

OTONOM UYUM SİSTEMİNE NE KADAR GÜVENEBİLİRİZ?

RegTech'te Güvenilir Yapay Zekâ, İnsan Gözetimi ve İzlenebilir Düzenleyici Karar Mimarisi

Barış ÇORUH – Biyomedikal Y. Mühendisi

YÖNETİCİ ÖZETİ

Tıbbi cihaz sektöründeki RegTech dönüşümü yeni bir eşiğe yaklaşmaktadır. İlk dijitalleşme dalgası dokümanları elektronik ortama taşıdı. Sonraki aşamada kalite, gereksinim, risk, doğrulama, klinik değerlendirme ve piyasa sonrası gözetim süreçleri dijital platformlar üzerinde birbirine bağlanmaya başladı. Ardından izlenebilirlik, karar mimarisi, Canlı Teknik Dosya ve Dijital Regülasyon İkizi gibi daha ileri yapılar gündeme geldi. Son aşamada yapay zekâ, yalnızca bilgiye erişimi hızlandıran bir araç olmaktan çıkarak düzenleyici ilişkileri yorumlayan bir katmana dönüşmeye başladı. Bu dönüşümün mantıksal devamı otonom uyum sistemleridir.

Bu sistemlerin amacı insanın yerine düzenleyici karar vermek değildir. Daha önemli yetenekleri, organizasyonun sürekli değişen düzenleyici durumunu izlemek; sapmaları tespit etmek; değişikliklerin gereksinim, risk, doğrulama, klinik kanıt ve piyasa sonrası gözetim üzerindeki olası etkilerini değerlendirmek ve uzman ekiplerin önüne aksiyon önerileri getirmektir. Önceki makalede tanımlanan otonom uyum yaklaşımının merkezinde de insanın sistemden çıkarılması değil, insanın tek başına yönetmekte zorlandığı ilişki ağlarının görünür hale getirilmesi yer almaktadır. Ancak sistem yorumlamaya ve öneri üretmeye başladığı anda yeni bir yönetim problemi ortaya çıkar: **Bir organizasyon, sistem tarafından üretilen düzenleyici öneriye ne kadar güvенеbilir?** Bu soru yalnızca yapay zekânın doğruluk oranı ile cevaplanamaz.

Düzenleyici bir sistemin güvenilir olması için organizasyonun hangi verinin kullanıldığını, hangi ilişkilerin değerlendirildiğini, hangi kanıtların dikkate alındığını, hangi belirsizliklerin bulunduğunu ve sistemin neden belirli bir aksiyon önerdiğini anlayabilmesi gerekir. Bu nedenle otonomluk arttıkça kontrol ihtiyacı ortadan kalkmaz. **Kontrolün biçimi değişir.**

Geleneksel kalite sistemlerinde kontrol, insanların işlemleri gerçekleştirmesi ve sonuçları gözden geçirmesi üzerine kuruludur. Otonom sistemlerde ise insanın rolü giderek işlemleri gerçekleştirmekten sistemin davranış sınırlarını belirlemeye, istisnaları değerlendirmeye ve kritik kararları yönetmeye doğru kayar.

Bu makalenin temel argümanı şudur: **Otonom RegTech sistemlerinde güven, yapay zekânın ne kadar güçlü olduğundan değil; sistemin karar üretme sürecinin ne kadar izlenebilir, açıklanabilir, kanıta dayalı, kontrollü ve denetlenebilir olduğundan**

doğar. Bu nedenle geleceğin RegTech mimarisinde yeni bir katmana ihtiyaç vardır: **Düzenleyici Güven Katmanı.** Bu katman altı temel yetkinliği bir araya getirir:

Veri bütünlüğü → İzlenebilirlik → Açıklanabilirlik → Kanıt → İnsan gözetimi → Denetlenebilirlik

Geleceğin RegTech rekabeti yalnızca hangi sistemin daha fazla yapay zekâ kullandığı üzerinden şekillenmeyecektir. Asıl fark, hangi organizasyonun yapay zekâyı **kontrollü bir düzenleyici karar sistemine** dönüştürebildiğinde ortaya çıkacaktır.

