyi kapsadığından, sistem sahibinin rızası veya açık kanuni yetki olmadan kapsamlı tarama risklidir. Hukuka uygun ulusal taramada yetkilendirilmiş hedef listesi, yazılı rıza veya açık yetki, ilan edilmiş kaynak IP'leri, irtibat adresi, hız sınırı, kimlik doğrulamayı aşmama, exploit için özel izin, veri minimizasyonu, otomatik durdurma, değiştirilemez kayıt ve bağımsız denetim bulunmalıdır.

Nihai değerlendirme

Siber Devriye bütünüyle hayal değildir. Mevcut mevzuat; kamu sistemlerinin korunması, SOME/CSIRT kurulması, tehdit istihbaratı, zararlı alan adı tespiti, olay bildirimi ve izinli güvenlik taraması için başlangıç zemini sunar. Ancak "KKTC'nin bütün internet trafiğinin Türkiye'ye aktarılması, kullanıcıların sürekli izlenmesi, istenilen IP'lerin taranması ve gerektiğinde içeriğin okunması" şeklindeki bir model hukuken kırılgan, anayasal olarak tartışmalı, veri koruma bakımından riskli ve uluslararası insan hakları sorumluluğu doğurabilecek niteliktedir.

Doğru model; KKTC'de yerleşik, KKTC hukukuna tabi, yargısal ve bağımsız denetimli, ham veriyi yerelde tutan ve

Türkiye'den yalnızca sınırlı teknik destek ile tehdit istihbaratı alan savunma amaçlı bir ulusal siber güvenlik merkezi olmalıdır. Sensörler ve ayrıntılı kayıtlar KKTC'de kalmalı; BTHK haberleşme işletmecilerini, KKTC Başbakanlık Dijital Dönüşüm ve Elektronik Devlet Kurumu kamu SOC/SOME faaliyetini, polis ve savcılık suç soruşturmasını, KVK Kurulu veri işleme ve aktarımı, mahkemeler ise hedefli gözetimi denetlemelidir. Türkiye'ye kural olarak yalnızca zararlı IP ve alan adları, dosya hash'leri, anonimleştirilmiş göstergeler, toplulaştırılmış akışlar ve belirli olaylarda mahkeme kararıyla yetkilendirilmiş veriler aktarılmalıdır.

Son olarak cevaplanması gereken kritik soru şudur: KKTC ve Türkiye hukukunda port taraması, zafiyet doğrulaması veya erişim teşebbüsü suç riski taşıyabiliyorsa, USOM'un KKTC'ye bildirdiği tespitler hangi teknik yöntemle, hangi hedef yetkisiyle ve hangi sözleşme ya da kanuni dayanakla üretilmektedir? Kamuya açık belgeler bu ayrıntıyı göstermemektedir. Eğer işlem yalnızca pasif tehdit istihbaratı ve kamuya açık verilerin analizi ise durum farklıdır; buna karşılık açık rıza, yazılı yetki veya kanuni görev olmadan aktif tarama ve zafiyet doğrulaması yapılıyorsa suç ve hukuka aykırılık tartışması doğabilir. Bu nedenle yöntem, yetki zinciri, hedef listesi ve denetim mekanizması şeffaf biçimde açıklanmalıdır.

**Kazım Ateş**
Elektronik ve Bilişim Uzmanı

# Avustralya'nın sosyal medya yasağı işe yaramadı: Çocukların %80'i hala platformlarda

Avustralya'nın 16 yaş altına yönelik sosyal medya yasağının yürürlüğe girmesinden üç ay sonra yayımlanan ilk resmi değerlendirme raporu, uygulamanın beklenen etkiyi yaratmadığını ortaya koydu. Ülkenin çevrim içi güvenlik kurumu eSafety Commissioner tarafından hazırlanan rapora göre, çocukların %80'den fazlası Instagram, TikTok ve Snapchat gibi yaş sınırı bulunan platformları kullanmayı sürdürüyor.

803 çocuk (10-15 yaş) ve ebeveynleriyle gerçekleştirilen araştırma, yasağın Aralık 2025'te yürürlüğe girmesinden önceki veriler ile Mart-Nisan 2026 döneminde toplanan üç aylık takip verilerini karşılaştırdı.

Rapora göre yaş sınırı bulunan platformlarda hesabı olan çocukların oranı yaklaşık %52'den %42'ye gerilese de sosyal medya kullanımındaki düşüş oldukça sınırlı kaldı. Yasa öncesinde çocukların %85,9'u en az bir sosyal medya platformunu kullanırken, bu oran üç ay sonra yalnızca %81,5'e düştü.

## Yaş doğrulama sistemleri yetersiz kaldı

Raporda, sınırlı etkinin temel nedeni olarak sosyal medya şirketlerinin yaş doğrulama sistemlerini etkili şekilde uygulamaması gösterildi. Ankete katılan çocukların yarısından fazlası platformların yaşlarını doğrulamak için herhangi bir işlem yapmadığını söyledi.

Bunun yanında çocukların %18'i platformların yaşlarını yanlışlıkla 16 yaşın üzerinde değerlendirdiğini, %37'si ise erişimini sürdürebilmek için hesaplarında yaşını 16 veya üzeri olarak belirttiğini ifade etti. Rapor, çocukların hesaplarına erişmeye devam etmek için karmaşık yöntemlere ihtiyaç duymadığını, mevcut doğrulama sistemlerinin kolayca aşılabildiğini vurguladı.
Reddit ve Pinterest'e yöneliş dikkat çekti

Araştırma, bazı çocukların Instagram ve TikTok gibi platformlardan uzaklaşırken Reddit ve Pinterest gibi alternatif platformlara yönelmeye başladığına dair ilk işaretleri de ortaya koydu.

Bunun yanında yasağın beklenmeyen bir sonucu da tespit edildi. Çocuklarının sosyal medya kullandığını bilmeyen ebeveynlerin oranı yaklaşık %10 arttı. Uzmanlar bunun çocukların hesaplarını ailelerinden daha gizli kullanmaya başlamış olabileceğine işaret ettiğini belirtiyor.

Öte yandan Başbakan Anthony Albanese'nin yasağın çocukların dışarıda daha fazla vakit geçirmesini sağlayacağı yönündeki beklentisi de gerçekleşmedi. Rapor, çocukların çevrim dışı aktivitelerinde kayda değer bir değişim yaşanmadığını ortaya koydu.

## Hükümet yaptırımları artırmaya hazırlanıyor

Sonuçların ardından Avustralya hükümetinin sosyal medya şirketlerine yönelik yaptırımları sertleştirmesi bekleniyor. Hükümet, platformlara uygulanabilecek para cezalarını artırmayı ve eSafety Commissioner'ın bilgi toplama yetkilerini genişletmeyi planlıyor.

Öte yandan yaş doğrulama teknolojileri geliştiren şirketler de hükümete, sosyal medya platformlarının yaş doğrulama sistemlerini gerçekten uygulayıp uygulamadığını denetlemek amacıyla bağımsız ve zorunlu denetimler yapılması çağrısında bulundu.

Uzmanlara göre platformlar kurallara tam olarak uysa bile sorun tamamen çözülmeyebilir. Çünkü mevcut yasa, çocukların hesap açmasını engellese de sosyal medya içeriklerini oturum açmadan görüntülemelerini yasaklamıyor. - *Kaynak: donanimhaber.com*

Ağustos 2026
btkibris.org


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

BTKıbrıs



**Sayı 5**