www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:7 Sayı:2

Geliş:14.12.2025
Kabul:29.12.2025

Mahremiyet Artırıcı Teknolojiler, Gizlilikten Ödün Vermeden Yapay Zekâ Teknolojisinin Gelişimini ve Kullanımını Nasıl Teşvik Edebilir? Türkiye İçin Bir Politika Önerisi

Doç. Dr. Hüseyin Can, AKSOY
Bilkent Üniversitesi Hukuk Fakültesi
hcaksoy@bilkent.edu.tr
ORCID ID: 0000-0002-9243-189X

ÖZ

Yapay zekâ teknolojisinin gelişimi, veri işleme becerimizde devrim yaratarak toplumsal refah, bilginin yayılması ve zenginlik yaratılması için derin bir potansiyelin kilidini açmıştır. Ancak bu sistemlerin yüksek doğrulukta çalışabilmesi için büyük hacimli verilere ihtiyaç duyması, kişisel verilerin korunmasına ilişkin hukuki ilkelerle, özellikle veri minimizasyonu ile yapısal bir gerilim yaratmaktadır. Bu gerilim aynı zamanda yapay zekâya duyulan kamu güvenini de zayıflatmaktadır. Mahremiyet artırıcı teknolojiler (MATlar), tasarımdan itibaren mahremiyet yaklaşımının teknik karşılığı olarak, mahremiyetin korunması ile inovasyonun sürdürülmesi arasında pozitif toplamlı çözümler sunmaktadır. Sentetik veriler, homomorfik şifreleme, farklılaştırılmış gizlilik, federe öğrenme ve benzeri teknolojiler, bir yandan mahremiyeti korurken diğer yandan veri temelli analiz yapılmasını mümkün kılmakta ve mahremiyetten ödün verilmeksizin yapay zekâ teknolojisinden azami fayda sağlanmasına imkân tanımaktadır. Bununla birlikte MATların etkili biçimde benimsenebilmesi, hukuki belirlilik, düzenleyici rehberlik ve uygun teşvik mekanizmalarıyla desteklenen bir politika çerçevesinin oluşturulmasını gerektirmektedir.

Anahtar Sözcükler: Mahremiyet artırıcı teknolojiler – PET – Mahremiyet – Yapay Zekâ – Tasarımdan İtibaren Mahremiyet.

How Can Privacy-Enhancing Technologies Promote The Development And Use Of Artificial Intelligence Without Compromising Privacy? A Policy Proposal For Türkiye

ABSTRACT

The development of artificial intelligence technology has revolutionized our capacity to process data, unlocking profound potential for social welfare, the dissemination of knowledge, and the creation of wealth. However, the fact that these systems require large volumes of data to operate with high accuracy creates a structural tension with the legal principles governing the protection of personal data—particularly the principle of data minimization. This tension also undermines public trust in artificial intelligence. Privacy-enhancing technologies (PETs), as the technical embodiment of the privacy-by-design approach, offer positive-sum solutions that reconcile the protection of privacy with the continued pursuit of innovation. Technologies such as synthetic data, homomorphic encryption, differential privacy, federated learning, and similar methods make it possible to conduct data-driven analysis while safeguarding privacy, thereby enabling the maximization of the benefits of artificial intelligence without compromising privacy. Nevertheless, the effective adoption of PETs requires the establishment of a policy framework supported by legal certainty, regulatory guidance, and appropriate incentive mechanisms.

Keywords: Privacy-Enhancing-Technologies – PET – Privacy - Artificial Intelligence – Privacy by design given

Atıf Gösterme	Aksoy, H. C., (2025). Mahremiyet Artırıcı Teknolojiler, Gizlilikten Ödün Vermeden Yapay Zekâ Teknolojisinin Gelişimini ve Kullanımını Nasıl Teşvik Edebilir? Türkiye İçin Bir Politika Önerisi, *Kişisel Verileri Koruma Dergisi*. *7*(2), 173-188.

GİRİŞ

Yapay zekâ teknolojisinin gelişimi, veri işleme becerimizde devrim yaratarak toplumsal refah, bilginin yayılması ve zenginlik yaratılması için derin bir potansiyelin kilidini açmıştır. Ancak algoritmalar, onları eğitmek için kullandığımız veriler kadar başarılıdır. Bu çerçevede, temelinde istatistik bilimi yatan yapay zekâ uygulamaları, kendi kendine öğrenebilmek, sonuç çıkarabilmek ve karar alabilmek için kişisel veri niteliğindeki sağlık kayıtlarından finansal işlemlere kadar farklı konularda çok büyük miktarda veriye erişim ihtiyacı duymaktadır (Aksoy, 2022).

Yapay zekâ sistemleri tarafından işlenen verilerin bir kısmı kişisel veri niteliğindedir. Bu durum, yapay zekâ sistemleri kullanılarak gerçekleştirilen kişisel veri işleme faaliyetlerinin veri koruma hukuku kurallarına uygun şekilde gerçekleştirilmesini gerekli kılmaktadır. Ne var ki, yapay zekâ teknolojisinin "veri açlığının" tam olarak karşılanması, veri koruma hukuku kuralları yürürlükte olduğu sürece güçtür. Zira veri koruma hukukunun temel ilkelerinden birisi olan veri minimizasyonu (ölçülülük) ilkesi, veri sorumlularının yalnızca amaçlarını gerçekleştirmek bakımından gerekli olan asgari miktarda veriyi işlemlerini gerektirmektedir.