1. REGTECH'İN PROBLEMİ DEĞİŞİYOR

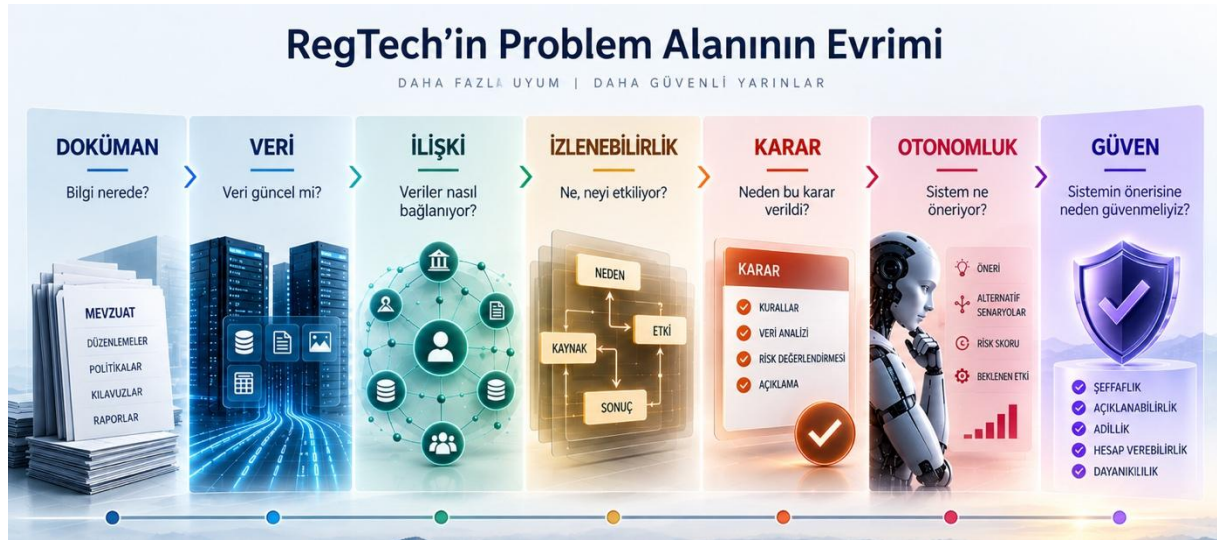
Tıbbi cihaz sektöründeki dijital dönüşümün ilk yıllarında temel problem veriye erişimdi. Gereksinimler farklı dosyalarda tutuluyordu. Risk analizleri ayrı tablolarda yönetiliyordu. Test sonuçları başka ortamlarda bulunuyordu. Klinik kanıt teknik dosyanın farklı bölümlerinde yaşıyor, piyasa sonrası veriler ise çoğu zaman bu yapının dışında kalıyordu. Dolayısıyla ilk RegTech problemi verilerin dijital hale getirilmesi ve merkezi olarak yönetilebilmesiydi. Ancak süreçler dijitalleştikçe daha temel bir problem görünür hale geldi: **Verilerin aynı sistemde bulunması, aralarında doğru ilişkilerin kurulduğu anlamına gelmiyordu.**

Bir gereksinimin hangi riskle ilişkili olduğu, belirli bir riskin hangi doğrulama faaliyetiyle kontrol edildiği veya bir piyasa sonrası sinyalin teknik dosyanın hangi bölümlerini etkilediği görülemiyorsa organizasyon dijitalleşmiş olabilir; fakat gerçek anlamda RegTech mimarisi kurmuş değildir. Bu nedenle RegTech'in ikinci problemi **ilişki yönetimi** oldu. Platformlar bu ihtiyaca cevap verdi. Gereksinim, risk, test, DÖF, değişiklik ve kalite kayıtları arasındaki bağlantılar daha görünür hale geldi. Ancak bunun da bir sınırı vardı.

Serinin 11. makalesinde ortaya konduğu üzere bir gereksinimin bir riskle, riskin bir doğrulama faaliyetiyle bağlantılı olduğunu göstermek gerekli olmakla birlikte yeterli değildir. **(8)** Çünkü izlenebilirlik çoğu zaman çok daha kritik bir soruya cevap vermez: **Neden?** Bir ilişkinin var olması, o ilişkinin nasıl yorumlandığını ve hangi karar mantığıyla belirli bir düzenleyici sonuca dönüştürüldüğünü açıklamaz. Bu nedenle “veri izlenebilirliği” ile “karar izlenebilirliği” arasında yeni bir boşluk ortaya çıkar. RegTech böylece üçüncü probleme ulaştı: **Karar.**

Bugün yapay zekâ destekli sistemler bizi bunun da ötesine taşıyor. Sistemler artık yalnızca ilişkileri göstermeye değil, onları yorumlamaya başlıyor. Bir yazılım gereksinimi değiştiğinde sistem ilgili riskleri tarayabilir. Potansiyel olarak etkilenen doğrulama faaliyetlerini belirleyebilir. Teknik dosya ilişkilerini analiz edebilir. Piyasa sonrası verilerin yeniden değerlendirilmesi gerekip gerekmediğini gösterebilir. Otonom uyum yaklaşımı tam olarak burada ortaya çıkar. 14. makalede tanımlandığı biçimiyle otonom sistem yalnızca veri saklamaz veya göstermez; organizasyonun düzenleyici durumunu sürekli değerlendirir, potansiyel sapmaları belirler ve aksiyon önerileri üretir. Nihai

değerlendirme ve onay ise uzman ekiplerde kalır. Bu ilerleme önemli bir verimlilik kazancı yaratabilir. Ancak aynı zamanda yeni bir risk üretir. Sistem ne kadar fazla yorum yaparsa, sistemin **kendi yorumunun güvenilirliği** o kadar önemli hale gelir. RegTech'in bir sonraki problemi artık veri değildir. İzlenebilirlik de değildir. Hatta yalnızca karar da değildir. **Yeni problem güvendir.**



Şekil 1 – RegTech'in Problem Alanının Evrimi
RegTech olgunlaştıkça problem teknoloji kullanımından sistem davranışının yönetimine kaymaktadır.

2. OTONOMLUK HATAYI YALNIZCA HIZLANDIRMAZ

Otomasyon tartışmalarında verimlilik genellikle temel başarı ölçütü olarak ele alınır. Bir işlemin daha kısa sürede gerçekleştirilmesi, daha az manuel kontrol gerektirmesi veya daha fazla verinin analiz edilebilmesi doğal olarak değer yaratır. Ancak düzenleyici operasyonlarda otomasyonun farklı bir özelliği vardır. **Otomasyon yalnızca doğru işlemleri hızlandırmaz. Yanlış işlemleri de ölçeklendirebilir.**

Manuel bir sistemde hatalı bir değerlendirme tek bir kararın içerisinde sınırlı kalabilir. Otonom bir sistemde ise aynı yanlış yorum çok sayıda bağlı ilişkiye yayılabilir. Basit bir örnek düşünelim. Bir yazılım gereksiniminde değişiklik yapılmıştır. Otonom sistem bu değişikliği algılar ve ilgili risk kayıtlarını değerlendirir. Ancak gereksinim ile kritik bir risk arasındaki bağlantı veri modelinde eksiktir. Sistem daha sonra doğrulama kapsamını analiz eder. Eksik ilişkinin sonucu olarak belirli bir doğrulama faaliyetinin etkilenmediği sonucuna varır. Bu öneri uzman tarafından yeterince sorgulanmadan kabul edilirse problem artık tek bir eksik bağlantı değildir. Eksiklik;

- Gereksinim değerlendirmesinden risk analize,
- Risk analizinden doğrulama planına,
- Doğrulama planından teknik dosyaya ve
- Nihayet düzenleyici karara taşınmıştır.

