



Elektrik Mühendisleri Odası
İstanbul Şubesi

EYLÜL 2026

BÜLTEN

SAYI 85



İÇİNDEKİLER

Başyazı	4
Halkın Faturası ve Enerjide Özelleştirme Kışkacı: Devlet Desteği Nereye Gidiyor? - Enerji Komisyonu	5
Teknik Emeğin Sınıfsal Yeniden Konumlanması ve Geleceği - Mehmet Yeşiltepe	8
Küresel Enerji Denkleminde Mühendislik: Ağırlaşan Tüketim Yükü ve Yeni Elektrik/Yangın Standartları - Murat Erbaş	16
Elektrik Enerjisinde Dijital Dönüşüm - Emre Akçin	20
EEMKON 2027 Hazırlık Çalışmaları ve Katılım Çağrısı	25
Ücretli Çalışan ve İşsiz Mühendisler Komisyonu	27
Kurumsal Yapay Zeka Dönüşümünde Adreslenmesi Gereken 6 Alan - Sinan Kezer	29
Yapay Zeka Güvenliği ve Yapay Zekanın Oluşturduğu Riskler - Orhan Mordoğan	32
Komisyonlar: Mühendislikte Kamu Yararı ve Mesleki Sorumluluk	42
Şubeden Teknik ve Mesleki Gündem	44

KÜNYE

Sayı: 85 / Eylül 2026

**Elektrik Mühendisleri
Odası İstanbul Şubesi
Adına Sahibi**
ERHAN KARAÇAY

**Sorumlu Yazı İşleri
Müdürü**
REHA ŞEN

Yayın Kurulu
ERHAN KARAÇAY
ERHAN GÜROL MUTAF
REHA ŞEN
NEDİM BİNGÖL
MURAT GÜNDÜZAY
HASAN AKSU
CİVAN ATEŞ
MEHMET VEYSİ ÇEVİRİM
SİBEL TETİK
CENK GÖÇER
TÜLİN OKAY
ONUR DOĞAN

Hazırlayan
MURATHAN DEMİRCİOĞLU

Yayın Türü
DİJİTAL DERGI / SÜRELİ YAYIN

Yayın Tarihi
EYLÜL 2026

**Türk Mühendis ve Mimar
Odaları Birliği (TMMOB)
Elektrik Mühendisleri Odası
(EMO) İstanbul Şubesi Bülteni**

Yönetim Yeri: EMO İstanbul
Şubesi **Adres:** Ergenekon Mah.
Cumhuriyet Cad. Adli Han No:
173/1 34373 Harbiye Şişli/İstanbul
Tel: (0212) 259 11 50
Faks: (0212) 258 36 55
İnternet Sitesi:
<http://istanbul.emo.org.tr>
E-posta: istanbul@emo.org.tr

Bu bülten EMO İstanbul Şubesi
tarafından üyelerine ulaştırılmak
üzere hazırlanmıştır.

Değerli Okurlarımız,

EMO İstanbul Şubesi Bülteni'nin Eylül 2026 sayısı ile karşınızdayız. Şubemizin 45. Dönem Yönetim Kurulu ve çalışma birimleriyle yürüttüğümüz faaliyetleri, mesleğimizin güncel sorunlarını ve mühendislik alanındaki gelişmeleri sizlerle paylaşmayı sürdürüyoruz.

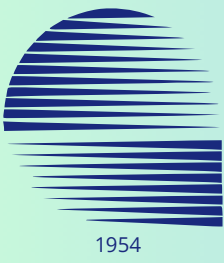
Bu sayımızda, şube etkinliklerimize ilişkin bilgilerin yanı sıra enerji politikalarından teknik emeğin dönüşümüne, elektrik güvenliğinden dijitalleşmeye uzanan başlıklara yer veriyoruz. Bilimsel ve teknik gelişmeleri, mesleki sorumluluklarımız ve toplum yararı çerçevesinde birlikte değerlendirmeyi önemsiyoruz.

Mesleki bilgi ve deneyimlerimizi paylaşmanın, ortak sorunlarımızı tartışmanın ve çözüm üretmenin örgütlü dayanışmamızı güçlendireceğine inanıyoruz. Bültenimize yazılarıyla katkıda bulunan meslektaşlarımıza ve hazırlanmasında emeği geçen herkese teşekkür ediyor; sizleri de görüş, öneri ve çalışmalarınızla gelecek sayılarımıza katkı sunmaya davet ediyoruz.

İyi okumalar diliyoruz.

Saygılarımızla,

Yayın Kurulu



BAŞYAZI

EMO İSTANBUL ŞUBESİ

45. DÖNEM YÖNETİM KURULU

Sevgili Meslektaşlarımız,

EMO İstanbul Şubesi 45. Dönem çalışmalarımızı, üyeleri adına değil, üyelerle birlikte karar alan, kolektif, katılımcı ve şeffaf bir yönetim anlayışı ile sürdürmeyi hedefliyoruz.

Mesleki, ekonomik ve demokratik haklarımızı savunurken, kamu yararı, bilimsel yaklaşım ve meslek etiği ilkelerimize de sahip çıkacağız.

Yeni mezun, işsiz, kamu, ücretli, serbest çalışan ve emekli tüm meslektaşlarımızın çözüm bekleyen sorunlarına sahip çıkarak; EMO-TMMOB birlikteliği ile çözüm bulmaya çalışacağız.

Bilimin ve teknolojinin insanlığın ortak geleceğine hizmet etmesini savunurken barıştan, eşitlikten, özgürlükten ve demokrasiden yana tutumumuzu koruyacağız.

Savaşlara, işgallere, soykırıma ve sivilleri hedef alan saldırılara karşı çıkıyoruz; Filistin halkıyla dayanışmamızı yineliyoruz. Bütün halkların güven içinde, özgürce yaşayabildiği bir dünya ile ülkemizde laik, demokratik ve adil bir yaşam talebimizi mesleğimizin toplumsal sorumluluğunun ayrılmaz bir parçası olarak görüyoruz.

Bu sayımızda ele aldığımız enerji politikaları, kamusal kaynakların kullanımı ve teknik emeğin geleceği, meslek alanımızın toplumsal yaşamla doğrudan kurduğu bağ ortaya çıkardığı düşüncesindeyiz. Elektriğe güvenli ve kesintisiz biçimde, insan hakkı olarak erişimi temel bir hak olarak savunuyoruz.

Enerjide özelleştirme uygulamalarının sonuçlarını, halkın faturalarına yansıyan yükleri ve devlet desteklerinin nasıl kullanıldığını bu anlayışla sorguluyoruz. Kamu kaynaklarının kullanımında şeffaflığın, hesap verebilirliğin ve toplum yararının esas alınmasını talep ediyoruz.

Enerji ihtiyacının karşılanması, altyapının planlanması ve elektrik tesislerinin güvenliği, mühendislik hizmetlerinin niteliğiyle doğrudan ilişkili olduğuna inanıyoruz. Elektrik ve yangın güvenliğine ilişkin standartların uygulanmasını, etkin denetimi ve mesleki yetkinliği can ve mal güvenliğinin temel unsurları olarak değerlendiriyoruz. Güvenli yapıların, iş yerlerinin ve kentlerin oluşturulması için mühendislik hizmetlerinin planlamadan işletmeye kadar her

aşamada hak ettiği değeri alması gerektiğini vurguluyoruz.

Teknik emeğin dönüşümü de öncelikli gündemlerimiz arasında yer almaktadır. Ücretli çalışan mühendislerin çalışma koşulları, ücretleri, özlük hakları, mesleki formasyonlarının yükseltilmesi için, işsizlik ve güvencesizlik kaygısı yaşamadan mesleklerini sürdürebildiği koşulların oluşturulması için örgütlü dayanışmayı yaygınlaştıracaktır.

Elektrik enerjisinde dijital dönüşümü de bu toplumsal ve mesleki sorumluluk çerçevesinde ele almaktayız. Yeni teknolojilerin güvenli, denetlenebilir ve kamu yararını gözeten biçimde kullanılmasını; meslektaşlarımızın bilgi ve becerilerinin geliştirilmesini ve bu dönüşümde söz sahibi olma olanaklarının artırılmasını savunuyoruz.

Bu sayımızda yer verdiğimiz EEMKON 2027 başlığı, meslek alanlarımızdaki gelişmeleri ortak bir tartışma zemini içinde değerlendirmek açısından önem taşıdığına inanıyoruz. Bilimsel bilgi ile mesleki deneyimi buluşturan, mühendisliğin toplumsal sorumluluğunu görünür kılan buluşmaları üyelerimizin katkılarıyla güçlendirmeyi hedefliyoruz.

Şube çalışmalarımızda üyelerimizin katılımını ve ortak üretimi esas alıyoruz. Komisyonlarımızı ve çalışma gruplarımızı güçlendirmek, mesleki eğitim ve paylaşım olanaklarını geliştirmek, üniversitelerden kamu kurumlarına ve sektör kuruluşlarına uzanan ilişkilerimizi toplum yararına çalışmalarla ilerletmek önceliklerimiz arasındadır. Tüm üyelerimizi bilgi, deneyim ve önerileriyle şube çalışmalarına katılmaya davet ediyoruz.

Bültenimizin hazırlanmasında emeği geçen Yayın Kurulu'na, yazılarıyla katkı sunan meslektaşlarımıza, şube çalışmalarını birlikte yürüttüğümüz tüm üyelerimize ve çalışanlarımıza teşekkür ediyoruz.

Daha güçlü bir Oda ve daha güçlü bir Şube için dayanışmayla çalışmayı sürdüreceğiz.

Saygılarımızla,

EMO İstanbul Şubesi
45. Dönem Yönetim Kurulu adına
Erhan KARAÇAY

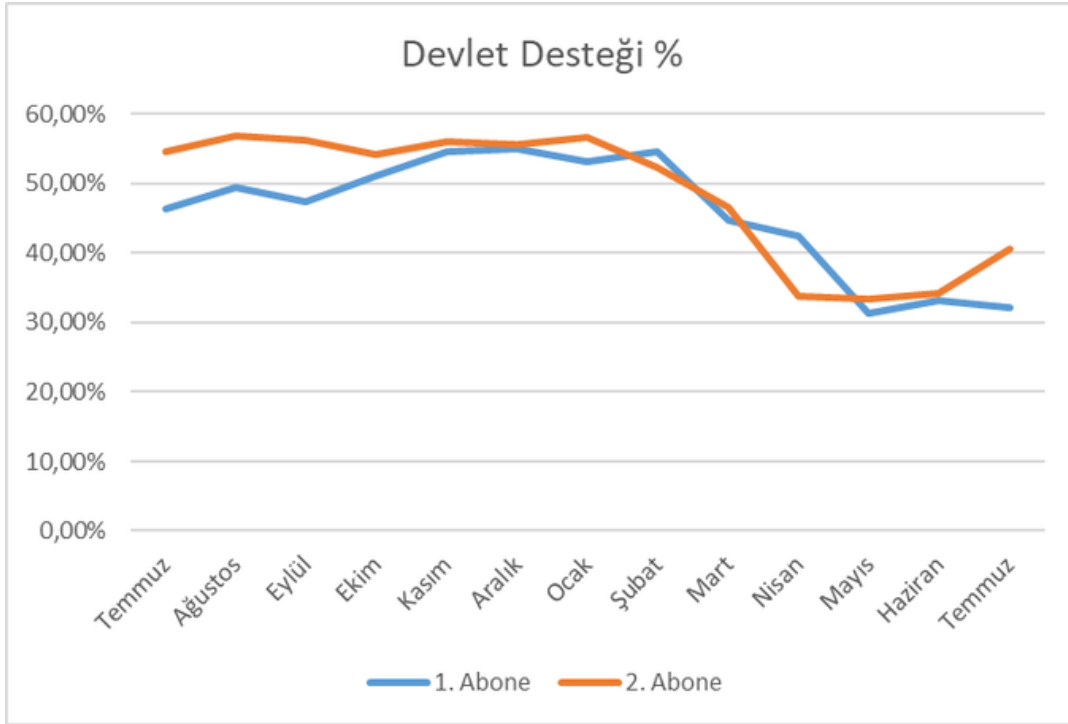
HALKIN FATURASI VE ENERJİDE ÖZELLEŞTİRME KISKACI: DEVLET DESTEĞİ NEREYE GİDİYOR?

1. Giriş: Enerji Bir Hak mı, Ticari Bir Mal mı?

Enerji, modern yaşamın sürdürülebilmesi için hava ve su kadar hayati, devredilemez ve temel bir insan hakkıdır. Ancak Türkiye’de mevcut enerji yönetimi, bu kamusal hakkı korumak yerine enerjiyi kar hırsının hüküm sürdüğü piyasa dinamiklerine ve insafsız bir "serbest piyasa" kurgusuna terk etmiştir. Elektrik Mühendisleri Odası (EMO) İstanbul Şubesi olarak, teknik uzmanlığımızı toplumcu bir bakış açısıyla harmanlayarak bir kez daha hatırlatıyoruz: Enerji bir ticari meta değil, kamusal bir hizmettir.

Bugün "devlet desteği" adı altında sunulan sübvansiyonlar, aslında özelleştirme sonrası iflas eden sistemin sürdürülemez maliyetlerini ve sermayeye yapılan gizli kaynak aktarımını maskeleyen çabasıdır. Stratejik veriler, bu desteğin bir lütuf gibi sunulmasına rağmen sistematik olarak geri çekildiğini ve hane halkı bütçesinin kurgulanmış bir piyasanın volatilitesine kasten maruz bırakıldığını göstermektedir. Faturadaki rakamlar sadece birer sayı değildir; halkın cebinden doğrudan enerji baronlarının kasasına yapılan sistematik bir sermaye transferinin belgesidir.

2. Veriler Konuşuyor: Devlet Desteğindeki Büyük Erime



Enerji yönetimindeki "piyasacı" dönüşüm, veriler analiz edildiğinde kamusal desteğin nasıl bir erozyona uğradığını net bir şekilde ortaya koymaktadır. Özellikle 2025 yılının ortasından 2026 Temmuz’una kadar geçen süreç, halkın sırtındaki yükün planlı bir şekilde artırıldığını kanıtlamaktadır.

Aşağıdaki tablo, farklı abone grupları bazında devletin maliyeti üstlenme oranındaki dramatik düşüşü sergilemektedir:

Dönem	1. Abone Grubu (Devlet Katkısı %)	2. Abone Grubu (Devlet Katkısı %)
Tem 2025	%46,27	%54,53
Oca 2026	%53,21	%56,63
Tem 2026	%32,14	%40,55

Olan Ne? Verilerin derinlemesine analizi, durumun sadece bir "düşüş" değil, bilinçli bir terk ediş olduğunu göstermektedir. Konut tüketimini temsil eden 1. Abone grubu için 2025 Temmuz'da %46,27 olan destek, **2026 Mayıs ayında %31,26 ile "uçurumun dibini" görmüştür.**

Asıl çarpıcı yıkım ise 2. Abone grubunda yaşanmıştır. 2026 yılının başında Ocak ayında %56,63 olan devlet desteği, sadece dört ay içerisinde, Mayıs 2026'da %33,36'ya gerilemiştir. **Sadece dört ayda yaşanan bu 23,27 puanlık devasa geri çekilme,** tüketicinin piyasa spekülasyonları karşısında nasıl savunmasız bırakıldığının vesikasıdır. Devlet, maliyet kontrolü ve kamusal denetim görevini bırakmış, faturanın yükünü doğrudan vatandaşın omzuna yıkmıştır.

3. Piyasa Oyunu: PTF ve YEKDEM Kıskaçında Tüketici

Elektrik maliyet yapısını belirleyen PTF (Piyasa Takas Fiyatı) ve YEKDEM (Yenilenebilir Enerji Kaynakları Destekleme Mekanizması) kavramları, halkın anlayacağı dille bir "teknik soygun" düzeneğine dönüşmüştür. PTF'yi elektriğin o anki "borsa fiyatı", YEKDEM'i ise enerji şirketlerine verilen "dolar bazlı fahiş alım garantisi" olarak okumak mümkündür.

İbretlik Veri: Piyasa Ucuzlarken Fatura Neden Düşmüyor? 2026 yılının Mayıs ve Haziran verileri, sistemin "smoking gun" (suçüstü) kanıtıdır:

- ◆ **Mayıs-Haziran 2026 Dönemi:** PTF (borsa fiyatı) 921,06 birimden 590,90 birime hızla düşerken; şirketlere ödenen YEKDEM garantisi 1.038,34 birimden 1.306,10 birime fırlatılmıştır.
- ◆ **Paradoksun Deşifresi:** Temmuz 2025'te toplam elektrik maliyeti (PTF+YEKDEM) 2.859,44 birim iken, Haziran 2026'da bu maliyet 1.897,00 birime gerilemiştir.

Piyasa maliyeti yaklaşık 1000 birim düşmesine rağmen, devlet aynı dönemde destek oranlarını en düşük seviyeye çekerek (1. Abone için %33 bandı), bu maliyet düşüşünün vatandaşa yansıtılmasını engellemiştir.

YEKDEM mekanizması, yoksuldan alıp yenilenebilir enerji baronlarına veren bir "taban fiyat" işlevi görerek faturaların düşmesini engellemektedir. Bu, piyasa fiyatları düşse dahi halkın cebinden sermayeye kesintisiz kaynak aktarılmasını sağlayan kurgulanmış bir mekanizmadır.

4. Özelleştirmenin Bedeli: Kimin İçin Devlet, Kimin İçin Destek?

Türkiye enerji sektörü, "verimlilik ve ucuzluk" masallarıyla sermayeye peşkeş çekilmiştir. Ancak bugünkü tablo, özelleştirmenin sadece fatura kabusu ve arz güvenliği riski anlamına geldiğini somutlaştırmıştır.

Devletin faturanın bir kısmını ödüyor gibi görünmesi, aslında özelleştirilmiş sistemin yapısal krizini halktan gizleme çabasıdır. YEKDEM üzerinden özel şirketlere aktarılan milyarlarca lira halkın sırtına yüklenmekte, destekler azaldığında ise vatandaş doğrudan piyasanın insafına terk edilmektedir. "Özelleştirme pişmanlıktır" gerçeği, her ay gelen kabarık faturalarda ve eriyen destek oranlarında vücut bulmaktadır. Kamu kaynakları, halkın refahı yerine enerji tekellerinin karlılığını güvence altına almak için harcanmaktadır.

5. Sonuç ve Çözüm: Enerji Kamulaştırılmalıdır

TMMOB Elektrik Mühendisleri Odası İstanbul Şubesi olarak, bu piyasa dayatmasına ve teknik kılıflarla gizlenen soyguna karşı çözüm önerilerimizi net bir şekilde sunuyoruz:

- 1. Tazminatsız Kamulaştırma:** Enerji bir kâr alanı değil, kamu hizmetidir. Üretim, iletim ve dağıtım zinciri acilen ve tazminatsız olarak kamulaştırılmalı, kamusal denetim yeniden tesis edilmelidir.
- 2. Piyasa Mekanizmalarının İptali:** Sadece enerji baronlarını ihya eden PTF ve YEKDEM gibi piyasa bazlı, spekülasyon mekanizmaları derhal iptal edilmelidir.
- 3. Kamusal Sorumluluk:** Enerji desteği bir lütuf değil, devletin anayasal sorumluluğudur. Faturalardaki devlet desteği, enerji maliyetleri tam kontrol altına alınana dek %100'e yakın seviyelerde tutulmalı ve enerji halka maliyetine ulaştırılmalıdır.

Halkımızı, en temel hakkı olan enerjiye sahip çıkmaya, faturalar üzerinden yürütülen bu sermaye transferine karşı birlikte durmaya çağırıyoruz.

TMMOB Elektrik Mühendisleri Odası
İstanbul Şubesi
Enerji Komisyonu



TEKNİK EMEĞİN SINIFSAK YENİDEN KONUMLANIŞI VE GELECEĞİ

Mühendislik, mimarlık ve şehir planlama gibi teknik meslekler, modern üretimin ve toplumsal yaşamın örgütlenmesinde özgül bir yere sahiptir. Bu meslekler yüksek düzeyde eğitim, uzmanlık ve teknik bilgi gerektirir. Mühendisler, mimarlar ve şehir plancıları üretim süreçlerinin tasarlanması, planlanması, denetlenmesi ve geliştirilmesinde önemli roller üstlenirler. Bu nedenle teknik meslekler, uzun süre **görece yüksek toplumsal statü, mesleki özerklik ve çalışma güvencesiyle** ilişkilendirilmiştir.

Kapitalist üretimin dönüşümü, teknik emeğin bu **geleneksel konumunu** önemli ölçüde değiştirmektedir. **Teknik bilgi üretim açısından giderek daha merkezi hale gelirken, bu bilgiyi üreten çalışanların üretim süreci üzerindeki denetimi aynı ölçüde genişlememektedir.** Teknik kararlar maliyet, zaman, yatırım getirisi, rekabet ve performans gibi piyasa ölçütleri tarafından daha fazla belirlenmektedir. Böylece teknik çalışanların uzmanlığı üretim açısından değerini korurken, bu uzmanlığın hangi amaçlarla ve hangi koşullarda kullanılacağı üzerindeki **karar gücü**, çoğu zaman çalışanların dışındaki **kurumsal ve ekonomik aktörlerde** toplanmaktadır.

Bu durum, teknik emeğin günümüzdeki sınıfsal konumunu anlamak açısından **temel bir çelişki** yaratır. Teknik çalışanlar, üretim sürecinde özgül bir bilgiye ve belirli bir karar yetkisine sahip olsalar da büyük çoğunluğu yaşamlarını sürdürürebilmek için emek **güçlerini ücret karşılığında satmaktadır.** Marx'ın kapitalist üretim ilişkilerine dair çözümlemesinde belirleyici olan da çalışanın beceri düzeyinden önce, **üretim araçlarıyla kurduğu ilişki** ve emek-gücünün hangi toplumsal koşullarda satıldığıdır (Marx, Kapital, I. Cilt).

Dolayısıyla teknik emeğin **sınıfsal konumu** yalnızca mesleki statü, eğitim düzeyi veya gelir üzerinden açıklanamaz. **Uzmanlık**, ücretli emek ilişkisini ortadan kaldırmaz; bu ilişkinin özgül biçimini belirler. **Teknik emeğin dönüşümü**, uzmanlığın üretim sürecindeki öneminin artmasına karşın, bu uzmanlığın kullanım koşulları üzerindeki denetimin ne ölçüde çalışanlarda kaldığı üzerinden değerlendirilebilir.

BİLGİ
TASARIM
PLANLAMA
DENETİM
DAHA İYİ BİR
GELECEK

UZMANLIK
TOPLUM İÇİN
DAHA GÜÇLÜ
YARINLAR İÇİN



İnsan
Yaşamı
Güvenli
Kentler

Mesleki Özerkliğin Aşınması ve Teknik Etiğin Piyasa Baskısı Altına Girmesi

Teknik mesleklerin tarihsel özelliklerinden biri, **uzmanlığın belirli ölçüde mesleki özerklikle** birlikte kullanılmasıdır. Teknik çalışanların mesleki bilgileri doğrultusunda karar verebilmesi ve teknik gereklilikleri ekonomik ve idari baskılardan belirli ölçüde bağımsız değerlendirebilmesi, bu özerkliğin önemli bir parçasıdır.

Günümüz çalışma rejiminde bu alan daralabilmektedir.

Proje süreleri, maliyet hedefleri, yatırım beklentileri, performans göstergeleri ve kurumsal denetim mekanizmaları, teknik kararların sınırlarını daha fazla belirlemektedir. Teknik doğruluk ile ekonomik hedeflerin çatıştığı durumlarda, kararların sınırlarını yalnızca teknik gereklilikler değil, **işletmenin mali ve yönetsel öncelikleri** de belirleyebilmektedir.

Mühendislikte **güvenlik ve maliyet** arasındaki gerilim bunun açık örneklerinden biridir. Daha dayanıklı veya güvenli bir çözüm daha yüksek maliyet gerektirebilir. Ücretli mühendis bu durumda teknik sorumluluğu ile işverenin ekonomik beklentileri arasında konumlanır. Mimarlıkta tasarım kararları yatırım değeri ve piyasa talepleriyle; şehir planlamada ise kamusal yarar ile sermaye odaklı kentsel gelişme politikalarıyla karşı karşıya gelebilir.

Bu nedenle **teknik etik**, yalnızca **bireysel meslek ahlakı** olarak değerlendirilemez. Teknik bilginin hangi amaçlarla kullanılacağı, hangi risklerin kabul edileceği ve hangi toplumsal ihtiyaçların önceliklendirileceği, **üretim ilişkileriyle** doğrudan bağlantılıdır. Teknik çalışandan etik sorumluluk beklenirken çalışma sürecindeki gerçek karar yetkisinin sınırlandırılması, **sorumluluk ile karar gücü arasında yapısal bir çelişki** yaratır.

Teknik çalışanın bir kararın sonuçlarından sorumlu tutulması ile o kararın ekonomik ve yönetsel koşullarını belirleyebilmesi aynı şey değildir. Teknik etiğin gerçek anlamda işlerlik kazanabilmesi, teknik çalışanların yalnızca doğruyu söyleme yükümlülüğüne değil, **mesleki kararlarının koşulları üzerinde belirli bir söz hakkına** da sahip olmasına bağlıdır.

Teknik Emeğin Sınıfsal Konumu ve Proleterleşme Eğilimi

Teknik çalışanların **sınıfsal konumu**, eğitim düzeyi veya mesleki prestij üzerinden açıklanamaz. Kapitalist üretim ilişkileri açısından temel mesele, kişinin üretim araçlarıyla kurduğu ilişki ve yaşamını sürdürebilmek için **emek gücünü hangi koşullarda sattığıdır**. Ücretli mühendis, mimar veya şehir plancısı yüksek düzeyde uzmanlığa sahip olabilir; ancak **üretim araçlarının sahibi olmadığı** ve yaşamını sürdürmek için emek gücünü ücret karşılığında sattığı sürece, ücretli emek ilişkisi içinde yer alır (Marx, Kapital, I. Cilt).

Bununla birlikte teknik çalışanların konumu, geleneksel sanayi işçisinin konumuyla bütünüyle özdeş değildir. **Teknik çalışanlar üretim sürecinde belirli bir bilgi, uzmanlık ve karar alanına sahip olabilir**; buna karşılık üretimin genel yönünü, yatırımların dağılımını veya üretim araçlarının mülkiyetini belirleme gücüne çoğunlukla sahip değildir.

Erik Olin Wright'ın sınıf çözümlemesi, uzmanlık, otorite ve denetim sahibi bazı çalışanların temel sınıf ilişkileri içinde özgül ve çelişkili konumlar taşıyabileceğini göstermektedir. Wright'ın **"Sınıflar"** adlı çalışması, sınıfsal konumların yalnızca mülkiyet ilişkileriyle değil, otorite ve uzmanlık gibi üretim sürecindeki farklı güç ilişkileriyle birlikte değerlendirilmesi gerektiğini ortaya koyar (Wright, Sınıflar).

Bu çerçevede **proleterleşme**, mühendislerin, mimarların veya şehir plancılarının geleneksel sanayi işçileriyle bütünüyle aynı hale gelmesi anlamında kullanılmamaktadır. Buradaki anlamıyla proleterleşme, esas olarak **üretim süreci üzerindeki denetimin zayıflaması, çalışma koşullarının sermaye ve yönetim tarafından daha yoğun biçimde belirlenmesi ve emek gücünün piyasa karşısındaki bağımlılığının artmasıdır**.

Bu yaklaşım, Marx'ın kapitalist emek sürecine ilişkin analizleriyle ve **Harry Braverman'ın** geliştirdiği **emek süreci perspektifiyle** ilişkilendirilebilir. Marx, kapitalist emek sürecini ele alırken kapitalistin satın aldığı emek-gücünü üretim sürecinde belirli bir amaç doğrultusunda kullandığını ve bu sürecin kapitalist denetim altında gerçekleştiğini ortaya koyar (Marx, Kapital, I. Cilt, 7. bölüm).



Braverman'ın “Emek ve Tekelci Sermaye” adlı çalışması ise gelişmiş kapitalizm bağlamında yönetsel denetimin bilgi, planlama ve emek sürecinin örgütlenmesi üzerindeki rolünü inceler. Bu yaklaşım, üretim sürecinin bilgisinin ve planlanmasının yönetimde yoğunlaşmasının çalışanların **emek sürecindeki özerkliğini** zayıflatabileceğini göstermektedir (Braverman, Emek ve Tekelci Sermaye).

Dolayısıyla teknik emeğin proleterleşmesi, **uzmanlığın ortadan kalkması değildir**. Asıl mesele, teknik çalışanın sahip olduğu bilgi ve becerilerin **kullanım koşulları üzerindeki bireysel ve kolektif denetimin zayıflamasıdır**. Uzmanlık devam ederken, bu uzmanlığın üretim sürecindeki kullanım biçimleri giderek daha fazla kurumsal ve ekonomik hedefler tarafından belirlenebilir.

Bilgi Emeği, Uzmanlık ve Sınıfsal Konum

Kapitalist üretimde bilim, teknoloji ve teknik bilgi giderek daha önemli hale gelmektedir. Mühendislik, yazılım, tasarım, veri analizi, araştırma-geliştirme ve diğer uzmanlık alanlarının ekonomik ağırlığının artması, bilgi sahibi çalışanların üretim içindeki konumunu da dönüştürmektedir. Ancak bilginin üretimdeki öneminin artması, bu bilgiyi üreten çalışanların üretim üzerindeki toplumsal denetiminin otomatik olarak güçlendiği anlamına gelmez.

Buradaki temel mesele, bilginin üretim sürecine nasıl dahil olduğudur. Kapitalist üretim açısından bilgi, üretimin diğer unsurları gibi örgütlenebilir, ölçülebilir ve denetlenebilir bir üretim kapasitesine dönüşebilir. Çalışanın uzmanlığı korunurken, bu uzmanlığın kullanım amacı, çalışma temposu ve üretim içindeki işlevi sermaye ve yönetim tarafından belirlenebilir.

Bu nedenle, bilgi ile karar gücünün aynı kişilerde toplanması zorunlu değildir. Bir mühendisin ileri düzey teknik bilgiye sahip olması, üretim araçlarının mülkiyetine sahip olduğu anlamına gelmez.

Bir mimarın yaratıcı tasarım kapasitesi, projenin hangi ekonomik amaçla gerçekleştirileceği üzerinde belirleyici olduğu anlamına gelmez. Teknik emeğin özgüllüğü tam da burada ortaya çıkar; **yüksek düzeyde uzmanlaşma, üretim üzerindeki toplumsal ve ekonomik denetimi kendiliğinden beraberinde getirmez**.

Marx'ın iş bölümü ve manifaktür üzerine çözümlemeleri, teknik becerilerin kapitalist üretim içinde bireysel bir ustalık olmaktan çıkarılarak daha **geniş bir üretim örgütlenmesinin parçası** haline gelmesini anlamak açısından önemlidir (Marx, Kapital, I. Cilt, 14. bölüm). **Braverman** ise bu sürecin modern kapitalist çalışma örgütlenmesindeki sonuçlarını, planlama ve uygulama arasındaki ayrışma ve yönetsel denetimin güçlenmesi üzerinden tartışmaktadır (Braverman, Emek ve Tekelci Sermaye).

Bu açıdan teknik çalışanları, “**uzmanlaşmış ücretli emek**” kavramı üzerinden değerlendirmek işlevsel bir çerçeve sunar. Bu kavram, teknik çalışanların uzmanlıklarını ve üretim sürecindeki özgül rollerini görmezden gelmeden, onların ücretli emek ilişkisi içindeki konumunu vurgular. Böylece **mesleki özgünlük ile sınıfsal konum** birbirinin alternatifi olmaktan çıkar.

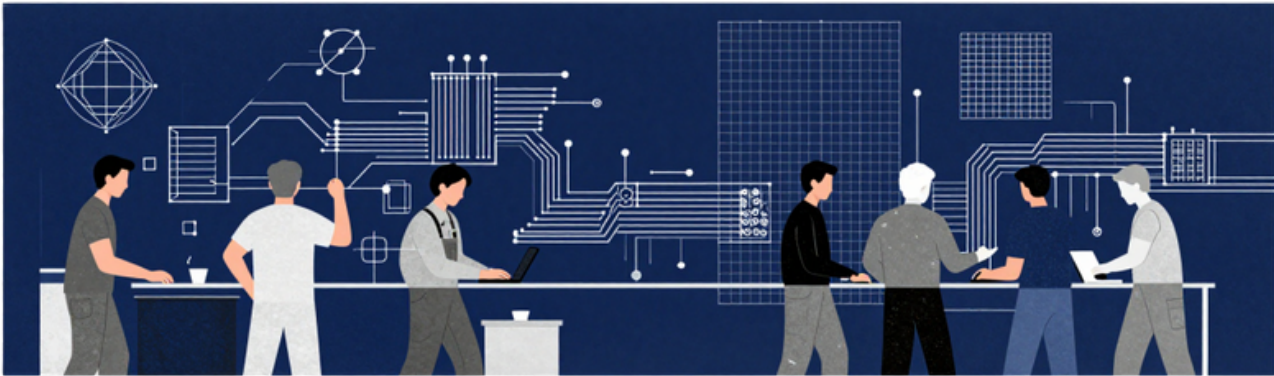
Teknik Emegın Örgütlenme Sorunu ve Sınıfsal Farkındalık

Teknik çalışanların örgütlenmesi önündeki önemli engellerden biri, **mesleki kimliğin sınıfsal konumun önüne geçebilmesidir**. Mühendis, mimar veya şehir plancısı olmak; uzun bir eğitim süreci, uzmanlık ve toplumsal prestij üzerinden şekillenen güçlü bir kimlik yaratmaktadır. Çalışma koşullarından kaynaklanan sorunlar bu nedenle sıklıkla mesleki itibar, kişisel kariyer veya bireysel başarı üzerinden değerlendirilebilmektedir.

Bireyselleşmiş çalışma kültürü de bu eğilimi güçlendirmektedir. Rekabet, kişisel kariyer yönetimi, sürekli kendini geliştirme ve bireysel piyasa değerini artırma baskısı, ortak çalışma deneyimlerinden doğabilecek **kolektif bilincin** gelişmesini zorlaştırabilir. Düşük ücret, uzun çalışma saatleri, güvencesizlik ve yoğun performans baskısı yalnızca bireysel sorunlar olarak algılandığında, bunların arkasındaki **yapısal emek ilişkileri** görünmez hale gelebilir.