Bu nedenle otonom sistemlerde güven problemi yalnızca “Yapay Zekâ yanlış cevap verebilir” probleminden ibaret değildir. Daha temel risk **hata yayılımıdır**. Başka bir ifadeyle:

Otonomluk, karar zincirindeki bir hatanın organizasyonun diğer düzenleyici katmanlarına yayılma hızını artırabilir.

Bu nedenle güçlü RegTech mimarilerinde sistemin yalnızca ne önerdiği değil, önerinin hangi veri yapısına ve hangi ilişki zincirine dayandığı görünür olmalıdır.

3. GÜVEN İLE DOĞRULUK AYNI ŞEY DEĞİLDİR

Yapay zekâ sistemlerinin değerlendirilmesinde güven çoğu zaman doğruluk kavramıyla özdeşleştirilir. Model yüksek doğruluk oranına sahipse güvenilir olduğu varsayılır. Düzenleyici operasyonlarda bu varsayım yetersizdir. Ulusal Standartlar ve Teknoloji Enstitüsü Yapay Zekâ Risk Yönetim Çerçevesi (NIST – National Institute of Standards and Technology AI Risk Management Framework), güvenilir yapay zekâyı tek bir performans metriği olarak ele almaz. Çerçeve; geçerlilik ve güvenilirlik, güvenlik, dayanıklılık, hesap verebilirlik ve şeffaflık, açıklanabilirlik ve yorumlanabilirlik gibi birden fazla özelliğin birlikte değerlendirilmesini önerir. **(1)** Bu ayrım RegTech açısından daha da önemlidir. Bir sistemin şu öneriyi ürettiğini varsayalım: **“Bu değişiklik nedeniyle doğrulama kapsamı yeniden değerlendirilmelidir.”** Sonuç doğru olabilir. Ancak organizasyonun yalnızca sonucu görmesi yeterli değildir. Aynı zamanda şu soruların cevaplanabilmesi gerekir:

- Hangi değişiklik bu öneriyi tetikledi?
- Hangi gereksinimler etkilendi?
- Bu gereksinimlerin hangi risklerle ilişkisi vardı?
- Hangi mevcut risk kontrolleri dikkate alındı?
- Hangi doğrulama faaliyetlerinin bu kontrollerle ilişkili olduğu değerlendirildi?
- Hangi kanıtlar güncel kabul edildi?
- Sistem hangi noktada belirsizlik gördü?
- Neden mevcut kanıtın yeterli olmadığı sonucuna ulaştı?

Bu sorular cevaplanamıyorsa sistem doğru bir sonuç üretmiş olabilir. Ancak organizasyon henüz **düzenleyici güven** üretmiş değildir. Bu nedenle RegTech açısından: **Doğruluk, sistemin doğru sonuca ulaşmasıyla ilgilidir. Güven ise bu sonucun hangi veri, ilişki, kanıt ve karar mantığı üzerinden üretildiğinin kontrol edilebilir ve savunulabilir olmasıyla ilgilidir.** Bu iki kavram birbirinden ayrılmalıdır.

4. DÜZENLEYİCİ GÜVEN BİR MİMARİ ÖZELLİK OLMALIDIR

Birçok organizasyonda yapay zekâyı güven davranışsal bir mesele olarak ele alınmaktadır. Kullanıcılar sistemi zaman içerisinde tanır. Başarılı sonuçlar gördükçe güven artar. Hatalarla karşılaşıldığında güven azalır. Bu yaklaşım günlük dijital araçlar için

kabul edilebilir olabilir. RegTech için değildir. Çünkü düzenleyici sistemlerde güven kullanıcının hissine bırakılamaz. **Tasarlanmalıdır.**

TS EN ISO/IEC 42001 (Bilgi teknolojisi- Yapay Zekâ - Yönetim Sistemi) standardı, yapay zekâ kullanımını yalnızca teknik model performansı üzerinden değil; organizasyonel bir yönetim sistemi yaklaşımıyla ele alır. Standart, YZ sistemlerinin geliştirilmesi veya kullanılmasındaki risklerin yapılandırılmış biçimde yönetilmesini ve sistemlerin sürekli iyileştirilmesini hedefler. **(2)**

Benzer şekilde Avrupa Birliği (AB) Yapay Zekâ Yasası (EU AI Act), yüksek riskli YZ sistemleri için kayıt tutma, şeffaflık ve insan gözetimi gibi unsurları sistem tasarımının bir parçası haline getirmektedir. Özellikle yüksek riskli sistemlerin çalışmasının yaşam döngüsü boyunca olay kayıtları oluşturabilmesi, çıktılarının kullanıcı tarafından yorumlanabilecek ölçüde şeffaf olması ve uygun insan gözetimine imkân vermesi öngörülmektedir. **(3)** Burada önemli bir sınırın altını çizmek gerekir. **Her RegTech yapay zekâ uygulaması, AB Yapay Zekâ Yasası kapsamında “yüksek riskli tıbbi cihaz yapay zekâsı” değildir.**