Bu nedenle teknik çalışanların örgütlenmesi, iki boyutun birlikte düşünülmesini gerektirir. **Meslek örgütleri** bilimsel doğruluk, meslek etiđi, kamusal yarar ve uzmanlık alanlarının korunması açısından önemli bir işleve sahiptir. **Sendikal ve işyeri temelli örgütlenmeler** ise ücret, çalışma süresi, iş güvencesi ve emek sürecinin koşulları üzerinde kolektif güç yaratır. Teknik emegın özgül sorunları, bu iki alanın birbirinden tamamen koparılmasını zorlaştırmaktadır.

Türkiye’de mühendis ve mimar odaları da tarihsel olarak mesleki hakların yanı sıra **kamu yararı, bilimsel doğruluk ve meslek etiđi** konularında müdahil olmuştur. Ücretli teknik çalışanların çalışma koşullarının emek ilişkileri tarafından daha doğrudan belirlenmesi, mesleki örgütlenme ile emekçi örgütlenmesi arasındaki ilişkinin yeniden düşünülmesini gerekli kılmaktadır.



Teknik alıřanların ortak ıkarlarını fark etmesi, **mesleki kimliđin reddi** anlamına gelmez. Tersine, uzmanlıđın toplumsal deđerini daha geniř bir erevede deđerlendirmeyi mümkün kılar. Teknik alıřan, kendi emeđinin hangi kořullarda üretildiđini, ürettiđi bilginin kimin ıkarlarına hizmet ettiđini ve alıřma sürecindeki temel kararların kim tarafından belirlendiđini sorguladıđında, **mesleki kimlik ile sınıfsal bilin arasında yeni bir iliřki kurulabilir**.

Bu aıdan örgütlenme, daha iyi ücret veya alıřma kořulları talep etmekle sınırlı deđildir. **Teknik kararların alınma biimi, mesleki sorumluluđun kořulları ve üretilen bilginin kullanım amacı** da kolektif mücadelenin konusu haline gelebilir.

Teknik Emegın Toplumsal Rolünün Yeniden Tanımlanması

Teknik bilgi toplumun fiziksel evresini, altyapısını, teknolojik kapasitesini ve yařam kořullarını dođrudan biimlendirmektedir. Bu nedenle **mühendislik, mimarlık ve řehir planlama** faaliyetlerinin sonuçları, ekonomik üretimin sınırlarını ařan toplumsal etkiler yaratır.

Teknik kararlar, bütünüyle nötr deđildir. Bir yapının hangi güvenlik standartlarıyla tasarlanacađı, hangi teknolojinin kullanılacađı, hangi maliyetlerin kabul edileceđi veya bir kentsel alanın hangi amaçla deđerlendirileceđi, teknik bilgi kadar **toplumsal önceliklerle** de iliřkilidir.

Andrew Feenberg, teknoloji ile toplumsal deđerler ve iktidar iliřkileri arasındaki bađlantıyı eleřtirel teknoloji kuramı erevesinde inceler. “**Teknoloji ve Toplum**” adlı alıřması, teknolojik gelişmenin toplumsal deđerlerden bađımsız, yalnızca teknik bir süreç olarak ele alınamayacađını savunan yaklařımını ortaya koymaktadır (Feenberg, Teknoloji ve Toplum).

Bu nedenle, teknik alıřanın toplumsal sorumluluđu, meslek etiđi kurallarıyla sınırlanamaz. **Mühendislikte güvenlik, mimarlıkta yařam kalitesi, řehir planlamada kamusal yarar ve evresel sürdürülebilirlik** gibi meseleler, teknik uzmanlıđın dıřında kalan ikincil konular deđildir. Bunlar, teknik bilginin hangi amaçlarla kullanılacađına iliřkin kararların dođrudan paralarıdır.

Teknik emeđin toplumsal rolünün yeniden tanımlanması, **uzmanlıđın siyasallařtırılması** anlamına gelmez. Teknik kararların zaten belirli ekonomik ve toplumsal iliřkiler içinde alındıđını kabul etmek anlamına gelir. Bu nedenle, teknik alıřanların kendi emek süreçlerinde daha fazla söz sahibi olması, yalnızca alıřma kořullarını deđil, üretilen teknik özümmlerin toplumsal niteliđini de etkileyebilir.

Bu aıdan **teknik emeđin özgürleşmesi**, ekonomik kořulların iyileřtirilmesinden daha geniř bir meseledir. alıřanın ürettiđi bilginin kullanım kořulları üzerinde **söz sahibi olması**, mesleki etik ile alıřma kořulları arasındaki bađın güçlendirilmesi ve teknik

kararların toplumsal sonuçları üzerine **kolektif bir söz üretilebilmesi** bu sürecin temel unsurlarıdır.

Sonuç: Teknik Emeğin Geleceği ve Toplumsal Yönelimi

Teknik emeğin günümüzdeki dönüşümü, yalnızca mühendislik, mimarlık ve şehir planlama mesleklerinin çalışma koşullarındaki değişim olarak ele alınamaz. Bu dönüşüm, **bilginin üretim içindeki artan önemi ile bilgiyi üretenlerin bu üretim üzerindeki sınırlı denetimi arasındaki çelişkiyi** görünür hale getirmektedir.

Teknik çalışanların sınıfsal konumu bu nedenle eğitim, mesleki statü veya uzmanlık üzerinden değil, öncelikle **üretim araçlarıyla ve emek süreci üzerindeki denetimle kurdukları ilişki** bağlamında değerlendirilmelidir. Teknik emeğin özgünlüğü, yüksek düzeyde bilgi ve uzmanlık gerektiren bir faaliyetin aynı zamanda **ücretli emek ilişkisi içinde yürütülmesinde** ortaya çıkar. **Proleterleşme** ise uzmanlığın ortadan kalkması değil, uzmanlığın kullanım koşulları üzerindeki **bireysel ve kolektif denetimin zayıflaması** olarak anlaşılmalıdır.

Bu durum, teknik çalışan açısından **mesleki sorumluluk ile gerçek karar yetkisi arasındaki gerilimi** de ortaya çıkarır. Teknik çalışandan **güvenlik, doğruluk ve kamusal yarar** konusunda sorumluluk beklenirken, bu kararların ekonomik ve yönetsel koşulları üzerindeki etkisi sınırlı kalıyorsa, mesleki etik ile üretim ilişkileri arasında yapısal bir çelişki oluşur.

Bu nedenle, teknik emeğin geleceği açısından mesele; daha yüksek ücret, daha iyi çalışma koşulları veya daha güçlü mesleki statü elde etmekle sınırlı değildir. Bunlar önemlidir; ancak asıl mesele, teknik bilginin üretiminde ve kullanımında **karar gücünün kimde olduğudur**.

Buradan hareketle üç alan özellikle önem kazanmaktadır. Birincisi, **mesleki etik ile çalışma koşulları arasındaki bağın güçlendirilmesidir**. Teknik sorumluluğun gerçek anlamda yerine getirilebilmesi, bu sorumluluğun gerektirdiği kararlar üzerinde çalışanların söz hakkına sahip olmasını gerektirir.

İkincisi, **mesleki örgütlenme ile emekçi örgütlenmesinin birbirinin alternatifi olarak görülmemesidir**. Meslek örgütleri uzmanlığın bilimsel ve etik ölçütlerini, kamusal sorumluluğunu ve mesleki hakları savunurken; sendikal ve işyeri temelli örgütlenmeler teknik emeğin çalışma koşulları, kolektif pazarlık gücü ve emek süreci üzerindeki etkisini artırabilir. Teknik emeğin özgünlüğünü koruyan, ancak onu sınıfsal ilişkilerden koparmayan bir örgütlenme anlayışı bu iki boyutun birlikte düşünülmesini gerektirir.

Üçüncüsü, **teknik çalışanların yalnızca emeğinin karşılığı üzerinde değil, ürettikleri bilginin kullanım koşulları üzerinde de söz sahibi olmasıdır**. Teknik kararların hangi maliyetlerle, hangi riskleri kabul ederek ve hangi toplumsal ihtiyaçları önceleyerek alınacağı, yalnızca yöneticilerin veya sermaye sahiplerinin belirleyeceği bir mesele

değildir. Bu kararların, üretim sürecinin içinde bulunan teknik çalışanların kolektif deneyimiyle birlikte ele alınması, mesleki özerkliğin toplumsal bir boyut kazanmasını sağlayabilir.

Sonuç olarak, teknik emeğin geleceği uzmanlığın piyasa karşısında ne ölçüde korunacağından çok, **uzmanlığın toplumsal yöneliminin kim tarafından belirleneceği** sorusunda düğümlenmektedir. Teknik bilgi sermaye birikiminin ve rekabetin hizmetinde örgütlenebileceği gibi, güvenli yaşam alanlarının, kamusal altyapının, çevresel sürdürülebilirliğin ve toplumsal ihtiyaçların karşılanmasına da yöneltilebilir. Bu tercih, teknik bilginin kendisinden değil, onun üretildiği ve kullanıldığı **toplumsal ilişkilerden** kaynaklanır.

Bu açıdan **teknik emeğin özgürleşmesi**, uzmanlığın sınıfsal ilişkilerin dışına çıkarılması değil, **uzmanlığın üretim üzerindeki toplumsal denetimle yeniden ilişkilendirilmesidir**. Mühendislerin, mimarların ve şehir plancılarının gelecekteki konumu yalnızca sahip oldukları bilgi ve beceriler tarafından değil, bu bilgi ve becerilerin kullanım koşulları üzerinde ne ölçüde **kolektif söz hakkına sahip olacakları** tarafından da belirlenecektir.

Dolayısıyla teknik emeğin meselesi, bir meslek grubunun geleceğinden ibaret bir olgu değildir. **Bilgi, emek, teknoloji ve toplumsal ihtiyaç arasındaki ilişkinin nasıl kurulacağı**, daha geniş bir toplumsal geleceğin de temel sorunlarından biridir. Teknik emeğin sınıfsal konumunun görünür hale gelmesi, mesleki değerlerin terk edilmesini değil; uzmanlığın, mesleki etiğin ve kamusal sorumluluğun emek süreçlerinin gerçek koşullarıyla birlikte yeniden düşünülmesini mümkün kılar.

Mehmet YEŞİLTEPE

Kaynakça

- *Braverman, Harry. (2008). Emek ve Tekelci Sermaye: Yirminci Yüzyılda Çalışmanın Değersizleştirilmesi. İstanbul: Kalkedon Yayınları.*
- *Feenberg, Andrew. (2010). Teknoloji ve Toplum: Yıkıcı Bir Direniş ve Yeniden Yapılanma. İstanbul: Kalkedon Yayınları.*
- *Marx, Karl. (2011). Kapital: Ekonomi Politikin Eleştirisi, Birinci Cilt: Sermayenin Üretim Süreci. Çev. Alaattin Bilgi. Ankara: Sol Yayınları.*
- *Wright, Erik Olin. (2016). Sınıflar. Çev. Selma Toral. İstanbul: NotaBene Yayınları.*

KÜRESEL ENERJİ DENKLEMİNDE MÜHENDİSLİK: AĞIRLAŞAN TÜKETİM YÜKÜ VE YENİ ELEKTRİK/YANGIN STANDARTLARI

Küresel enerji mimarisi; karbonsuzlaşma hedefleri, ulaşımın elektrik enerjisi odaklı artması ve yapay zekâ veri merkezlerinin üssel hızla büyümesiyle tarihin en köklü dönüşümlerinden birini yaşamaktadır. Uluslararası enerji politikaları şebeke esnekliği ve yenilenebilir enerji entegrasyonuna odaklanırken, sahadaki elektrik mühendisliği uygulamaları her geçen gün daha karmaşık teknik zorluklarla karşılaşmaktadır. Elektrik altyapıları artık yalnızca enerji ileten hatlar olmaktan çıkmış; yüksek termal ve harmonik yükler altında çalışan, yangın risk katsayısı artmış ve çok daha sıkı mevzuat uyumları gerektiren sistemlere dönüşmüştür. Bu tablo karşısında elektrik mühendisliği mesleği, teknolojik gelişmeler ile can ve mal güvenliğinin tam kesişim noktasında durmaktadır.

Küresel Güç Talebi ve Elektrik Altyapıları Üzerindeki Yük Baskısı

Yüksek performanslı yapay zekâ veri merkezlerinin, endüstriyel otomasyon tesislerinin ve yüksek güçlü elektrikli araç (EV) şarj altyapılarının hızla yaygınlaşması, dağıtım şebekelerindeki yük profillerini kökten değiştirmiştir. Yüksek yoğunluklu sunucuların kesintisiz çalışma gereksinimleri—doğrusal olmayan yükler ve yüksek harmonik bozulmalarla birleştiğinde—trafolar, şalt tesisleri ve kablo hatları üzerinde daha önce benzeri görülmemiş bir stres yaratmaktadır.

Sürekli yüksek yük seviyeleri, yalıtkan malzemelerin yaşlanmasını hızlandırmakta ve bina içi dağıtım sistemlerinde termal kontrolden çıkma ve fazlar arası denge bozulumu riskini artırmaktadır. Bu doğrultuda, uluslararası elektrik standartları sürekli güncellenmekte; Ark Hatası Algılama Cihazları ve gelişmiş koruma topolojileri gibi teknolojilerin kullanımı zorunlu hale gelmektedir.

Yerli Üretim, Sertifikasyon Engelleri ve İthal Ürün Baskısı

Uluslararası direktifler ve yangın koruma kodları katılaştıkça, yerli elektrik ekipmanı üreticileri belgelendirme, laboratuvar testleri ve direktiflere uygunluk konusunda kritik engellerle karşılaşmaktadır. Yapı Malzemeleri Yönetmeliği kapsamında kabloların yangına tepki sınıflarının tespiti, Alçak Gerilim Direktifi ve Elektromanyetik Uyumluluk gereksinimleri, akredite test tesisleri ve yüksek belgelendirme maliyetlerini beraberinde getirmektedir.

Yerli üreticiler ise, ithal ürünlerin rekabetiyle de yüzleşmektedir. Yerli sanayici Avrupa standartlarına uyum sağlamakta zorlanırken, projelerde denetlenmemiş veya uygunsuz bileşenlerin kullanılması kritik altyapılarda yangın ve güvenlik risklerini büyötmektedir.

Piyasa gözetimi ve denetimi mekanizmalarının sıkılaştırılması, test edilmiş ve tip testi sertifikalı ürünlerin projelerde önceliklendirilmesi, kamusal ve endüstriyel güvenliğin teminatı olacaktır.

Çatı Güneş Enerji Santralleri (GES): Yangın Riskleri ve Bölümlendirme

Ticari ve endüstriyel yapılarda çatı tipi güneş enerji santrallerinin (GES) yaygınlaşması, sadece bina içi yangın güvenliği açısından değil, yapı dışı yeni bir risk matrisi oluşturmuştur. Çatı GES sistemleri, gün ışığı var olduğu sürece enerjiyi kesmenin mümkün olmadığı sürekli Doğru Akım (DC) kaynaklarıdır. Bu durum, olası bir yangın anında acil kapatma ve söndürme müdahalelerini zorlaştırmaktadır.

Çatı GES projelerinde öngörülmesi gereken temel yangın güvenlik tedbirleri şunlardır:

- ◆ **Hızlı DC Ark Yalıtımı ve Modül Düzeyinde Kapatma:** Şebeke kesintisi veya yangın ihbarı durumunda DC dizi gerilimini saniyeler içinde güvenli seviyelere (<30V) düşüren modül düzeyinde güç elektroniği ve otomatik hızlı kapatma sistemlerinin tesisi.
- ◆ **Yapısal Bölümlendirme ve Geçiş Yolları:** Çatılarda yangının yatayda yayılmasını önleyecek yangına dayanıklı bariyerlerin oluşturulması ve itfaiye müdahale personeli için yürüyüş ve müdahale koridorlarının bırakılması.
- ◆ **Termal Denetim ve Kablo Yönetimi:** DC kablo güzergahlarının yanıcı çatı kaplamalarından izole edilmesi ve yüksek dirençli sıcak noktaların tespiti için periyodik IR termografik muayenelerin zorunlu ve periyodik kılınması.

“

**Güvenli GES,
sürdürülebilir
enerjinin
teminatıdır .**

YENİLENEBİLİR
ENERJİ
DAHA GÜVENLİ
YARINLAR İÇİN

Temel Yangın Güvenlik Tedbirleri



Hızlı DC Ark Yalıtımı ve Modül Düzeyinde Kapatma

Şebeke kesintisi veya yangın ihbarı durumunda DC dizi gerilimini saniyeler içinde güvenli seviyelere (<30V) düşüren modül düzeyinde güç elektroniği ve otomatik hat kapatma sistemlerinin tesisi.



Yapısal Bölümlendirme ve Geçiş Yolları

Çatılarda yangının yatayda yayılmasını önleyecek yangına dayanıklı bariyerlerin oluşturulması ve itfaiye müdahale personeli için yürüyüş ve müdahale koridorlarının bırakılması.