Bir üreticinin kendi kalite veya düzenleyici operasyonlarını desteklemek için kullandığı Yapay Zekâ (YZ) sistemi ile MDR kapsamında cihazın kendisi veya cihazın güvenlik bileşeni olan bir YZ sistemi aynı hukuki kategori değildir. Bununla birlikte AB YZ Yasasının yüksek riskli sistemler için getirdiği **kayıt, şeffaflık, insan gözetimi ve risk temelli kontrol mantığı**, RegTech tasarımı açısından güçlü bir yönetim referansı sunmaktadır. Haziran 2025 tarihli MDCG (Medical Device Coordination Group – Tıbbi Cihaz Koordinasyon Grubu) 2025-6 dokümanı da MDR/IVDR ile AB YZ Yasası arasındaki kesişimde özellikle veri yönetimi, kayıt tutma, şeffaflık ve insan gözetiminin kalite yönetim sistemi içerisine entegre edilmesi gerektiğini vurgulamaktadır. **(4)** Bu gelişmeler bize daha genel bir tasarım prensibi gösteriyor: **Yapay zekâya güven, modele eklenen bir özellik değil; sistem mimarisinin sonucudur.**



5. GÜVENİN İLK KOŞULU: VERİ BÜTÜNLÜĞÜ

Yapay zekâ üzerine yapılan tartışmalar çoğu zaman algoritmanın gücüyle başlar. RegTech açısından bu başlangıç noktası yanlıştır. Daha temel soru şudur: **Sistem ne görüyor?** Bir yapay zekâ modeli yalnızca erişebildiği düzenleyici bağlam kadar güçlüdür. 13. makalede ortaya konduğu gibi parçalı veri mimarisi üzerinde çalışan bir yapay zekâ, ne kadar gelişmiş olursa olsun eksik ilişkilere dayanarak yorum üretmek zorunda kalır (5). Entegre veri mimarisinde ise aynı model gereksinim, risk, test, değişiklik, klinik veri ve piyasa sonrası gözetim arasındaki daha geniş bağlamı değerlendirebilir. Bu nedenle RegTech'te güvenilir yapay zekânın ilk katmanı model değildir. Veri mimarisidir. Çünkü sistem, bilmediği ilişkiyi değerlendiremez; görmediği kanıtı kararına dahil edemez. Veri bütünlüğü birkaç boyut içerir:

- Bilginin doğru olması gerekir.
- Güncel olması gerekir.
- Kaynağı bilinmelidir.
- Versiyonu izlenebilmelidir.
- İlişkileri korunmalıdır.
- Yetkisiz değişikliklere karşı kontrol edilmelidir.

Bir risk analizi üç ay önce güncellenmiş, ancak ilişkili doğrulama planı eski versiyonda kalmışsa sistemin her iki kaydı da doğru biçimde okuması yeterli değildir. Problem verinin kendisinden çok **bağlamın bütünlüğüdür**. Bu nedenle geleceğin RegTech sistemlerinde veri kalitesi yalnızca alanların doluluğuyla ölçülemez. Yeni bir kalite sorusu gerekir: **Bu veri, ilişkili olduğu düzenleyici bağlamla birlikte güncel mi?**

6. İZLENEBİLİRLİKTEN KANIT İZLENEBİLİRLİĞİNE

Geleneksel izlenebilirlik sistemi şu ilişkilere odaklanır:

- Gereksinim → Risk
- Risk → Kontrol
- Kontrol → Test
- Test → Sonuç

Bu yapı halen vazgeçilmezdir. Ancak otonom sistemlerde yeni bir izlenebilirlik boyutuna ihtiyaç vardır. Çünkü artık yalnızca veriler arasında değil, **sistemin ürettiği yorum ile kanıt arasında da bağlantı kurulmalıdır**. Bir sistem: “Risk yeniden değerlendirilmelidir” dediğinde organizasyon geriye doğru yürüyebilmelidir:

- **Öneri** ← hangi etki analizinden geldi?
- **Etki** ← hangi ilişkiler üzerinden belirlendi?
- **İlişkiler** ← hangi verilere dayanıyor?
- **Veri** ← hangi kaynaktan ve hangi versiyondan geldi?

Bu yapı yeni bir kavram ortaya çıkarır: **Düzenleyici Kanıt İzlenebilirliği**. Düzenleyici kanıt izlenebilirliği yalnızca bir kararın neyle bağlantılı olduğunu değil, kararın **hangi kanıt yolu üzerinden üretildiğini** gösterir. Bu, 11. makalede (6) ortaya konan karar izlenebilirliği yaklaşımının otonom sisteme taşınmış halidir. 11. makalede karar kuralları, bağlam ve kararın dayandığı kanıt yapısı sistematik hale geldiğinde kararın yalnızca kayıtlı değil; doğrulanabilir ve savunulabilir hale geldiği vurgulanmıştı. Otonom sistemlerde bu yaklaşım zorunluluk haline gelir. Çünkü sistem artık yalnızca kanıtı depolamamaktadır. **Kanıtı yorumlamaktadır**.



Her düzenleyici öneri, **geriye doğru kendi kanıt zincirine izlenebilmelidir**.