Termal Denetim ve Kablo Yönetimi

DC kablo güzergahlarının yanıcı çatı kaplamalarından izole edilmesi ve yüksek dirençli sıcak noktaların tespiti için periyodik IR termografik muayenelerin zorunlu ve periyodik kılınması.

Elektrikli Araç (EV) Şarj İstasyonları: Yangın Riskleri ve Söndürme Teknikleri

Kapalı otoparklarda ve çok katlı binalarda Elektrikli Araç Şarj İstasyonlarının artışı, özellikle Lityum-iyon batarya yangınları nedeniyle özel önlemler gerektirmektedir. Lityum-iyon batarya yangınları; kontrolsüz sıcaklık artışı, toksik gaz salınımı, kendi oksijenini üreterek yanma ve yeniden alevlenme gibi aşırı tehlikeli özellikler taşımaktadır.

EV şarj istasyonu tasarımında standart aşırı akım korumasının ötesine geçilmelidir. Tesisatlar, binanın yangın algılama sistemine entegre otomatik güç kesme cihazlarına sahip olmalıdır. Kapalı ve yeraltı otoparklarda yer alan şarj odalarında; mekanik duman tahliye sistemleri, termal kamera takibi ve termal kontrolden çıkma olaylarını baskılamaya yönelik özel baskılama ve söndürme (özel köpük/su sisi, toz veya gazlı söndürme) altyapıları tasarlanmalıdır.

İtfaiye erişim güzergahları ve araç tahliye prosedürleri proje aşamasında belirlenmelidir.



Lityum-iyon Batarya Yangınlarının Tehlikeleri



Kontrolsüz sıcaklık artışı

Kısa sürede çok yüksek sıcaklıklara ulaşabilir.



Toksik gaz salınımı

Zehirli ve aşındırıcı gazlar açığa çıkar.



Kendi oksijenini üreterek yanma

Yanma süreci kendi oksijenini üreterek devam edebilir.



Yeniden alevlenme

Söndürme sonrasında dahi yeniden alevlenme riski yüksektir.



Mesleki Sorumluluk, İnsan Yaşamı ve Can/Mal Güvenliği

Binaların Yangından Korunması Hakkında Yönetmelik ve güncellenen elektrik tesisat standartları çerçevesinde; elektrik mühendisinin üzerine düşen yasal, teknik ve vicdani sorumluluk her zamankinden daha ağırdır.

Proje onayı, saha denetimi, kabul testleri ve periyodik kontroller sıradan birer bürokratik prosedür değildir; insan yaşamını ve milli serveti koruyan ana savunma hattıdır.

Mühendisler; kablo kesitlerinden, koruma elemanlarından veya yangın bölümlendirme kurallarından ticarileşme baskısı nedeniyle taviz vermemelidir. Teknik etik, standartlara kesin uyum ve mesleki denetim, elektrik merkezli dünyada can ve mal güvenliğinin en temel teminatıdır.

Halen görev yaptığım 45. Dönem Elektrikli Araçlar ve Raylı Sistemler Komisyonu üyesi olarak bu konularda kamuyu bilgilendirmek ve farkındalık yaratmak amacıyla çalışmalarımıza devam ediyoruz.



Mühendis Murat ERBAŞ
HazerFen.Net Enerji Güvenlik ve NDT Sistemleri



ELEKTRİK ENERJİSİNDE DİJİTAL DÖNÜŞÜM

Enerjide dijital dönüşüm son yılların en sık kullanılan kavramlarından biri. Ancak sahadaki gerçekliğe baktığımızda, beklentilerle mevcut uygulamalar arasında hâlâ önemli bir mesafe bulunduğunu görüyoruz. Günlük uygulamalara baktığımızda aslında enerjide dijitalleşmenin birçok farklı alanı olmasına rağmen bu yazıda kendi uzmanlık alanımız olan elektrik altyapılarında dijitalleşmeye odaklanacağız.

Günümüzde hâlâ pek çok işletmede aylık tüketim faturadan ya da haberleşme özelliği bulunmayan basit ölçüm cihazlarından , teknik ekiplerin düzenli ziyaretleri ve aldıkları manuel kayıtlar ile takip ediliyor; fakat enerjinin hangi hatta, hangi saatlerde ve hangi güç kalitesi koşullarında tüketildiği yeterince bilinmiyor. Bu görünürlük oluşmadan verimlilikten, kestirimci bakımdan veya yapay zekâdan söz etmek çoğu zaman eksik kalıyor.

Elektrik altyapısında dijital dönüşümün çıkış noktası oldukça net: Ölçemediğimiz bir sistemi göremeyiz, izlemediğimiz bir sistemi yönetemeyiz. Bu nedenle dönüşüm; önce doğru noktadan ve doğru cihazla ölçmekle, ardından veriyi düzenli biçimde toplamakla başlar. Analiz ve aksiyon ise bu iki adımın üzerine kurulur.



Dijitalleşme ile dijital dönüşüm aynı şey değil

Bir enerji analizörü ve sensörün panoya yerleştirilmesi, sayaçların haberleşmeye açılması veya bir izleme yazılımının kurulması dijitalleşmenin parçalarıdır. Dijital dönüşüm ise bu araçlardan gelen verinin bakım, işletme ve yatırım kararlarına düzenli olarak yansımasıdır. Başka bir ifadeyle dijitalleşme veriyi üretir; dijital dönüşüm, o veriden kurumsal bir çalışma biçimi oluşturur.

Bu ayrım önemlidir. Çünkü ölçüm cihazları kurulmuş olmasına rağmen verisi okunmayan, alarmları tanımlanmayan veya raporları karar toplantılarına girmeyen çok sayıda tesis bulunuyor. Böyle bir yapıda teknoloji vardır; ancak dönüşüm tamamlanmamıştır. Gerçek dönüşümde enerji verisi yalnızca elektrik biriminin ekranında kalmaz. Bakım planlamasına, üretim hedeflerine, satın alma kararlarına, karbon raporlamasına ve üst yönetime sunulan performans raporlarına kadar geniş bir alanda kendini gösterir.

Sahada sık karşılaştığım bir başka beklenti de enerji izleme sistemi kurulduğunda tasarrufun kendiliğinden oluşacağı düşüncesidir. Oysa ölçüm cihazı tek başına enerji tasarrufu sağlamaz; kaybın nerede ve ne zaman oluştuğunu gösterir. Tasarrufu yaratan, bu bilgiye bağlı alınan hedef ve aksiyonlardır.

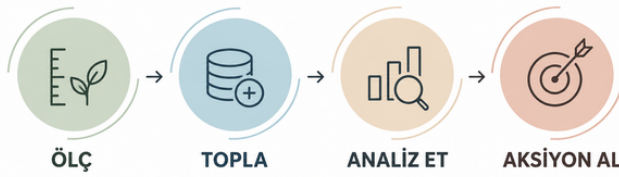
Enerjide neden daha fazla görünürlüğe ihtiyaç duyuyoruz?

Elektrik sistem ve altyapıları teknolojik gelişmelerin hızına paralel olarak daha karmaşık bir hal alıyor. Yenilenebilir enerji kaynakları, elektrikli araçlar, enerji depolama sistemleri, UPS'ler, hız kontrol sürücüleri, veri merkezleri ve hassas elektronik yükler hem tüketim profilini hem de güç kalitesi dinamiklerini değiştiriyor. Tek yönlü enerji akışına göre tasarlanmış geleneksel yapı, artık daha değişken ve daha fazla veri üreten bir sisteme dönüşüyor.

Uluslararası Enerji Ajansı, 2025 yılında küresel enerji yatırımlarının 3,3 trilyon ABD dolarına ulaşacağını; bunun yaklaşık 2,2 trilyon dolarının temiz enerji teknolojilerine yöneldiğini belirtiyor. Bu ölçekte bir dönüşümde yalnızca yeni üretim kapasitesine değil, enerjiyi güvenilir biçimde ölçen ve yöneten dijital altyapıya da ihtiyaç var.

ABD Enerji Bakanlığının enerji yönetimi rehberinde de etkili enerji kararlarının sürekli ölçüm, izleme ve veri analizine dayanması gerektiği vurgulanıyor. Başka bir ifadeyle dijitalleşmenin değeri, sahadan daha fazla veri toplamakta değil; doğru ve güvenilir veriyi karar mekanizmasına taşıyabilmekte ortaya çıkıyor.

Dönüşümün Dört Temel Adımı



1. Ölç

Ölçüm mimarisi, “her panoya bir cihaz koyalım” yaklaşımıyla değil, tesisin riskleri ve karar ihtiyaçlarıyla tasarlanmalıdır. Şebeke girişi, trafo çıkışları, jeneratör ve UPS giriş-çıkışları, kritik dağıtım panoları ile enerji yoğun yükler önceliklendirilmelidir. Burada dijital ölçüm cihazları dönüşümün temel saha katmanıdır. Sadece ekranda akım, gerilim veya kWh gösteren bir analizör yerine; haberleşebilen, zaman damgalı kayıt tutabilen, trend ve olay verisi üretebilen cihazlar tercih edilmelidir. Gerilim, akım, aktif-reaktif güç, enerji, talep ve güç faktörünün yanında; harmonikler, faz dengesizliği, gerilim çökmesi-yükselmesi, kesintiler ve geçici olaylar da ihtiyaca göre izlenmelidir.

2. Topla

Farklı noktalardaki ölçümlerin ortak bir haberleşme altyapısında toplanması gerekir. Modbus RTU/TCP, Ethernet, haberleşme ağ geçitleri, SCADA ve enerji izleme yazılımları bu katmanın araçlarıdır. Buradaki kritik konu yalnızca bağlantı kurmak değildir. Zaman senkronizasyonu, ölçüm periyotları, veri kaybı, cihaz adlandırma standardı ve siber güvenlik daha tasarım aşamasında ele alınmalıdır. Güvenilir olmayan veri, çok gelişmiş bir analiz yazılımında bile güvenilir sonuç üretmez.

3. Analiz Et

Ham verinin anlamlı bilgiye dönüşmesi için karşılaştırma gerekir. Baz yük nedir? En yüksek talep hangi saatte oluşuyor? Reaktif enerji hangi yük rejiminde artıyor? Harmonik bozulma hangi ekipman devreye girdiğinde yükseliyor? Gerilim olayı ile üretim duruşu aynı zaman damgasında mı gerçekleşiyor? Tesisin normal çalışma davranışı tanımlandığında sapmalar daha erken görülebilir. Yapay zekâ ve ileri analitik burada değerli bir üst katman olabilir; ancak doğru etiketlenmiş, sürekliliği olan ve mühendislik katkısı sağlanmış veri olmadan sağlıklı sonuç beklenmemelidir.

4. Aksiyon Al

Analiz, uygulanabilir bir karara dönüşmediği sürece rapor olarak kalır. Aksiyon yalnızca bir ekipman yatırımı da değildir. Enerji izleme ve yönetim yazılımlarında alarm eşikleri oluşturmak, pik talebi takip etmek, bölüm veya hat bazında enerji KPI'ları tanımlamak ve otomatik raporlar üretmek ilk adımlardan biri olabilir. Fiziksel tarafta ise aktif harmonik filtre, SVG veya uygun kompanzasyon çözümü; pompa ve fanlarda hız kontrol sürücüsü, verimli motor uygulaması, yük dengeleme, otomatik talep/yük yönetimi, arızalı ekipmanın bakımı ya da kablo-şalter boyutlandırmasının gözden geçirilmesi gündeme gelebilir. Hangi çözümün gerçekten fayda sağladığı ölçümle belirlenmeli; uygulama sonrasında aynı noktadan tekrar doğrulanmalıdır. Böylece süreç tek seferlik ölçümden sürekli iyileştirme döngüsüne geçer.

Dijitalleşmemiş enerjinin görünmeyen riskleri

Dijitalleşmemiş bir elektrik altyapısındaki temel risk, sistemin çalışmaması değil; bozulmanın geç fark edilmesidir. Aylık fatura toplam tüketimi gösterir fakat gece oluşan kısa bir gerilim çökmesini, nötr iletkende büyüyen üçüncü harmonik akımını, bir fazın giderek daha fazla yüklenmesini veya bir bağlantı noktasındaki sıcaklık artışını göstermez. Bu tür olaylar zaman içinde enerji kaybına, ekipman ömrünün kısılmasına, beklenmeyen açmalara, üretim duruşlarına ve bazı durumlarda güvenlik risklerine dönüşebilir.

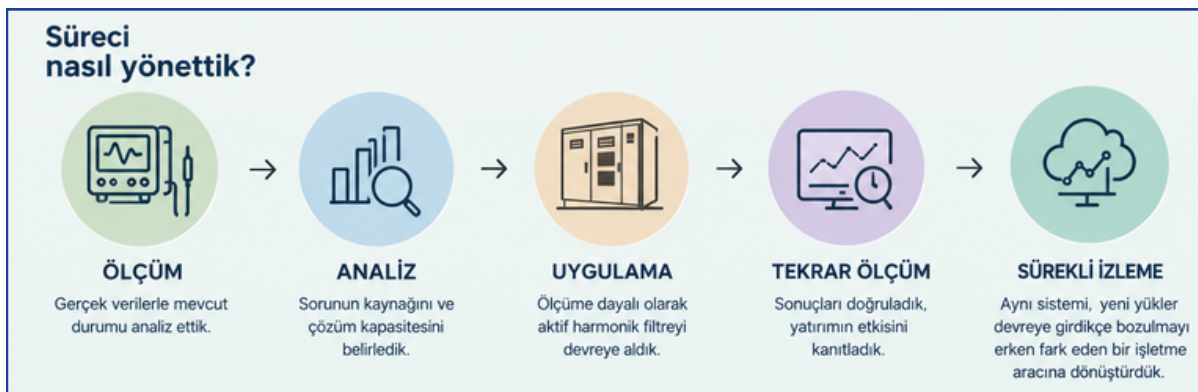
Harmonikler bunun iyi bir örneğidir. Yüksek harmonik seviyeleri transformatör, motor, kablo ve özellikle nötr iletkenlerde ek ısınmaya; koruma elemanlarında beklenmeyen açmalara ve hassas elektronik cihazlarda çalışma problemlerine yol açabilir. Gevşek veya hasarlı elektrik bağlantıları ise ark ve yangın riskinin kaynaklarından biridir. NFPA'nın 2017-2021 ABD endüstriyel tesis verilerine göre; elektrik dağıtım, aydınlatma ve güç aktarım ekipmanları, endüstriyel yapılarda yangın başlangıcında öne çıkan ekipman grubu olarak gösteriliyor. Dijital izleme; koruma sistemlerinin, periyodik bakımın veya termal kontrolün yerine geçmez. Ancak akım, sıcaklık, harmonik, gerilim olayı ve alarm trendlerini görünür hâle getirerek anormalliğin daha erken fark edilmesini sağlar.

Saha verisi neyi değiştirir?



Yakın dönemde gerçekleştirdiğimiz kritik altyapı uygulamalarından birinde, ölçüm sonuçları UPS tarafından beslenen yüklerde yüksek akım harmonikleri ve belirgin faz akımı dengesizliği olduğunu gösterdi. Ölçüme dayalı olarak seçilen aktif harmonik filtre sonrasında akım harmonik bozulumu yaklaşık yüzde 60'tan yüzde 14'e, faz akımı dengesizliği yüzde 27,3'ten yüzde 2,6'ya geriledi; güç faktörü 0,970 ve $\cos\phi$ 0,997 seviyesinde ölçüldü.

Bu örneğin asıl mesajı belirli bir ürün değildir. Ölçüm yapılmadan sorunun kaynağı ve çözüm kapasitesi doğru belirlenemezdi; uygulama sonrasında tekrar ölçüm yapılmadan da yatırımın etkisi kanıtlanamazdı. Sürekli izleme eklendiğinde ise aynı sistem, yeni yükler devreye girdikçe bozulmayı erken fark eden bir işletme aracına dönüşür. Elektrik altyapısının “röntgenini çekmek” olarak gördüğümüz güç kalitesi ölçümü, bu nedenle dijital dönüşümün güçlü başlangıç noktalarından biridir.



Sonuç: Görünmeyi yönetemeyiz

Elektrik enerjisinde dijital dönüşüm büyük ölçekli bir yazılım projesiyle başlamak zorunda değildir. Kritik noktalara doğru dijital ölçüm cihazlarını yerleştirmek, veriyi ortak bir sistemde toplamak ve anlamlı alarmlar tanımlamak çoğu tesis için güçlü bir başlangıçtır. Çünkü aylık faturada görünmeyen bir 200 milisaniyelik gerilim çökmesi üretim hattını durdurabilir; artan harmonikler bir transformatörü veya nötr iletkeni gereksiz yere ısıtabilir; faz dengesizliği motorların ömrünü kısaltabilir. Görünür olmayan bu olaylar ölçülmediğinde çoğu zaman arıza gerçekleştikten sonra fark edilir.

Bu nedenle başarı göstergesi kurulan cihaz sayısı değil; erken fark edilen risk, önlenen duruş, azaltılan kayıp ve doğrulanabilen iyileşmedir. Elektrik mühendisinin rolü de yalnızca cihaz seçmek veya bağlantı yapmak değil; hangi verinin neden ölçüleceğini belirlemek, veriyi doğru yorumlamak ve sonucu güvenli bir aksiyona dönüştürmektir. Ölçmeden göremeyiz, izlemeden yönetemeyiz; dijital dönüşümün gerçek değeri de tam olarak burada başlar.

Emre AKÇİN

Elektrik Mühendisi, Exmas Energy Yönetici Ortağı

Kaynakça

- *International Energy Agency (IEA). (2025). World Energy Investment 2025.*
- *U.S. Department of Energy, Advanced Manufacturing Office. AMO eGuide: Measure, Monitor and Analyze Performance Metrics.*
- *NFPA Research. (2023). Fires in Industrial and Manufacturing Properties.*
- *IEC 61557-12:2018+A1:2021. Power Metering and Monitoring Devices (PMD).*
- *IEC 62586-1:2017. Power Quality Instruments (PQI).*
- *TS EN 50160; IEC 61000-4-30; IEEE Std 519-2022.*
- *Schneider Electric. The Seven Types of Power Problems. White Paper.*

EEMKON 2027 HAZIRLIK ÇALIŞMALARI VE KATILIM ÇAĞRISI



Değerli Meslektaşlarımız, Sevgili EMO Üyeleri,

TMMOB Elektrik Mühendisleri Odası tarafından gelenekselleşen ve vizyoner bakış açısıyla sektöre yön veren EEMKON 2027'nin (Elektrik Elektronik Mühendisliği Kongresi) düzenlenmesi görevi EMO İstanbul Şubemize verilmiştir.

EEMKON Kongresi 2015, 2017, 2019 ve 2026 yıllarında yapılmış, yaklaşık 10.000 kişi izlemiştir. 2019 yılından sonra **pandemi nedeniyle** bir süre ara verilmiştir. Kongre hazırlıkları için çalışmalarımız hız kesmeden devam ediyor.

Üniversiteler, Sanayi, Kamu Kurumları, Sektör Kuruluşları, Mesleki Dernekler, Meslek Odaları temsilcilerinin yer alacağı Kongre'nin amacı; dünyada ve ülkemizde hızla gelişen elektrik, elektronik, elektronik haberleşme, kontrol ve otomasyon, biyomedikal ve tıp mühendisliği alanlarındaki yenilikleri paylaşmak, irdelemek ve geleceğe ilişkin politikaları tartışmaktır. Bildiri oturumları ile akademik çalışmaların kongrede yer almasını ve yayınlanmasını sağlamaktır.

Kongre formatında çeşitli oturumlar, bildiri oturumları, yurt içi ve yurt dışından davetli konuşmacılar, sergi alanları ve sosyal etkinlikler bulunmaktadır.

Kongremize katılım için vereceğiniz destek, mesleğimizin olduğu kadar ülkemizin bilim ve teknoloji alanlarındaki birikimi güncelleyerek geliştirmeye, zenginleştirmeye yapacağı katkı açısından da önem taşımaktadır. **Aralık 2027** tarihinde gerçekleştireceğimiz kongremizin başarıya ulaşması, siz değerli üyelerimizin akademik, sektörel ve entelektüel katkılarıyla mümkün olacaktır.

Kongremiz kapsamında eş zamanlı olarak düzenlenecek 7 ana sempozyum ve kapsamları şu şekildedir:

◆ **A. Biyomedikal Mühendisliği Sempozyumu (Biomedical Engineering Symposium):** Tıbbi cihazlar, biyomedikal sinyal işleme, giyilebilir teknolojiler, sağlıkta yapay zeka.

◆ **B. Kent - Elektrik ve Deprem Sempozyumu (Urban Infrastructure Electricity and Earthquake Resilience Symposium):** Akıllı şehirler, enerji dayanıklılığı, afet yönetimi, kentsel altyapı, mikro şebekeler.

◆ **C. Yapay Zeka Sempozyumu (Artificial Intelligence Symposium):** Makine öğrenmesi, derin öğrenme, endüstride AI uygulamaları, büyük veri, etik ve mevzuat.

◆ **D. Elektronik ve Haberleşme Teknolojileri Sempozyumu (Electronics and Telecommunications Technologies Symposium):** Yarıiletkenler, 5G/6G, uydu haberleşme, IoT, siber güvenlik, savunma elektroniği.

◆ **E. Kontrol ve Otomasyon Teknolojileri Sempozyumu (Control and Automation Technologies Symposium):** Güç elektroniği, robotik, e-mobilite, endüstri 4.0/5.0, dijital ikiz, akıllı üretim.

◆ **F. Enerji Politikaları Sempozyumu (Energy Policy Symposium):** Enerji dönüşümü, yenilenebilir enerji, enerji depolama, hidrojen, karbon piyasası, mevzuat.

◆ **G. Mühendislik Eğitimi Sempozyumu (Engineering Education Symposium):** Mühendislik müfredatları, Yapay Zeka destekli eğitim, yetkinlikler, üniversite-sanayi iş birliği, kadın mühendisler.

Yürütülen diğer organizasyonel süreçlerin öne çıkan başlıkları ise şöyledir:

◆ **Akademik Bildiri Süreçleri:** Kongremizin bilimsel niteliğini en üst düzeyde tutmak amacıyla, gönderilecek tüm bildiriler çift kör hakem (double-blind peer review) sistemiyle objektif bir değerlendirmeden geçecektir. Özgün araştırmalarınızı ve saha deneyimlerinizi paylaşmanız için bildiri gönderim takvimi yakında ilan edilecektir.

◆ **Endüstriyel İş Birlikleri ve Sponsorluk:** Sektörün lider firmalarını ve yenilikçi start-up'ları bir araya getirecek sponsorluk çalışmalarımız olacaktır. Kurumlarınızın Ar-Ge çıktısını ve sektörel gücünü kongre fuaye alanında sergilemek için komitemizle iletişime geçebilirsiniz.

◆ **Davetli Konuşmacılar ve Paneller:** Küresel ölçekte tanınan akademisyenler ve endüstri liderlerinin yer alacağı Keynote oturumları ile sektörel dönüşümün tartışılacağı geniş katılımlı paneller planlanmaktadır.

◆ **Sektörel Oturumlar:** Sanayi ve kamu temsilcilerinin yer alacağı özel oturumlardır. Amaç akademi-sanayi arasındaki bilgi ve teknoloji transferini hızlandırmaktır.

Mühendislik dünyasının bu büyük buluşmasında yer almak, bildiri sunmak veya organizasyon komitelerinde görev alarak katkı koymak isteyen tüm üyelerimizi **EEMKON 2027 çalışma gruplarına katılmaya davet ediyoruz.**

Kongre detayları, bildiri kılavuzu ve güncel duyurular için eemkon.org.tr adresini ziyaret edebilirsiniz.

Saygılarımızla,

İsa GÜNGÖR

EEMKON 2027 Düzenleme Kurulu Başkanı

ÜCRETLİ ÇALIŞAN VE İŞSİZ MÜHENDİSLER KOMİSYONU



Mühendisler, üretim süreçlerinin teknik ve bilimsel faaliyetlerinden sorumlu, toplumun ihtiyaçlarının karşılanmasında önemli rol üstlenen uzmanlık sahibi çalışanlardır. Ancak mühendislerin üretim sürecindeki konumu, sahip oldukları mesleki bilgi ve uzmanlıktan bağımsız olarak çalışma ilişkileri tarafından belirlenmektedir. Kamu veya özel sektörde ücret karşılığında çalışan mühendisler, toplumsal sınıflar içerisindeki konumları bakımından işverenlerinden ayrılmakta; işyerindeki ve işyeri dışındaki koşulları, sorunları ve talepleri bu çalışma ilişkileri çerçevesinde şekillenmektedir. Üretim sürecinin dışında kalan işsiz mühendisler ise ekonomik ve sosyal sorunlarla karşı karşıya olup koşulları, sorunları ve talepleri bakımından ücretli çalışan mühendislerle ortaklaşmaktadır.

Düşük ücretler, uzun çalışma saatleri, fazla mesai, güvencesiz çalışma, mobbing, üretim kapasitesi ve insan gücüyle orantısız biçimde belirlenen proje ve iş yükleri, işyerlerinde yeterli teknik ve idari desteğin sağlanmaması, mesleki bilgi ve deneyimin karşılığının alınamaması ve taşeronlaşmayla birlikte derinleşen çalışma sorunları, ücretli çalışan mühendislerin çözüm bekleyen başlıca sorunlarıdır. Bunun yanında binlerce elektrik elektronik mühendisi ve alanla ilişkili mühendis, işsizlik ve güvencesizlik koşullarında giderek yoksullaşmakta, mesleğini güvenceyle sürdürebileceği bir çalışma olanağı aramaktadır.

Elektrik Mühendisleri Odası Ücretli Çalışan ve İşsiz Mühendisler Komisyonu olarak ürettiğimiz ve geliştireceğimiz politikaların temel amacı; mühendislerin insanca yaşam ve çalışma koşullarına kavuşması, emeğinin karşılığını alması, mesleki haklarının korunması ve işsiz mühendislerin güvenceli istihdama erişebilmesidir.

Bu politikaların hayata geçirilebilmesinin en temel koşulu ise yaşadığı sorunların farkında olan, haklarından vazgeçmeyen ve bu sorunları ortadan kaldırmak için ortak bir irade ortaya koyabilen mühendislerin örgütlü gücünü yaratmaktır.

Kamu yararını temel alan bir meslek odasının görevi yalnızca mesleki standartları ve üyelerinin mesleki haklarını korumakla sınırlı değildir. Meslek alanına ilişkin bilimsel ve teknik bilgi birikimini toplumun yararına sunmak; güvenli, sağlıklı ve nitelikli üretim ve hizmet koşullarını savunmak; kamusal kaynakların ve emeğin toplum yararına kullanılmasını gözetmek; özelleştirme, taşeronlaşma ve güvencesizleştirme politikalarının yarattığı sonuçlara karşı çıkmak; enerji, iletişim, teknoloji ve altyapı gibi alanlarda toplumun eşit ve nitelikli hizmetlere erişimini savunmak da meslek odasının kamusal sorumluluğunun parçasıdır. Bu nedenle mühendislerin çalışma ve yaşam koşullarının iyileştirilmesi, aynı zamanda toplumun güvenli, nitelikli ve kamu yararını gözetken mühendislik hizmetlerine erişmesinin de koşuludur.

Elektrik Mühendisleri Odası, kamu yararı ve emekten yana yaklaşımı doğrultusunda, ücretli çalışan ve işsiz mühendislerin ortak sorunları etrafında örgütlenebileceği güçlü ve etkin bir alan yaratmalıdır. Ücretli Çalışan ve İşsiz Mühendisler Komisyonu bu bir araya gelişin araçlarından biridir. Komisyon; mühendislerin sorunlarını görünür kılan, ortak talepleri geliştiren, çalışma yaşamına ilişkin politikalar üreten ve bu politikaların hayata geçirilmesi için örgütlü mücadeleyi büyüten bir anlayışla çalışmalarını sürdürmelidir. Mühendislerin emeğine, mesleğine ve geleceğine sahip çıkması; meslek odasının da kamu yararını önceleyen, emekten yana ve toplumcu bir mühendislik anlayışını güçlendirmesiyle mümkündür.

Şakir Ardıl ACAR
45. Dönem Ücretli Çalışan
ve İşsiz Mühendisler Komisyonu Başkanı

KURUMSAL YAPAY ZEKA DÖNÜŞÜMÜNDE ADRESLENMESİ GEREKEN 6 ALAN

Şirketler yapay zeka (YZ) projelerine başlarken çoğunlukla teknoloji seçimine odaklanıyor; oysa dönüşümün başarısını asıl belirleyen unsurlar çoğu zaman teknik değil, kurumsal ve hukuki niteliktedir. Uzunca bir süredir YZ geliştiren firmalardan aldığımız geri bildirimlerle bu alanları EMO olarak 6 başlıkta derledik.

Veri Egemenliği

“Verimle rekabeti mi eğitiyorum?”

YZ sistemlerinin performansı, beslendiği veriyle de orantılıdır; ancak bu veri kimin mülkiyetinde ve kimin erişimine açık olacaktır? Kurumsal verinin üçüncü taraf bulut servislerine gönderilmesi, rekabet avantajı taşıyan bilginin şirket dışına çıkması riskini doğurur. Hangi verinin dışarıda işlenebileceği, hangisinin şirket sınırları içinde (yerinde sunucu veya özel bulut) kalması gerektiği konusunda net bir tasnif yapılmalıdır. Hibrit mimari tercih edilirse hassas veri kurum içinde tutulurken, daha az kritik iş yükleri dış servislerden faydalanabilir.

Veri egemenliği yalnızca teknik bir konumlandırma sorunu değil, aynı zamanda bir risk yönetimi kararıdır ve sözleşme, denetim ve ihlal bildirim süreçlerini de kapsayacak şekilde tasarlanmalıdır. Ayrıca hangi sağlayıcının verileri model eğitiminde kullanıp kullanmadığı, verinin ne kadar süreyle saklandığı ve silme talebinin nasıl işleneceği ve bunların nasıl belgelendirileceği gibi sorular, tedarikçi seçiminin bir parçası olarak sözleşme öncesinde netleştirilmelidir.

Yönetişim

“Şirketimin maaş politikası nedir?” sorusunun cevabını, ortalama bir çalışan, üst kademe bir yönetici ve İK müdürü farklı almalıdır.

Yapay zeka sistemlerine kimin, hangi yetkiyle, hangi bilgiye erişebileceği sorusu, organizasyon şemasının dijital bir yansımasını gerektirir. Etkili bir yönetim modeli; rol bazlı erişim kontrolü (İng. : RBAC) , denetim izleri (İng. : audit trail) ve onay mekanizmalarını içerir. Yönetişim eksikliği kısa vadede hızlı sonuç üretse de, orta vadede veri sızıntısı, yanlış bilgi üretimi (halüsinasyon) ve hesap verebilirlik sorunlarına yol açar. Yönetişim, projeye sonradan eklenecek bir katman değil, mimarinin başlangıç noktası olmalıdır.

Yasalar

“Yaptığım projeler, YZ düzenlemesi gelince, bana geriye dönük bir borç yükü oluşturacak mı?”

Düzenleyici çerçeve yeterince hızla şekillenmiyor. Gerçi Avrupa Birliği'nin Yapay Zeka Yasası (EU AI Act) kademeli olarak yürürlüğe giriyor: yasaklı uygulamalar ve okuryazarlık yükümlülükleri Şubat 2025'ten, genel amaçlı yapay zeka modellerine ilişkin kurallar Ağustos 2025'ten itibaren uygulanıyor; şeffaflık yükümlülükleriyle birlikte düzenlemenin büyük bölümü 2 Ağustos 2026 itibarıyla yürürlüğe girdi, [1] ancak ABD ve Çin'de bu tür denetimler/yönetmelikler yeterince belirgin değil.

Türkiye'deyse yapay zekâya özgü, yürürlükte tek bir kanun henüz bulunmuyor; düzenleme bugün itibarıyla Kişisel Verilerin Korunması Kanunu (6698 sayılı), Türk Ceza Kanunu ve 5651 sayılı İnternet Kanunu gibi mevcut mevzuatın yapay zekâ bağlamına uyarlanmasıyla sağlanıyor, meclise sunulan kanun teklifleri ise henüz komisyon aşamasında.[2] Türkiye'nin daha önce KVKK konusunda AB GDPR çerçevesini esas aldığı ve EU AI Act'ın halen en detaylı çerçeve olduğu düşünülecek olursa, yapılacak yatırımın bu çerçeveye uygun olması önemli olacaktır.

Platform Döngüsü – Güncelliği Yakalamak

“Her gün yeni model ve donanım çıkıyor. Nasıl izleyeceğim? İzlemeli miyim?”

YZ modelleri ve araçları birkaç ayda bir köklü değişim geçiriyor. Belirli bir modele veya sağlayıcıya sıkı sıkıya bağlanan mimariler, bir yıl içinde teknik ve mali borca dönüşebilir. Bunun yerine model ve sağlayıcı bağımsız bir katman tasarlamak; iş mantığını, veriyi ve entegrasyonları belirli bir modelden ayırştırmak, hem maliyet optimizasyonu hem de en güncel yeteneklere erişim açısından esneklik sağlar. SaaS modelinde KVKK'ya uygun sağlayıcılar ile çalışmak esnek ve güvenli bir alan yaratabileceği düşünülmelidir.

Maliyet

**“Dün 100 token karşılığında 10 iş yaptırırken
bugün 5 işe düştü. Proje kaçta çıkacak?”**

Üstelik, YZ projelerinde maliyet yalnızca model kullanım giderlerinden ibaret de değildir; veri hazırlama, entegrasyon, güvenlik katmanları, izleme ve sürekli bakım, toplam sahip olma maliyetinin büyük bölümünü oluşturur. Pilot aşamada düşük görünen bir maliyet kalemi, ölçeklenme sonrası kat kat büyüyebilir. Bu nedenle yatırım kararı; birim işlem başına maliyet, kullanıcı başına maliyet ve süreç başına elde edilen zaman ve kalite kazanımı üzerinden karşılaştırmalı olarak modellenmelidir. Farklı model sağlayıcıları arasında fiyat/performans karşılaştırması yapabilen, iş yüküne göre daha ucuz veya daha güçlü yapıya yönlendirme yapabilen bir mimari, sabit tek sağlayıcı yapılarla kıyasla belirgin bir maliyet avantajı sunar.