Şekil 3 – Düzenleyici Önerinin Kanıt Zinciri

7. AÇIKLANABİLİRLİK, İYİ BİR AÇIKLAMA YAZMAK DEĞİLDİR

Üretken yapay zekânın yaygınlaşması açıklanabilirlik konusunda yeni bir yanılsama yaratmaktadır. Bir sistem, verdiği cevabı oldukça ikna edici biçimde açıklayabilir. Ancak açıklamanın iyi yazılmış olması, kararın doğru kanıta dayandığını göstermez. RegTech'te gerçek açıklanabilirlik farklıdır. Sistem kendi sonucunu retorik olarak gerekçelendirmemelidir. **Kanıtsal olarak yeniden oluşturmalıdır.**

Örneğin sistem: “Yeni doğrulama gereklidir.” diyorsa açıklama şu yapıda olmalıdır:

- Bir yazılım gereksinimi değişti.
- Bu gereksinim şu riskle ilişkili.
- Risk kontrolü şu yazılım davranışına dayanıyor.
- Mevcut doğrulama kanıtı önceki gereksinim versiyonuna göre oluşturuldu.
- Yeni gereksinim, test edilen sınır koşullarını değiştiriyor.

Bu nedenle mevcut doğrulama kanıtının yeterliliği yeniden değerlendirilmelidir. Burada sistemin değeri dili değildir. **İlişki zinciridir.** Bu nedenle güvenilir RegTech'in açıklanabilirlik standardı şu soru olmalıdır: **Sistem, önerisini organizasyonun mevcut kanıt mimarisi üzerinden gösterebiliyor mu?** NIST'in güvenilir YZ yaklaşımında açıklanabilirlik ve yorumlanabilirliğin güven yönetiminin ayrı unsurları olarak ele alınması da bu ayrımı desteklemektedir. (1)

8. “İNSAN MÜDAHALESİ İÇEREN SİSTEM” YETERLİ DEĞİLDİR

Yapay zekâ yönetiminde en sık kullanılan kavramlardan biri “**insan müdahalesi içeren sistem (human-in-the-loop)**” yaklaşımıdır. Temel fikir doğrudur: **Kritik karar döngüsünde insan bulunmalıdır.** Ancak yalnızca bir insan onay adımı eklemek güvenli bir sistem oluşturmaz. Bir uzmanın sistem tarafından üretilen önerinin altında “Onayla” butonuna basması gerçek gözetim değildir. Eğer uzman;

- Sistemin hangi veriyi kullandığını,
- Hangi ilişkinin kritik olduğunu,
- Hangi kanıtın eksik olduğunu,
- Sistemin hangi varsayımı yaptığını ve
- Belirsizliğin nerede bulunduğunu

göremiyorsa insan karar döngüsünde görünüşte vardır. Gerçekte ise **otomasyonun doğrulayıcısına** dönüşmüştür. Bu risk AB YZ yasası içerisinde “otomasyon önyargısı (automation bias)” bağlamında açık biçimde ele alınmaktadır.

Yüksek riskli YZ sistemlerindeki insan gözetimi mekanizmalarının, kullanıcıların sistemin kapasite ve sınırlamalarını anlamasını, çıktıyı doğru yorumlayabilmesini ve gerektiğinde sistemi yok sayabilmesini, geçersiz kılabilmesini veya durdurabilmesini desteklemesi beklenmektedir. (3)

MDCG 2025-6 da yüksek riskli tıbbi cihaz YZ sistemlerinde insan gözetiminin risk, otonomi düzeyi ve kullanım bağlamıyla orantılı olması gerektiğini; gözetim

mekanizmalarının açık biçimde tanımlanmasını ve dokümanle edilmesini vurgulamaktadır. RegTech açısından bundan çıkarılabilecek sonuç önemlidir. Doğru hedef yalnızca: **“İnsan Müdahalesi İçeren Sistem (human-in-the-loop)”** değildir. Daha gelişmiş hedef: **“Yönetişimde İnsan Unsuru (Human-in-governance)”** olmalıdır. İnsan sistemin yaptığı her hesabı yeniden yapmak zorunda değildir. Ancak insan;

- Sistemin yetki sınırlarını,
- Karar kategorilerini,
- Kritiklik seviyelerini,
- İstisna mekanizmalarını ve
- Durdurma kriterlerini

tanımlamalıdır. İnsan sistemden çıkmaz. **İnsanın sistemdeki rolü değişir.**

9. HER KARAR AYNI ÖLÇÜDE OTOMATİKLEŞTİRİLEMEZ

Otonomluk çoğu zaman teknik bir kapasite olarak ele alınır. Sistem bir işi yapabiliyorsa otomatikleştirilebilir olduğu düşünülür. Düzenleyici sistemlerde doğru yaklaşım bunun tersidir. Temel soru: **“Sistem bunu yapabilir mi?”** değil, **“Bu karar yanlış verilirse ne olur?”** olmalıdır. Bu ayrım bir **Düzenleyici Karar Kritiklik Modeli** gerektirir.

Örneğin eksik bir izlenebilirlik bağlantısının tespit edilmesi görece düşük riskli bir aktivitedir. Sistem bunu otomatik olarak gerçekleştirebilir. Bir risk kaydının güncellenmesi gerektiğinin önerilmesi orta seviyede bir karar olabilir. Sistem öneri sunabilir ancak insan doğrulaması gerekir. Buna karşılık bir artık riskin kabul edilebilir olduğu, klinik kanıtın yeterli olduğu veya önemli bir değişikliğin yeni bir düzenleyici değerlendirme gerektirmediği gibi kararların sonucu çok daha kritiktir. Bu durumda yapay zekânın rolü karar vermek değil: **kanıtı yapılandırmak, ilişkileri göstermek ve uzman kararını desteklemek** olmalıdır.