Proje Önceliklendirme

Çoğu şirket, YZ dönüşümüne veri ve süreç olgunluğu açısından hazır değil; bu nedenle "her yerde birden" başlamak yerine, ölçülebilir etkisi yüksek, veri kalitesi görece iyi ve organizasyonel direnci düşük bir alanda başlamak daha isabetlidir.

Önceliklendirme için iş-etki/maliyet analizi yapacak bir danışmanlık almak, hangi parametrelerin daha baskın olması gerektiği konusunda bir farkındalık sağlayacak en kritik yönetsel etkinliktir.

Sonuç olarak, YZ dönüşümü teknoloji seçiminden önce veri, yetki, hukuk, platform stratejisi, maliyet modeli ve önceliklendirme konusunda net bir yol haritası gerektirir. Bu altı alanda erken netlik sağlayan kurumlar, dönüşümü geçici bir proje olmaktan çıkarıp sürdürülebilir bir yetkinliğe dönüştürür.

Sinan KEZER
Elektrik Elektronik Mühendisi

Dipnotlar

- [1] Avrupa Komisyonu / [artificialintelligenceact.eu](https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1714), "AI Act Uygulama Takvimi", 2026.
- [2] Sanal Hukuk, "Yapay Zeka Hukuku 2026: Türkiye'de Güncel Durum ve Kapsamlı Rehber", Temmuz 2026. <https://sanalhukuk.org/yapay-zeka-hukuku-rehber/>

YAPAY ZEKA GÜVENLİĞİ VE YAPAY ZEKANIN OLUŞTURDUĞU RİSKLER

Yapay zeka, son birkaç yıl içinde deneysel bir teknolojiden, kurumların günlük operasyonlarının, ürünlerinin ve karar süreçlerinin merkezine yerleşen bir altyapı unsuruna dönüştü. Bu dönüşüm beraberinde yeni bir risk kategorisi getirdi: yapay zeka güvenliği. Bu alan artık ne salt bir akademik araştırma konusu ne de yalnızca teknoloji şirketlerini ilgilendiren dar bir uzmanlık alanı; bugün bir bankanın kredi değerlendirme sistemini, bir hastanenin teşhis destek yazılımını, bir çağrı merkezinin otonom asistanını ve bir yazılım şirketinin kod üretim araçlarını aynı anda ilgilendiren, kurumsal risk yönetiminin ayrılmaz bir parçası haline geldi.

Kuruluşlar büyük dil modellerini (LLM'ler) ve otonom yapay zeka ajanlarını üretim sistemlerine entegre etmek için yarışırken, saldırı yüzeyi çoğu güvenlik programının uyum sağlayabileceğinden daha hızlı değişmektedir. Yapay zeka güvenliği artık niş bir araştırma konusu değil; uygulama güvenliği, veri yönetimi ve çatışmalı (adversarial) makine öğrenmesinin kesişiminde yer alan temel bir disiplin haline gelmiştir.

Bu yazıdaki hedefimiz, hem teknik ekiplerin hem de konuya teknik olmayan bir bakış açısıyla yaklaşan okuyucuların takip edebileceği bütünlüklü bir çerçeve sunmak.

Genel Bakış: Neden Şimdi ve Neden Bu Kadar Önemli?

Geleneksel siber güvenlik; ağlar, sunucular, uygulamalar, kullanıcı kimlik bilgileri gibi belirli nispeten öngörülebilir bir saldırı yüzeyi üzerine kuruluydu. Yapay Zeka sistemleri -özellikle büyük dil modelleri ve bu modeller üzerine inşa edilen otonom ajanlar- bu saldırı yüzeyini iki yönde birden genişletti.

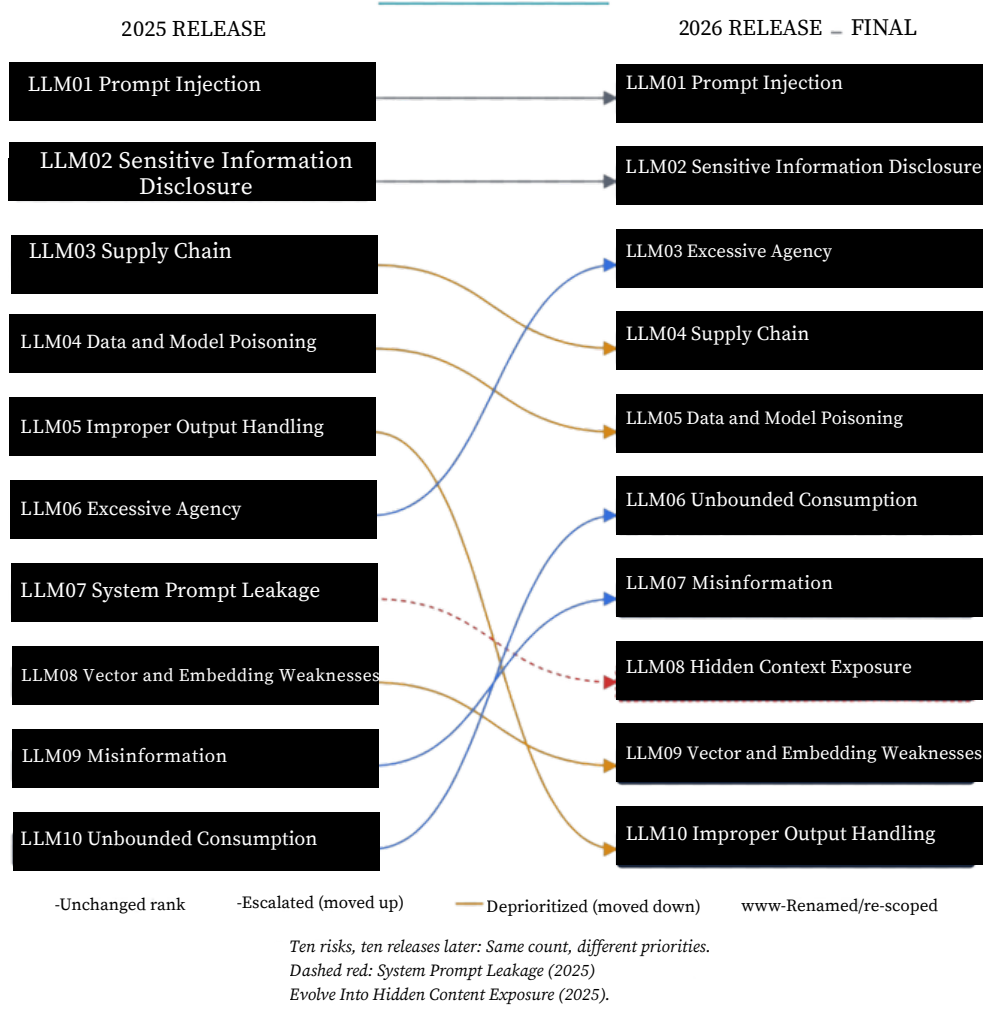
- ◆ **Birincisi, modellerin kendisi artık bir saldırı hedefi:** Yapay Zekadaki eğitim verisi, model ağırlıkları, sistem promptları ve modelin ürettiği çıktılar başlı başına değerli ve savunulması gereken varlıklar haline geldi.
- ◆ **İkincisi, bu modeller artık yalnızca metin üretmiyor:** Yapay Zeka e-posta gönderiyor, kod çalıştırıyor, veri tabanlarına erişiyor, ödeme işlemlerini tetikliyor. Yani bir güvenlik açığının sonucu artık “yanlış bir cevap” değil, gerçek dünyada geri alınamaz bir eylem olabiliyor.

Dolayısıyla yapay zeka güvenliğini anlamanın ilk adımı, bu sistemlerin *hem korunması gereken* varlıklar hem de *potansiyel saldırı araçları* olduğunu kabul etmektir.

OWASP GenAI Security Project'in 2026 yılında yayımladığı LLM/GenAI İlk 10 listesi, bu değişimi somut biçimde ortaya koyuyor. Liste ilk kez yalnızca uzman görüşüne değil, kamuya açık güvenlik açığı veri tabanlarından ve bir yapay zeka zarar veri tabanından derlenen 6.639 gerçek dünya olayına da dayandırıldı (değerlendirmelerde uzman görüşü %75, gerçek olay verisi %25 ağırlıkla). Bu, listenin artık teorik risklerden değil, fiilen istismar edilmiş zayıflıklardan oluştuğu anlamına geliyor.

Aşağıdaki resim Yapay Zeka tehdit sırasının gerçek dünya olaylarının da göz önüne alındığında 2025 yılından 2026 yılına nasıl değiştiğini göstermektedir

OWASP GenAI/LLM Top 10 (2025 2026): Rank Migration Bump Chart



Listenin arkasındaki felsefi çerçeve de dikkat çekici: OWASP, “hiçbir zaman kandırılmayacak bir model” hedefinin gerçekçi olmadığını, bunun yerine modelin çevresindeki sistemin, model kandırıldığında (ki kandırılacaktır) hiçbir kritik şeyin bozulmayacağı şekilde tasarlanması gerektiğini savunuyor. Bu, güvenlik camiasında “önleme” odaklı yaklaşımdan “hasar yarıçapını (blast radius) sınırlama” odaklı yaklaşıma geçişin bir yansımasıdır.

LLM’e Özgü Tehditler: Modelin Kendisi Saldırı Yüzeyi Haline Geldiğinde

Büyük dil modelleri, geleneksel yazılımlardan temelde farklı bir şekilde çalışıyor: talimatları ve kullanıcı girdisini net biçimde ayıramıyorlar, çünkü ikisi de aynı “bağlam penceresi” içinde doğal dil olarak işleniyor. Bu mimari özellik, LLM’lere özgü, geleneksel uygulama güvenliğinde karşılığı olmayan bir dizi tehdit doğuruyor. Aşağıda kısaca OWASP tarafında belirtilen bu riskleri incelemeye çalıştık.

Prompt injection (istem enjeksiyonu), üçüncü yıldır OWASP listesinin zirvesinde. Doğrudan yapılan saldırıda , bir kullanıcı modeli kandırıp güvenlik kısıtlarını aşmasını sağlayabilir (“jailbreak” olarak da bilinir). Daha tehlikeli olan ise dolaylı prompt injection: bu durumda saldırgan, modelin daha sonra okuyacağı bir belgeye, e-postaya veya web sayfasına gizli talimatlar yerleştirir; model bu içeriği “veri” olarak değil “talimat” olarak yorumlayıp saldırganın istediğini yapabilir. Bir müşteri, hiçbir şeyden habersiz şekilde bir web sitesini özetlemesini yapay zekadan istediğinde, o sitede gizlenmiş bir talimat modelin gizli verilerinin saldırgana göndermesine yol açabilir.

Hassas bilgi ifşası, listenin ikinci sırasında yer alıyor. Modeller, sistem promptlarını, eğitim verisinden sızan parçaları veya bağlı araçlardan (örneğin bir CRM ya da e-posta sistemi) alınan bağlamı, doğru şekilde sorgulandığında ifşa edebiliyor. Bu, özellikle şirket içi verilerle ince ayar yapılmış veya RAG (retrieval-augmented generation, gerialma/geribesleme ile zenginleştirilmiş üretim) mimarisiyle çalışan modellerde ciddi bir sızıntı kanalı oluşturuyor.

2026 listesindeki yeni maddeler, LLM uygulamalarının sohbet botu aşamasını geride bıraktığını gösteriyor.

- ◆ **Sistem promptu sızıntısı:** Geliştiricilerin model davranışını sınırlamak için kullandığı gizli talimatların açığa çıkması, saldırganlara modelin nasıl “kırılabilceğine” dair doğrudan bir yol haritası veriyor.
- ◆ **Vektör ve gömme (embedding) zayıflıkları:** RAG mimarilerine özgü bir risk. Zehirlenmiş veya manipüle edilmiş gömme vektörleri, modelin hangi bağlamı getireceğini yönlendirerek yanlış veya kötü niyetli içeriğin “güvenilir kaynak” gibi sunulmasına yol açabiliyor.
- ◆ **Aşırı özerklik (excessive agency):** Bir ajanın gerçekleştirmesine izin verilen eylemlerin, görevi için gerçekte ihtiyaç duyduğundan daha geniş olması. Bir e-posta özetleyen ajanın aynı zamanda e-posta silme veya para transferi yapma yetkisine sahip olması, tek bir başarılı enjeksiyonun felakete dönüşmesine izin verir.

Bu risklerin ötesinde, klasik makine öğrenmesinden miras kalan tehditler de LLM’ler için geçerliliğini koruyor. **Veri zehirlenmesi**, bir modelin eğitim ya da ince ayar verisine kasıtlı olarak bozuk örnekler eklenerek, yalnızca belirli tetikleyicilerle etkinleşen bir “arka kapı” davranışı kazandırılmasıdır; bu, halka açık veri kümeleri veya taranan web içerikleri üzerinden sessizce gerçekleşebilir. **Model çıkarımı/hırsızlığı**, tekrarlanan API sorgularıyla bir modelin davranışının veya parametrelerinin yeniden inşa edilmesidir; bu, rakiplerin tescilli bir modeli “kopyalamasına” imkân tanıyabilir. **Çekişmeli örnekler** ise, insan gözüyle fark edilmeyecek küçük değişikliklerle bir modelin yanlış sınıflandırma yapmasına neden olan girdilerdir ve özellikle içerik moderasyonu veya güvenlik filtrelerini atlatmak için kullanılabilir.

Ajan Tabanlı Yapay Zeka: Yeni Bir Risk Kategorisi

Otonom, araç kullanan yapay zeka ajanlarının yükselişi, mevcut yönetim çerçevelerinin yetersiz kalmasına neden olmaktadır. Ajan tabanlı (agentic) sistemlerin yaygınlaşması bu tabloyu daha da karmaşıklştırıyor. OWASP'ın Aralık 2025'te yayımladığı Ajan Tabanlı Uygulamalar için İlk 10 listesi, **hedef ele geçirme** (bir saldırganın ajanın görevinin ortasında yeniden yönlendirmesi) ve **“sahtekâr ajanlar”** (yetki kapsamı içinde teknik olarak çalışırken sessizce zararlı bir amacı takip eden ajanlar) gibi yeni kavramlar tanımlıyor.

Pratikte, 2026'nın baskın saldırı örüntüsü şu üçlüde toplanıyor: giriş noktası olarak **prompt injection**, aşırı geniş araç izinlerinden doğan **aşırı özerklik** ve meşru görünen araç çağrılarını üzerinden gerçekleştirilen **veri sızdırma**. Ajanlar birden fazla aracı zincirleyip insan onayı olmadan hareket edebildiğinden, tek bir başarılı enjeksiyon; yetkisiz işlemlere, veri kaybına veya bağlı sistemler arasında yanal harekete dönüşebiliyor -ve bu, günlük kayıtlarında sıradan bir ajan davranışı gibi görünüyor.

Kurumsal ve İş Riski: Yönetişim, Uyumluluk ve Tedarikçi Riski

Yapay zekanın kurumlar için oluşturduğu risk yalnızca teknik bir mesele değil; aynı zamanda bir yönetim, hukuki uyumluluk ve tedarik zinciri sorunu. Bugün kurumsal yapay zeka yığınlarının büyük çoğunluğu sıfırdan inşa edilmiyor, farklı sağlayıcılardan alınan model, API ve araçların bir araya getirilmesiyle oluşuyor. Bu da **“üçüncü taraf yapay zeka riski”** adı verilen yeni bir kategori doğurdu: bir kurum kullandığı modeli kendisi eğitmemiş olsa bile, o modelin ürettiği sonuçlardan hukuken ve operasyonel olarak sorumlu tutulabiliyor.

Bunun en somut örneği AB Yapay Zeka Yasası (EU AI Act). Yasa, “dağıtıcı” (deployer) yükümlülüklerini açıkça tanımlıyor: yüksek riskli bir yapay zeka sistemini kullanıma sunan kurum, o sistemin altyapısını kendisi geliştirmemiş olsa dahi uyumluluk yükümlülüğünü taşıyor. Ağustos 2026'da yüksek riskli sistemler için tam uyumluluk tarihi yaklaşıyor ve uyumsuzluk durumunda cezalar küresel cironun %7'sine veya 35 milyon avroya kadar çıkabiliyor. Bu ölçekteki bir yaptırım riski, yapay zeka yönetişimini artık BT departmanının değil, üst yönetimin ve hukuk biriminin gündemine taşıyor.

NIST Yapay Zeka Risk Yönetimi Çerçevesi'ni (AI RMF) üçüncü taraflar için uygulayan kurumların, AB Yapay Zeka Yasası'nın gerektirdiği temelin %60-70'ine zaten sahip olduğu değerlendiriliyor; ISO/IEC 42001:2023 standardı ise sertifikalandırılabilir bir Yapay Zeka Yönetim Sistemi (AIMS) çerçevesi sunuyor.

Türkiye'deki mevcut yasalar ve yapay zeka ile ilgili düzenlemeler

Türkiye'de yapay zeka konusunda ayrılmış, kapsamlı bir "yapay zeka kanunu" henüz yürürlüğe girmedir. Bunun yerine mevcut kanunların Yapay Zeka'ya uygulanması, birkaç TBMM'ye sunulmuş ama henüz kabul edilmemiş kanun teklifi, ve resmi bir ulusal strateji/eylem planı gibi dağınık bir yapı var.