FDA'nın (Food and Drug Administration – ABD Gıda ve İlaç Dairesi) Yapay Zekâ destekli cihaz yazılımı işlevleri (AI-enabled device software functions) için Ağustos 2025'te yayımladığı PCCP (Predetermined Change Control Plan – Önceden Belirlenmiş Değişiklik Kontrol Planı) yaklaşımında da değişikliğin yalnızca tanımlanması yeterli görülmemekte; planlanan değişikliklerin nasıl geliştirileceği, doğrulanacağı, uygulanacağı ve etkilerinin nasıl değerlendirileceği önceden yapılandırılmaktadır. **(7)** Bu yaklaşımın altında genel bir yönetim ilkesi vardır: **Otomasyon sınırı teknolojinin kapasitesine göre değil, değişikliğin ve kararın riskine göre belirlenmelidir.**



10. GÜVEN İKİLİ BİR DURUM DEĞİLDİR

Bugünkü birçok dijital sistem cevaplarını kesinlik izlenimiyle sunar. Bir sonuç vardır. Bir öneri vardır. Bir aksiyon vardır. Oysa düzenleyici gerçeklik çoğu zaman belirsizlik içerir. Klinik veri yetersiz olabilir. İki risk kaydı arasında çelişki bulunabilir. Doğrulama kanıtının güncelliği tartışmalı olabilir. Piyasa sonrası sinyal henüz yeterince güçlü olmayabilir. Bir değişikliğin etkisi açık olmayabilir. Gerçek anlamda güvenilir sistem bu belirsizliği gizlememelidir. Tam tersine görünür hale getirmelidir. Bu nedenle geleceğin RegTech sistemleri yalnızca: **“Önerim budur.”** dememelidir. Aynı zamanda: **“Bu öneriye hangi güven seviyesinde ulaşıyorum?”** sorusuna cevap vermelidir. Böylece yeni bir kavram ortaya çıkar: **Düzenleyici Güven Durumu**

Örneğin sistem yüksek güven seviyesinde bir öneri üretebilir çünkü veri günceldir, bütün kritik ilişkiler tamamdır ve kanıtlar tutarlıdır. Orta güven seviyesinde sistem bazı ilişkilerin belirsiz olduğunu belirtebilir. Düşük güven seviyesinde ise sistem karar önermek yerine insan incelemesini zorunlu hale getirebilir. Bu ayrım, otonom sistemlerde çok kritik bir tasarım ilkesine dönüşür: **Güvenilir sistem her soruya cevap veren sistem değildir. Ne zaman yeterli kanıt olmadığını bilen sistemdir.**

11. SİSTEMİN KENDİSİ DE SÜREKLİ İZLENMELİDİR

14. makalenin temel tezlerinden biri uyumun artık dönemsel olarak kontrol edilen bir durum olmadığıydı. Piyasa Sonrası Gözetim (PMS) sinyalleri, klinik kanıtlar, siber güvenlik olayları, yazılım güncellemeleri ve değişiklik yönetimi organizasyonun düzenleyici durumunu sürekli olarak değiştirmektedir. Aynı mantık otonom sistem için de geçerlidir.

Bir YZ sistemini bugün valide etmek, sistemin gelecekteki tüm koşullarda aynı davranışı göstereceğini garanti etmez. **Veri dağılımı değişebilir. Ürün portföyü büyüyebilir. Regülasyon değişebilir. Yeni ilişki tipleri sisteme eklenebilir. Model güncellenebilir. İnsanların sistemi kullanım biçimi değişebilir.** Dolayısıyla otonom RegTech sistemlerinde yalnızca düzenleyici durum değil, **sistemin performansı da sürekli izlenmelidir.**

FDA'nın YZ destekli tıbbi cihazlar (AI-enabled medical devices) için yaşam döngüsü yaklaşımı ve model güncellemelerini kontrol etmeye yönelik PCCP (Önceden Belirlenmiş Değişiklik Kontrol Planı) çalışmaları, değişen YZ sistemlerinin sürekli güvenilirliğinin tek seferlik doğrulamayla değil yaşam döngüsü yönetimiyle ele alınması gerektiğine işaret etmektedir. **(7)** Aynı prensip RegTech için uyarlanabilir. Bu durumda organizasyon yalnızca şunu izlememelidir: **Uyum durumumuz değişti mi?** Aynı zamanda: **Uyumu değerlendiren sistemin davranışı değişti mi?** sorusunu da sormalıdır.

12. DENETLENEBİLİRLİĞİN GERÇEK TESTİ:

ALTI AY SONRA AYNI KARARI AÇIKLAYABİLİYOR MUSUNUZ?

Otonom RegTech sistemlerinin güvenilirliğini ölçmek için en güçlü sorulardan biri basittir: **Altı ay sonra aynı kararı yeniden açıklayabilir miyiz?** Bir sistem bugün belirli bir aksiyon önerdiğinde yalnızca nihai önerinin kaydedilmesi yeterli değildir. O anda kullanılan;

- Veri sürümü,
- Gereksinim durumu,
- Risk kaydı,
- Doğrulama kanıtı,
- Klinik veri,
- Piyasa sonrası bilgi,
- İlişki haritası,
- Sistem tarafından üretilen etki analizi,
- İnsan değerlendirmesi ve
- Nihai karar

birlikte izlenebilmelidir. Bu yalnızca teknik “log” tutma meselesi değildir. **Karar durumunun dondurulabilmesidir.**

AB YZ Yasasının yüksek riskli sistemler için yaşam döngüsü boyunca olay kayıtlarının otomatik tutulmasını öngörmesi de izlenebilir sistem davranışının önemini göstermektedir. Bu kayıtların risk oluşturabilecek durumların belirlenmesi, piyasa sonrası izleme ve sistem operasyonunun izlenmesini desteklemesi beklenmektedir. **(3)**

MDCG 2025-6 da AB YZ Yasasının kayıt tutma yaklaşımını, sistemin işleyişinin ve performansının yaşam döngüsü boyunca izlenebilmesini sağlayan fonksiyonel izlenebilirlik olarak açıklamaktadır. RegTech açısından bundan daha genel bir ilke çıkarılabilir: **Bir öneri geriye dönük yeniden üretilemiyorsa tam anlamıyla denetlenebilir değildir.**

13. ÖĞRENEN SİSTEMLER GÜVEN PROBLEMİNİ BÜYÜTÜR

Otonom sistemlerin uzun vadeli potansiyeli yalnızca mevcut ilişkileri analiz etmek değildir. Asıl değer geçmiş olaylardan öğrenebilmesidir. Bir sistem zaman içerisinde hangi değişikliklerin hangi riskleri etkilediğini, hangi Piyasa Sonrası Gözetim (PMS) sinyallerinin daha kritik sonuçlar doğurduğunu veya hangi düzenleyici boşlukların belirli ürün ailelerinde tekrar ettiğini öğrenebilir. Bu organizasyonel açıdan son derece değerli olabilir. Fakat yeni bir paradoks yaratır: **Sistem öğrendikçe daha güçlü hale gelir.** Aynı zamanda: **Sistem öğrendikçe davranışı değişir.** Davranışı değişen bir sistemin geçmişte doğrulanmış performansının gelecekte aynen devam ettiği varsayılmaz.

ISO/IEC 42001'in sürekli iyileşme ve YZ risklerinin yönetimini yönetim sistemi yaklaşımı içerisinde ele alması tam olarak bu nedenle önemlidir. **(2)** FDA ve uluslararası düzenleyicilerin YZ/ML (ML: Machine Learning - Makine Öğrenimi) tabanlı tıbbi cihazlar için önceden belirlenmiş değişiklik planlarını ve yeniden eğitim risklerinin yönetimini tartışması da aynı problemi farklı bir bağlamda ele almaktadır. **(7)** RegTech açısından sonuç açıktır: **Öğrenme kontrolsüz olmamalıdır.** Sistem geçmiş bir olaydan yeni bir ilişki çıkarabilir. Ancak bu ilişkinin doğrudan sistemin gelecekteki karar mantığına dönüşmesi zorunlu değildir. Arada bir yönetim katmanı gerekir. Bu makale için buna: **Öğrenme Onayı** diyebiliriz. Sistem öğrenir. Organizasyon öğrenmenin ne olduğunu görür. Etkisini değerlendirir. Uygunsa sisteme alınmasını onaylar. Böylece: **öğrenen sistem ile kontrolsüz değişen sistem** birbirinden ayrılır.



Öğrenen sistem, **kontrolsüz değişen sistem** olmamalıdır.

Şekil 5 – Kontrollü Otonom Öğrenme Döngüsü

14. KALİTE VE REGÜLASYON EKİPLERİNİN ROLÜ DEĞİŞECEK

Otonom RegTech sistemlerinin en yanlış yorumlarından biri kalite ve regülasyon uzmanlarının önemini azaltacağı varsayımdır. Gerçekte tam tersi olabilir. Bugün kalite ve regülasyon ekipleri zamanlarının önemli bölümünü bilgi toplamak, kayıt kontrol etmek, doküman güncellemek, eksik bağlantıları araştırmak ve değişiklik etkilerini farklı kaynaklarda takip etmek için harcamaktadır.

14. makale (9) otonom uyum sistemlerinin bu görünmeyen ilişki boşluklarını daha erken görünür hale getirerek ekiplerin kayıt yönetiminden karar kalitesi ve stratejik düzenleyici planlamaya kaymasına olanak sağlayabileceğini ortaya koymaktadır. Bu dönüşüm ilerledikçe uzmanların rolü dört alanda yoğunlaşacaktır:

- Birincisi **istisna yönetimi** olacaktır. Sistem rutin ilişkileri yönetirken uzmanlar belirsiz, çelişkili ve yüksek kritik vakalara odaklanacaktır.
- İkincisi **karar kalitesi** olacaktır. Uzmanların değeri veriyi taşımaktan çok hangi kanıtın yeterli olduğunu değerlendirmeye kayacaktır.
- Üçüncüsü **sistem yönetişimi** olacaktır. Uzmanlar sistemin hangi karar sınıflarında ne kadar otonom olabileceğini tanımlayacaktır.
- Dördüncüsü **düzenleyici öğrenme** olacaktır. Kalite ekipleri yalnızca geçmiş kayıtları kontrol etmeyecek, organizasyonun düzenleyici davranışından yeni bilgi üretmeye başlayacaktır.

Böylece kalite fonksiyonunun rolü:

- Kayıt yönetimi
- Kontrol
- Karar desteği
- Yönetişim

çizgisinde evrilebilir.

15. CEO İÇİN ASIL SORU YAPAY ZEKÂ DEĞİL, YETKİ DEVRİDİR

Üst yönetim açısından otonom RegTech yatırımlarındaki en önemli soru hangi yapay zekâ modelinin kullanılacağı değildir. Asıl soru şunlardır:

- Organizasyon hangi karar yetkisini sisteme devretmeye hazır?
- Sistem yalnızca bilgi mi gösterecek?
- Sapma mı tespit edecek?
- Etki analizi mi yapacak?
- Aksiyon mu önerecek?
- Düşük riskli aksiyonları otomatik başlatabilecek mi?
- Risk kayıtlarını değiştirebilecek mi?
- İnsan onayı olmadan bir iş akışını kapatabilecek mi?
- Kritik kararları kim onaylayacak?
- Sistemin durdurulması gereken koşullar neler olacak?