Yapay Zeka sistemleri kendine özgü bir kanun yerine amacına ve verisine göre mevcut çerçevelere tabi. Kişisel veri işleyen Yapay Zeka uygulamaları için 6698 sayılı KVKK geçerli; KVKK ayrıca "15 Soruda Üretken Yapay Zeka ve Kişisel Verilerin Korunması Rehberi" adıyla bağlayıcı olmayan ama yol gösterici bir kılavuz yayımladı. Yapay Zeka üretimi içerikler (özellikle deepfake ve dezenformasyon) için 5651 sayılı İnternet Kanunu devreye giriyor. Yakın zamanda çıkan 32846 sayılı Siber Güvenlik Kanunu, kritik altyapıda veya bilgi sistemlerinde çalışan Yapay Zeka sistemlerine güvenlik ve olay bildirimi yükümlülükleri getiriyor. Bunların dışında ceza hukuku, 6502 sayılı Tüketicinin Korunması Hakkında Kanun ve genel ürün sorumluluğu hükümleri de AI kaynaklı zararlarda uygulanabiliyor.

Aralık 2025'te Kamu Yapay Zeka Genel Müdürlüğü kuruldu ve Siber Güvenlik Başkanlığı'nın yetkileri yeniden düzenlendi; bu kurumlar kamuda Yapay Zeka kullanımı ve güvenliği konusunda merkezi rol üstleniyor. Ulusal Yapay Zeka politikasının koordinasyonunu ise Sanayi ve Teknoloji Bakanlığı yürütüyor; sektörel alanlarda (finans, sağlık, veri koruma) ilgili düzenleyici kurumlar da kendi alanlarında Yapay Zeka'yı denetliyor.

TBMM'ye 2024-2025 arasında üç ayrı yapay zeka ile ilgili kanun teklifi sunuldu, hiçbirisi henüz yasalaşmadı:

- **25 Haziran 2024 tarihinde Ömer Faruk Gergerlioğlu** tarafından AB Yapay Zeka Yasası'na benzer, risk temelli, kapsamlı ve müstakil bir YAPAY ZEKA kanunu önerildi. Yasa önerisi "YAPAY ZEKA operatörleri" tanımı, ihlallere göre kademeli para cezaları (yanlış bilgi için 7,5 milyon TL'ye, yasaklı uygulamalar için 35 milyon TL'ye kadar) içeriyor.
- **10 Kasım 2025 tarihinde Halil Öztürk** tarafından yeni bir kanun yerine beş mevcut kanunda değişiklik önerildi. Yasal öneri deepfake içeriklerin etiketlenmesini zorunlu kılıyor, içerik sağlayıcı ve geliştiriciye müşterek sorumluluk getiriyor, 500 bin-5 milyon TL arası idari para cezası ve sistematik ihlallerde erişim engeli öngörüyor.
- **3 Aralık 2025 tarihinde İsmail Özdemir** tarafından daha dar kapsamlı bir yasa önerildi. Yasa önerisi İnternet Kanunu'nda değişikliklerle YAPAY ZEKA üretimi içeriklerde görünür "logo veya yazılı ibare" zorunluluğu getiriyor.

Hukukçular bu üç teklifin farklı felsefeler yansıttığını (kapsamlı risk bazlı düzenleme / hedefli içerik yönetimi / şeffaflık zorunluluğu) ve Türkiye'nin AB standartlarıyla uyumlu, tutarlı ve kapsamlı bir Yapay Zeka kanununa ihtiyacımız olduğunu vurguluyor.

Bu yıl Ağustos ayında (18 Ağustos 2026) Cumhurbaşkanlığı genelgesiyle Resmi Gazete'de yayımlanan Türkiye Yapay Zeka Eylem Planı (2026-2030), 2021-2025 Ulusal Yapay Zeka Stratejisi'nin devamı niteliğinde. Plan "Tespit Et, Fayda Sağla, Üret, Yönet" ilkeleri üzerine kurulu; insan merkezlilik, güvenilirlik, etik sorumluluk, dijital egemenlik ve sürdürülebilirlik vurgulanıyor. Sanayi ve Teknoloji Bakanlığı koordinasyonunda, kamu kurumları, özel sektör, üniversiteler ve sivil toplumun katılımıyla hazırlanmış olan eylem planı bağlayıcı bir kanun değil daha çok politika yol haritası niteliğinde.

Özetle: Türkiye'de şu anda yürürlükte bağlayıcı, kapsamlı bir yapay zeka kanunu yok. Yapay Zeka, KVKK, İnternet Kanunu ve Siber Güvenlik Kanunu gibi genel mevzuatla, KVKK'nın yumuşak hukuk niteliğindeki rehberleriyle ve yeni kurulan kamu Yapay Zeka kurumlarıyla yönetiliyor. Kapsamlı bir kanun için üç farklı teklif TBMM gündeminde bekliyor.

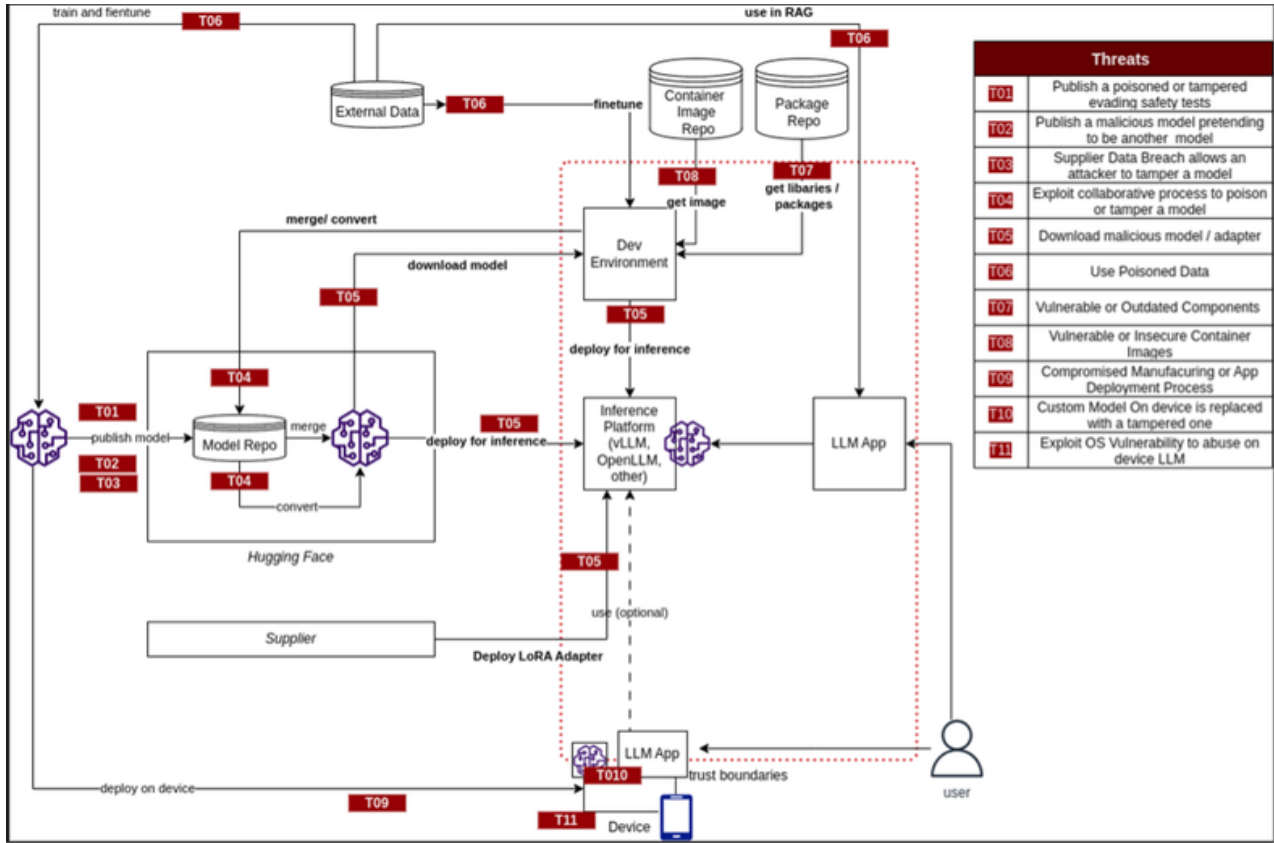
Yönetişim Geriden Yetişmeye Çalışıyor

Düzenleyici ve standart belirleyici kuruluşlar, ajan tabanlı yapay zeka dağıtımının hızının belirgin biçimde gerisinde kalıyor. 2026'nın başı itibarıyla, başlıca çerçevelerin hiçbiri - NIST Yapay Zeka Risk Yönetimi Çerçevesi, ISO/IEC 42001 veya AB Yapay Zeka Yasası- "ajan" veya "ajan tabanlı" sistemlere açık bir atıf içermiyor; bu da bu sistemlerin kağıt üzerinde nasıl yönetildiği ile üretimde fiilen nasıl çalıştığı arasında gerçek bir boşluk bırakıyor.

NIST bu boşluğu kapatmaya başladı. Şubat 2026'da, Yapay Zeka Standartları ve İnovasyon Merkezi (CAISI), dördüncü çeyrekte 2026'da yayımlanması hedeflenen bir Yapay Zeka Ajanı Birlikte Çalışabilirlik Profili ile birlikte Yapay Zeka Ajanı Standartları Girişimi'ni duyurdu. Bu arada, NIST'in daha geniş AI RMF (Risk Management framework) çalışması, temel, ilke düzeyinde rehberlikten daha operasyonel, sektöre özgü ve uygulamaya hazır kaynaklara doğru kaydı; bu da kuruluşların önümüzdeki yıl daha az değil, daha kuralcı beklentiler beklemesi gerektiğinin bir işareti.

Kurumsal risk yönetiminin ihmal ettiği bir diğer alan, çalışanların onay almadan kullandığı yapay zeka araçları: "gölge yapay zeka" (shadow AI). IBM'in 2025 Veri İhlali Maliyeti Raporu'na göre, ihlale uğrayan kuruluşların %20'si gölge yapay zeka üzerinden ele geçirildi ve bu olaylar ortalama ihlal maliyetine yaklaşık 670.000 dolar ekleyerek toplamı 4,63 milyon dolara çıkardı. Aynı raporda, yapay zeka kaynaklı bir ihlal yaşayan kuruluşların %97'sinin yeterli erişim kontrolüne sahip olmadığı, %63'ünün ise herhangi bir yapay zeka yönetim politikası bulunmadığı ortaya çıktı. Ankete katılan şirketlerin yalnızca %17'si, çalışanların gizli verileri kamuya açık yapay zeka araçlarına yüklemesini teknik olarak engelleyebiliyordu.

Tedarikçi yönetimi açısından da beklentiler değişiyor. Yapay zeka için OWASP tedarikçi yönetimi saldırı modeli aşağıda gösterilmiştir.



Yukarıdaki saldırı modeli incelendiğinde geleneksel tedarikçi güvenlik değerlendirmeleri -bir kerelik anketler, yıllık denetimler- yapay zeka tedarikçileri için yetersiz kaldığı görülmektedir. Çünkü bir modelin davranışı, altında yatan veri veya ince ayar güncellendiğinde sessizce değişebiliyor. Bu nedenle güncel yaklaşım, tedarikçi sözleşmelerine denetim hakları, şeffaflık yükümlülükleri ve net sorumluluk tanımları eklemeyi, ayrıca modelin doğruluğunda veya davranışında ani sapmaları tespit edecek sürekli izleme mekanizmalarını içeriyor olmalı.

Madalyonun öbür yüzünde ise somut bir iş gerekçesi var: yapay zeka yönetim çerçevelerine ve risk yönetimi araçlarına yatırım yapan kurumlar, tedarikçi kaynaklı olaylara %40 daha hızlı müdahale edebildiğini raporluyor. Yani yönetim, yalnızca bir uyumluluk maliyeti değil, aynı zamanda operasyonel dayanıklılığı artıran bir yatırım.

Özetle, kurumsal düzeyde yapay zeka riski üç eksende toplanıyor: *düzenleyici uyumluluk* (özellikle AB Yapay Zeka Yasası ve benzeri yaklaşan mevzuat), *iç yönetim boşlukları* (gölge yapay zeka, yetersiz erişim kontrolü) ve *tedarik zinciri şeffaflığı* (üçüncü taraf modellerin sürekli izlenmesi).

Katmanlı Bir Savunma Programı Kurmak

Hem olgunlaşan tehdit modelleri hem de yönetim boşluğu göz önüne alındığında, güvenlik ekipleri yapay zeka sistemlerine, ortamdaki yüksek değerli, yüksek hasar yarıçaplı başka herhangi bir bileşene davrandıkları gibi davranmalı:

- ◆ Sürekli, tek seferlik değil, kırmızı takım (red team) testleri yapılmalı. Etkili yapay zeka kırmızı takım çalışması tüm yaşam döngüsünü kapsar: tasarım aşamasında tehdit modellemesi, veri toplama sırasında zehirlenme testleri, eğitim sırasında çatışmalı dayanıklılık testleri, entegrasyonda API güvenlik testleri, üretim öncesinde tam kapsamlı kırmızı takım tatbikatları ve lansman sonrasında sürekli izleme ile olay müdahale tatbikatları.
- ◆ Yapay Zeka ajan özerkliği sınırlandırılmalı. Herhangi bir ajanın araç erişimine ve dosya izinlerine en az ayrıcalık ilkelerini uygulayın; modelin ne zaman yükseltme yapacağına dair kararına güvenmek yerine, sonuç doğuran veya geri alınamaz eylemler için insan onayı zorunlu kılın.
- ◆ Geribesleme/Geri alma (retrieval) hatlarını güvenilmeyen girdi olarak ele alınmalı. RAG sistemleri, model bağlamına ulaşmadan önce getirilen içeriği doğrulamalı ve arındırmalı; gömme vektörü depoları da diğer herhangi bir üretim veri deposuyla aynı bütünlük kontrollerine sahip olmalı.
- ◆ Yalnızca önleme için değil, tespit için de araçlandırılmalı. Model davranışında anomali tespiti, mümkün olduğunda diferansiyel gizlilik ve çatışmalı eğitim ek katmanlar sağlar; ancak önleyici kontrolleri aşan olayları gerçekten yakalayan şey, promptların, araç çağrılarının ve çıktıların günlüğe kaydedilmesi ve izlenmesidir.
- ◆ Gölge yapay zeka boşluğu kapatılmalı. Gölge yapay zekanın ihlal maliyetlerini ne kadar yükselttiği göz önüne alındığında, yalnızca yazılı politikalar değil, onaysız yapay zeka araç kullanımını tespit eden ve yöneten teknik kontroller artık temel bir beklenti.
- ◆ Veri kökeni takip edilmeli. Eğitim ve ince ayar verisi için sürüm kontrolü ve köken takibi, zehirlenmeyi hem devreye sokmayı zorlaştırır hem de bir şeyler ters gittiğinde izini sürmeyi hızlandırır.

Siber Güvenlikte Yapay Zeka: Aynı Teknoloji, İki Taraf

Yapay zekanın siber güvenlikle ilişkisi tek yönlü değildir. Aynı yetenekler hem saldırganların elini güçlendiriyor hem de savunma ekiplerine daha önce mümkün olmayan bir tespit ve müdahale hızı kazandırıyor. Dünya Ekonomik Forumu'na göre kuruluşların %94'ü, yapay zekayı 2026'da siber güvenlik ortamını şekillendiren en büyük güç olarak görüyor -bu oran, teknolojinin ne kadar merkezi bir konuma geldiğinin bir göstergesi.

→ **Saldırı tarafında;** yapay zeka saldırıları izole tehditlerden, minimal insan müdahalesiyle çalışan tam otomatik saldırı zincirlerine dönüştü. En belirgin riskler arasında yapay zeka ile üretilmiş ortalama (phishing) e-postaları, derin sahte (deepfake) dolandırıcılık, yapay zeka destekli kötü amaçlı yazılım ve otomatikleştirilmiş zafiyet keşfi sayılabilir. “Yapay zeka hizmet olarak” (AI-as-a-service) platformları sayesinde, teknik bilgisi sınırlı saldırganlar bile zafiyet taramalarını otomatikleştirebiliyor, ikna edici ortalama e-postaları üretebiliyor, kendini değiştirebilen kötü amaçlı yazılımlar oluşturabiliyor ve üst düzey yöneticileri taklit etmek için derin sahtekarlık (deepfake) teknolojilerini kullanabiliyor. Saldırganlar artık yapay zekayı saldırı zincirindeki (Cyber Kill Chain) keşif, ilk erişim, kimlik bilgisi hırsızlığı, tespitten kaçınma ve kalıcılık sağlama aşamalarının hepsinde kullanıyor; ajan tabanlı yapay zekanın saldırı kampanyalarında otomasyonu daha da artırması bekleniyor.

→ **Savunma tarafında** ise yapay zeka, deneysel bir avantaj olmaktan çıkıp operasyonel bir zorunluluğa dönüştü. Modern güvenlik operasyon merkezleri artık davranışsal anomali tespiti, yapay zeka destekli SIEM (güvenlik bilgi ve olay yönetimi) korelasyonu, otomatik olay müdahalesi (SOAR), tahmine dayalı risk puanlaması ve doğal dil işleme tabanlı gelişmiş ortalama tespiti gibi araçlara dayanıyor. IBM’in verilerine göre, kendi güvenlik operasyonlarında yapay zeka ve otomasyonu yoğun şekilde kullanan kuruluşlar, ihlal tespit süresini 80 gün kısaltıyor ve ortalama ihlal maliyetlerini 1,9 milyon dolar azaltıyor.