Bunlar yazılım özelliği değildir. **Yönetişim kararlarıdır**. Bu nedenle geleceğin RegTech olgunluk göstergesi: “Kaç yapay zekâ fonksiyonumuz var?” olmayacaktır. Daha güçlü soru şudur: **İnsan ile sistem arasındaki karar sınırını ne kadar açık tanımlayabiliyoruz?** Gerçek otonomluk daha az kontrol değildir. **Daha iyi tasarlanmış kontroldür.**



SONUÇ: REGTECH'İN BİR SONRAKİ SINIRI GÜVENDİR

RegTech dönüşümünün ilk aşamasında temel soru dokümanların nasıl dijitalleştirileceğiydi. Ardından verinin nasıl birleştirileceği soruldu. Sonra ilişkiler gündeme geldi. İzlenebilirlik kuruldu. Bunun da yetmediği görüldüğünde kararların nasıl açıklanacağı ve savunulacağı tartışılmaya başlandı.

Canlı Teknik Dosya ve Dijital Regülasyon İkizi yaklaşımları organizasyonun düzenleyici durumunu statik dokümanlardan çıkararak yaşayan bir veri modeline dönüştürdü. Yapay zekâ destekli düzenleyici zekâ bu ilişkilerin yorumlanmasını mümkün hale getirdi. Otonom uyum sistemleri ise yeni bir aşamaya işaret ediyor. Sistem artık soru sorulmasını beklemeden değişiklikleri algılayabilir, ilişki boşluklarını tespit edebilir, potansiyel etkileri analiz edebilir ve aksiyon önerileri oluşturabilir. Önceki makalenin ulaştığı eşik tam olarak budur. Ancak bu noktadan sonra daha fazla otonomluk tek başına ilerleme değildir. Çünkü sistemin kapasitesi büyüdükçe sistemin davranışını yönetme gereksinimi de büyür. Bu nedenle geleceğin RegTech mimarisinin merkezine yeni bir kavram yerleşmek zorundadır: **Düzenleyici Güven**. Bu güven; daha güçlü algorithmadan değil, daha büyük dil modelinden değil, daha fazla otomasyondan da değil; **veri bütünlüğünden, izlenebilirlikten, açıklanabilirlikten, kanıttan, insan gözetiminden ve**

denetlenebilirlikten doğacaktır. Geleceğin başarılı sistemleri yalnızca doğru cevap üretmeye çalışan sistemler olmayacaktır.

Hangi bilgiye dayandıklarını gösterebilen, hangi ilişkileri değerlendirdiklerini açıklayabilen, belirsizliklerini görünür hale getiren, insanın ne zaman devreye girmesi gerektiğini bilen ve verdikleri öneriyi aylar sonra yeniden kanıtlayabilen sistemler olacaktır. Bu nedenle otonom RegTech'in gerçek başarısı sistemin ne kadar az insana ihtiyaç duyduğu ile ölçülmemelidir. Daha doğru ölçüt şudur: **Sistem ile insan birlikte ne kadar daha kaliteli, izlenebilir ve savunulabilir düzenleyici karar üretebiliyor?** RegTech'in bir sonraki sınırı daha fazla otomasyon değildir. **Güvendir.**

KAYNAKLAR

- 1) **National Institute of Standards and Technology.** *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, 2023. Güvenilir YZ özellikleri ve risk temelli yönetim yaklaşımı.
- 2) **TS/EN ISO/IEC 42001:2023.** *Information technology — Artificial intelligence — Management system.* YZ yönetim sistemi, risk yönetimi, yönetim ve sürekli iyileştirme yaklaşımı.
- 3) **European Parliament and Council.** Regulation (EU) 2024/1689 — Artificial Intelligence Act. Özellikle yüksek riskli YZ sistemleri için kayıt tutma, şeffaflık ve insan gözetimi hükümleri, Madde 12–14.
- 4) **Medical Device Coordination Group & Artificial Intelligence Board.** *MDCG 2025-6 / AIB 2025-1 — Interplay between the Medical Devices Regulation, IVDR and the Artificial Intelligence Act*, June 2025. MDR/IVDR ile YZ Yasası arasındaki kalite sistemi, risk yönetimi, kayıt, insan gözetimi ve izlenebilirlik ilişkileri.
- 5) **“RegTech’in Yeni Evresi: Yapay Zekâ Destekli Düzenleyici Operasyon Çağı – Yapay Zekâ Tabanlı RegTech Mimarisi ve Düzenleyici Zekânın Yükselişi”** Barış ÇORUH, ÇORUH RegTech Makaleleri
- 6) **“RegTech Dönüşümünde Son Katman: Karar Sistemi ve İzlenebilir Karar Mimarisi”** Barış ÇORUH, ÇORUH RegTech Makaleleri
- 7) **FDA, Health Canada & MHRA.** *Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles.* Değişiklik sınırları, kanıt, şeffaflık ve yaşam döngüsü yönetimi.
- 8) **U.S. Food and Drug Administration.** *Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations*, January 2025. AI-enabled medical devices için toplam ürün yaşam döngüsü ve risk yönetimi yaklaşımı. Doküman yayımlandığı haliyle taslak rehberdir.
- 9) **“Otonom Uyum Sistemleri: RegTech’in Bir Sonraki Evrimi – Sürekli Uyumdan Otonom Düzenleyici Operasyonlara Geçiş”** Barış ÇORUH, ÇORUH RegTech Makaleleri
- 10) **ISO 13485:2016.** *Medical devices — Quality management systems — Requirements for regulatory purposes.*

- 11) IEC 62304:2006 + A1:2015.** *Medical device software — Software life cycle processes.*
- 12) ISO 14971:2019.** *Medical devices — Application of risk management to medical devices.*