Bu çift taraflı doğa, güvenlik ekipleri için pratik bir sonuç doğuruyor: yapay zekayı yalnızca korunması gereken bir varlık olarak değil, aynı zamanda savunmanın bir parçası olarak da değerlendirmek gerekiyor. Ancak bu, savunma araçlarını körü körüne yapay zekaya devretmek anlamına gelmiyor -aksine, otomatik tespit ve müdahale sistemlerinin kendisi de yukarıda anlatılan LLM’e özgü risklere (örneğin bir güvenlik kopyilotunun prompt injection ile yanıltılması) açık olabilir. Dolayısıyla savunma amaçlı yapay zeka dağıtımları da aynı titizlikle -sınırlı yetki, sürekli izleme, insan onayı gerektiren kritik eylemler- tasarlanmalı.

Sonuç: Katmanlı Bir Yaklaşımın Zorunluluğu

Yapay zeka güvenliğinde yaşadığımız, aslında tek bir gerçeğin farklı yüzleri: yapay zeka, hem korunması gereken bir varlık hem bir saldırı aracı hem de bir savunma yeteneği olarak aynı anda var oluyor. Bu çok katmanlı doğa, tek bir kontrolün (örneğin yalnızca bir güvenlik duvarı ya da yalnızca bir yönetim politikası) yeterli olmayacağı anlamına geliyor.

Pratikte etkili bir yaklaşım şu unsurları bir araya getiriyor: sürekli kırmızı takım (red team) testleri ve tehdit modellemesi; ajanlara ve araçlara en az ayrıcalık ilkesinin uygulanması; RAG hatları ve gömme depoları dahil olmak üzere getirim/geribesleme (retrieval) sistemlerinin güvenilmeyen girdi olarak ele alınması; hem model davranışını hem de tedarikçi performansını izleyen sürekli izleme mekanizmaları;

gölge yapay zekayı tespit eden teknik kontroller. Tüm bunlarla birlikte AB Yapay Zeka Yasası, NIST AI RMF ile ISO/IEC 42001 gibi çerçevelerle uyumlu, üst yönetim düzeyinde sahiplenilen bir yönetim yapısı gerekiyor.

Düzenleyici çerçeveler henüz ajan tabanlı sistemlerin hızına yetişebilmiş değil; NIST'in Şubat 2026'da duyurduğu Yapay Zeka Ajanı Standartları Girişimi bu boşluğu kapatmaya yönelik ilk adımlardan biri, ancak sonuçları 2026'nın son çeyreğinde bekleniyor. Türkiye'de ise belirli çalışmalar başlamasına rağmen ortada net bir yasa veya düzenleme şu an için bulunmuyor. Bu geçiş döneminde kurumların en güvenilir stratejisi, bitmiş bir düzenleyici yol haritasını beklemek yerine *“model kandırıldığında bile hiçbir kritik şeyin bozulmayacağı”* varsayımıyla katmanlı savunmalar kurmak olmalıdır.

2026'da yapay zeka güvenliği, web uygulama güvenliğinin yaklaşık yirmi yıl önce bulunduğu noktada duruyor. Gerçekleşen yapay zeka saldırı olayları, bu konudaki güvenlik standartları veya koruma önlemlerinden daha hızlı değişiyor. Kalıcı bir strateji olarak, bir model kandırıldığında hasar yarıçapının küçük kalmasını sağlayacak şekilde sistemler tasarlamak oluşacak zararları sınırlayacaktır. Bu durumda en iyi performans gösteren kuruluşlar, bitmiş bir düzenleyici yol haritasını beklemek yerine katmanlı, “ihlal varsayımı” savunmalar kuran kuruluşlardır.

Orhan MORDOĞAN
Elektronik ve Haberleşme Mühendisi

Kaynakça

- SD Times, “Prompt Injection tops 2026 OWASP GenAI / LLM Top Ten vulnerabilities”
- Help Net Security, “OWASP 2026 LLM Top 10: ‘The model will be fooled’”
- DeepTeam, “OWASP Top 10 for Agents 2026”
- IBM, “2025 Cost of a Data Breach Report: Navigating the AI rush without sidelining security”
- Shattered.io, “Shadow AI: 20% of Breaches, \$670K Cost”
- Openlayer, “Third-Party AI Risk Management and Vendor Governance”
- Secure Privacy, “AI Risk & Compliance 2026: Enterprise Governance Overview”
- Terralogic, “AI Third-Party Risk Management 2026”
- Cloud Security Alliance, “NIST AI Risk Management Framework: Agentic Profile”
- Cyber Defense Magazine, “2026 Cybersecurity Forecast: AI-Powered Threats to Significantly Intensify the Threat Landscape”
- DeepStrike, “AI Cybersecurity Threats 2026: Enterprise Defense Guide”
- Mindgard, “Training Data Poisoning: Risks, Detection Methods & Prevention Strategies”
- <https://npartners.com.tr/tr/turkiyede-2026-yapay-zeka-kanunu-tbmmye-sunulan-uc-kanun-teklifinin-detayli-karsilastirilmesi>
- <https://www.aa.com.tr/tr/bilim-teknoloji/turkiye-yapay-zeka-eylem-planina-iliskin-cumhurbaskani-genelgesi-resmi-gazetede/4030067>
- <https://cms.law/en/int/expert-guides/ai-regulation-scanner/tuerkiye>
- <https://afyonluoglu.org/news/kvkk-uretken-yapay-zeka-ve-kisisel-verilerin-korunmasi-rehberi/>
- <https://www.alomaliye.com/2026/08/18/turkiye-yapay-zeka-eylem-plan-2026-2030/>
- <https://www.sanayi.gov.tr/yapayzekaeylemplani>

MÜHENDİSLİKTE KAMU YARARI VE MESLEKİ SORUMLULUK

Mühendislik hizmetlerinde kamu yararının korunması, güncel teknik düzenlemeler ve etkin denetim kadar mesleki bağımsızlığa ve eşit çalışma koşullarına da bağlı. EMO İstanbul Şubesi komisyonlarının değerlendirmeleri, bu alanlardaki sorunları ve çözüm arayışlarını bir araya getiriyor

► Teknik Yönetmelikler Komisyonu

Elektrik İç Tesisleri Yönetmeliği'nin güncellenmesi, komisyonun öncelikli çalışma başlığı. Bu kapsamda, 2024-2025 yıllarında TEDAŞ bünyesinde EMO'nun katılımıyla yürütülen çalışmalar ve değerlendirme notları dokuz bölüm hâlinde düzenlenerek komisyon üyeleriyle paylaşıldı.

İlk bölüm üzerindeki görüşmelerde, önceki çalışmalarda öne çıkan konular ve görüş ayrılıkları ele alındı. Sonraki aşamada metin üzerinde düzenleme yapılması planlanıyor.

► Aydınlatma Teknikleri Komisyonu

Işık kirliliğinin önlenmesine yönelik teknik bir çerçeve oluşturulması, komisyonun çalışma konuları arasında yer alıyor. Hazırlanmakta olan Işık Kirliliği Şartnamesi taslağı, alt çalışma grubunda değerlendiriliyor. Çalışma sonucunda Teknik Yönetmelikler Komisyonuna görüş sunulması hedefleniyor.

Planlanan çevrim içi seminerlerin konuları arasında tünel aydınlatması, LED teknolojisindeki güncel gelişmeler, güneş enerjili aydınlatma ve yeşil bina sertifikasyonunda aydınlatma yaklaşımları bulunuyor. Sahne aydınlatması ve 3D mapping uygulamalarında aydınlatma yerleşimi de programın diğer başlıkları.

► Serbest Müşavir Mühendislik Komisyonu

Serbest Müşavir Mühendislik (SMM) hizmetlerinde teknik doğruluk, can ve mal güvenliği ile meslek etiği birlikte gözetilmelidir. Proje onaylarındaki uygulama farklılıkları, teknik değerlendirmelerde ortak yaklaşımın kurulamaması ve idari süreçlerde yaşanan sorunlar, hizmetlerin yürütülmesini güçleştiriyor.

SMM Komisyonu, üyelerden gelen görüşleri değerlendirerek uygulamalarda birlik sağlanmasına ve ilgili kurumlarla iletişimin geliştirilmesine katkı sunmayı amaçlıyor. Mevzuat değişikliklerinin izlenmesi, genç mühendislerin SMM süreçlerine hazırlanması ve meslektaşların haklarının korunması da komisyonun öncelikleri arasında.

Yapı Denetim Komisyonu

Yapı güvenliği, projeye uygunluğun sahada etkin biçimde denetlenmesini gerektiriyor. Komisyon, saha kontrolü yapılmadan verilen onayları, düşük denetçi ücretlerini ve yetersiz hizmet bedellerini denetimin niteliğini zayıflatan sorunlar arasında değerlendiriyor. Denetçilerin baskı ve şiddete maruz kalması ise mesleki bağımsızlığı tehdit ediyor.

Öneriler arasında, yer teslimi, temel, sıva öncesi ve iş bitimi aşamalarında farklı disiplinlerden denetçilerin birlikte saha kontrolü yapması, ziyaretlerin kayıt altına alınması ve ücretlerin güvenceye kavuşturulması bulunuyor. Şantiye şefliğinde süreklilik, çalışanların mesleki yeterliliği ve denetçilerin korunması da ele alınan başlıklar. Yapı kullanıma açıldıktan sonra bakım ve denetimin sürdürülmesi için teknik hizmet birimleri kurulması öneriliyor.

Bilirkişilik Komisyonu

Bilirkişilik, elektrik tesisatı ve enerji altyapısından iş güvenliğine uzanan teknik uyumsuzluklarda yargının uzmanlık bilgisiyle desteklenmesini sağlar. Raporların niteliği, teknik yetkinliğin yanı sıra tarafsızlığa, bilimsel yaklaşıma ve meslek etiğine bağlıdır.

Komisyon, meslektaşların bilgi ve yetkinliğini geliştirmeyi ve raporlama standartlarını yükseltmeyi amaçlıyor. Bu doğrultuda eğitim, çalıştay ve bilgi paylaşım toplantıları planlanıyor. Mevzuat değişikliklerinin izlenmesi ve uygulamada karşılaşılan sorunların birlikte değerlendirilmesi de bu çalışmaların temel başlıklarını oluşturuyor.

Kadın Komisyonu

İş yerinde ayrımcılık, ücret eşitsizliği ve kariyer engelleri, kadın mühendislerin mesleki yaşamını etkileyen başlıca sorunlar arasında. Kadın Komisyonu, bu sorunların belirlenmesini ve çözüm önerileri geliştirilmesini önceliklendiriyor.

Kadın istihdamının ve yönetici pozisyonlarındaki temsilin artırılması, iş yaşamında güvenlik ve kadın üyelerin örgütlü katılımının güçlendirilmesi hedefleniyor. Üniversitelerdeki kadın mühendislik öğrencileriyle deneyim paylaşımı ve mentorluk çalışmalarının yanı sıra teknik geziler, paneller ve dayanışma etkinlikleri planlanıyor. Bu çalışmaların meslekte kadınların görünürlüğünü artırması ve toplumsal cinsiyet eşitliğine katkı sunması amaçlanıyor.

ŞUBEDEN TEKNİK VE MESLEKİ GÜNDEM

45. Yönetim Kurulunun göreve başlamasının ardından EMO İstanbul Şubesi'nin etkinliklerinde tesis güvenliği, dijitalleşme ve mesleki yetkinlik öne çıkan başlıklar oldu. Teknik eğitimlere, öğrenci projelerinin paylaşımı ve mühendisliğin toplumsal sorumluluğunu ele alan çalışmalar eşlik etti.



Alçak Gerilimde Koruma ve Güç Kalitesi

28 Ağustos'ta İkitelli OSB iş birliğiyle düzenlenen Alçak Gerilim Sistemlerinde Koruma Semineri'nde MCB, RCBO, RCCB, AFCI ve AFDD koruma elemanlarının çalışma prensipleri, saha uygulamaları ve ilgili standartlar ele alındı.

29 Ağustos'ta Şube Eğitim Merkezi'nde gerçekleştirilen Kompanzasyon Sistemleri ve Güç Kalitesi Semineri'nde ise malzeme seçimi, kompanzasyon yöntemleri, arızalar ve harmonikler uygulama örnekleriyle değerlendirildi. Her iki semineri EMO Bursa Şubesi Yönetim Kurulu Üyesi Eray Yağız sundu.

Yangın Güvenliği ve Acil Durum

5 Ağustos'ta İkitelli OSB ile birlikte düzenlenen seminerde, Elektrik Elektronik Mühendisi ve A Sınıfı İş Güvenliği Uzmanı Mehmet Emin Erdem'in sunumuyla yangın güvenliği, risklere karşı alınacak önlemler ve acil durumlarda doğru müdahale yöntemleri değerlendirildi.

BIM ve Bakım Mühendisliği

9 Eylül'de Mimar Emre Akdeniz'in sunduğu BIM Destekli Tesis Yönetimi Semineri'nde, Yapı Bilgi Modellemesi (BIM) kavramı ve elektrik tesisat projelerindeki kullanımı incelendi.

EMO İstanbul, Kocaeli ve Bursa şubeleri ile MMO Kocaeli Şubesinin ortak Bakım Teknolojileri Çalışma Grubu, haziran ve temmuzda bir araya geldi. Şubedeki 29 Ağustos tarihli Bakım Mühendisliği Çalışma Grubu toplantısında ise uygulamadaki eksiklikler, planlanan çalıştay ve bilgilendirici içerik üretimi ele alındı.



Aydınlatma ve Enerji Verimliliği

28 Nisan'da İstanbul Kent Üniversitesinde YK Üyeleri Nedim Bingöl ve Civan Ateş'in verdiği eğitimde, peyzaj projelerinde elektrik ve mekanik sistemlerin entegrasyonu, güneş enerjisi, gece aydınlatması ve maliyet keşfi işlendi. Şube temsilcileri ayrıca 20-23 Temmuz'da Çevre, Şehircilik ve İklim Değişikliği Bakanlığının Enerji Kimlik Belgesi Uzmanı Eğitici Eğitimi'ne katıldı.

Mesleki Uygulamalar ve Bilirkişilik

21 Mayıs'taki BEDAŞ görüşmesinde serbest müşavir mühendislerin (SMM) karşılaştığı sorunlar ve çözüm olanakları ele alındı. 7 Mayıs'ta Çevre, Şehircilik ve İklim Değişikliği İstanbul İl Müdürlüğüyle yapılan görüşmede ise yangın, topraklama, yenilenebilir enerji ve şarj istasyonlarına ilişkin teknik düzenlemeler değerlendirildi.

5 Eylül'de düzenlenen Bilirkişilik Çalıştayı, İstanbul Üniversitesi Hukuk Fakültesinden Doç. Dr. Derya Belgin Güneş'in katılımıyla gerçekleştirildi.



Öğrenci Projeleri ve Teknik Yayınlar

26 Haziran'da Altınbaş Üniversitesi Bakırköy Yerleşkesi'nde düzenlenen Bitirme Projeleri Sergisi (BPS) 2026 İstanbul Yerel Sergisi, 35 proje ile 70 öğrenciyi bir araya getirdi.

23 Haziran'da Omega Grup ile imzalanan protokol kapsamında öğrencilere staj desteği, teknik eğitimler ve çalıştaylar planlandı.



Teknik Elemanların Çalışma Yaşamı

22 Haziran'da Prof. Dr. F. Serkan Öngel'in katıldığı çevrim içi etkinlikte, 15-16 Haziran 1970 Büyük İşçi Direnişi'nden hareketle Türkiye'de işçi sınıfının değişen yapısı ve teknik elemanların bu dönüşüm içindeki konumu tartışıldı.

Kamusal Elektrik Güvenliği ve Kent Planlaması

Şubenin 12 Mayıs tarihli açıklamasında, Kağıthane’de bir çocuğun elektrik direğine temas ederek akıma kapılmasının ardından kamusal alanlardaki elektrik altyapısının güvenliğine dikkat çekildi.

29 Temmuz’daki İstanbul Plan 2050 toplantısında planlama süreci ve meslek odalarının katkıları değerlendirildi. TMMOB ile İBB arasında 20 Ağustos’ta imzalanan protokol ise sağlıklı kentleşme, nitelikli yapılaşma ve kültürel değerlerin korunmasına yönelik iş birliğini konu aldı.



Nükleer Enerji ve Kamu Yararı

28 Mart’ta Çernobil’in 40. yılı dolayısıyla şubede düzenlenen panelde, nükleer enerjinin ekonomik, siyasi ve çevresel boyutları ele alındı. 27 Haziran’daki Nükleer Karşıtı Platform İstanbul Kongresi’nde ise çevre hakkı, iklim gündemi ve nükleer santrallerin insan sağlığı üzerindeki etkileri tartışıldı.

ODA’DAN HABERDAR OLUN

Sosyal medya hesaplarımızı, internet adresimizi, YouTube kanalımızı takip ederek bizden haberdar olun.