Öte yandan, yapay zekâ teknolojisine yönelik endişe verici bir kamuoyu güveni eksikliği mevcuttur. Örneğin, Avrupa Tüketici Örgütü tarafından 2020 yılında yapılan bir anket, Avrupalıların %45-60'ının yapay zekanın kişisel verilerin daha fazla kötüye kullanılmasına yol açacağına dair endişeleri olduğunu ortaya koymuştur (The European Consumer Organization, 2020).

Yapay zekâ teknolojisinin sunduğu çok sayıda sosyal ve ekonomik avantaj göz önüne alındığında, bu teknolojiyi geliştirenlerin, kanun koyucuların ve veri koruma otoritelerinin, bireyin kişilik hakkının bir parçası olan mahremiyetten ödün vermeden yapay zekâ teknolojisinden yararlanmanın bir yolunu bulmaları gerektiği açıktır. Bu çalışmanın konusunu oluşturan "mahremiyeti artırıcı teknolojiler" (MATlar), söz konusu dengenin sağlanması bakımından önemli avantajlar sunan araçlardır.

Çalışmanın birinci bölümünde MAT kavramı ve özellikle yapay zekâ teknolojisi bakımından önem taşıyan başlıca MAT türleri üzerinde durulacaktır. İkinci bölümde, MATların yapay zekâ ekosistemindeki rolü ile bunların gelişimi ve yaygınlaştırılması önündeki engeller ele alınacaktır. Çalışmanın üçüncü ve son bölümünde ise Türk hukukuna özel politika önerileri sunulacaktır.

MAHREMİYETİ ARTIRICI TEKNOLOJİLER (MATLAR) VE TÜRLERİ

MAT kavramı yeni bir kavram olmamakla birlikte, bu teknoloji grubuna ilişkin evrensel olarak kabul edilmiş bir tanım bulunmamaktadır. Yıllar içinde çeşitli kurum ve kuruluşlar MATları farklı şekillerde tanımlamış ve bu teknolojileri kendi ölçütlerine göre sınıflandırmıştır. [1] OECD'nin yaptığı ve bizim de benimsediğimiz geniş kapsamlı tanıma göre MATlar, mahremiyetin korunmasına yardımcı olan geniş bir teknoloji yelpazesini ifade eder (OECD, 2023).

MATlar, 1990'ların başlarında Kanadalı hukukçu Ann Cavoukian tarafından ortaya atılan "tasarımdan itibaren mahremiyet" (privacy by design) kavramının temelini oluşturan önemli araçlardan birisidir. Bu nedenle, MATların işlevleri ile türlerinin anlaşılabilmesi için öncelikle tasarımdan itibaren mahremiyet kavramı açıklanmalıdır.

Tasarımdan İtibaren Mahremiyet ve MAT İlişkisi

[1] Çeşitli tanımlar ve sınıflandırmalar için bkz. OECD, 2023).

Tasarımdan itibaren mahremiyet, yapay zekâ sistemleri dahil olmak üzere, henüz daha teknolojilerin oluşturulması aşamasında mahremiyetin dikkate alınması ve korunmasına yönelik kapsamlı bir metodolojinin benimsenmesini ifade eder (Rubinstein, 2011). Bu kavramın yaratıcısı olan Ann Cavoukian, konuya ilişkin çığır açıcı makalesinde tasarımdan itibaren mahremiyetin 7 temel ilkesine değinmiştir. Bu ilkeler şunlardır (Cavoukian, 2009):

i. Tepkisel değil, proaktif; tazmin yerine önleyici (*Proactive not Reactive; Preventative not Remedial*)
ii. Varsayılan ayar olarak mahremiyet (*Privacy as the Default*)
iii. Tasarımın içine gömülü mahremiyet (*Privacy Embedded into Design*)
iv. Tam işlevsellik — Sıfır toplamlı değil, kazan-kazan yaklaşımı (*Full Functionality — Positive-Sum, not Zero-Sum*)
v. Uçtan uca güvenlik — Yaşam döngüsü boyunca koruma (*End-to-End Security —Lifecycle Protection*)
vi. Görünürlük ve şeffaflık *(Visibility and Transparency)*
vii. Kullanıcı mahremiyetine saygı *(Respect for User Privacy*)

Tasarımdan itibaren mahremiyet kavramının 1990'larda Cavoukian tarafından oluşturulmasını, 1995 yılında Hollanda ve Kanada Veri Koruma Otoriteleri tarafından hazırlanan *"Mahremiyeti Artıran Teknolojiler - Anonimliğe Giden Yol"* adlı raporun kaleme alınması izlemiştir (Rossum ve Borking, 1995). Bu rapor da alışılagelmiş olan düşüncenin aksine, teknolojinin bireylerin mahremiyetini korumaya hizmet eden bir araç olabileceğini vurgulamıştır (van Blarkom vd., 2003). Bundan 25 yıl sonra, Ekim 2010'da düzenlenen 32. Veri Koruma ve Mahremiyet Komiserleri Konferansı'nda ise *"Tasarımdan İtibaren Mahremiyet Kararı"* kabul edilmiş olup bu karar tasarımdan itibaren mahremiyetin "temel mahremiyet korumasının temel bir bileşeni" olarak benimsendiği önemli bir kilometre taşı olarak kabul edilmektedir (European Data Protection Supervisor, 2018).

Günümüzde tasarımdan itibaren mahremiyet, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GDPR) genel bir ilke olarak kabul edilmektedir. Bu çerçevede, GDPR Madde 25 (1)'e göre, veri sorumlusu, hem işleme araçlarının belirlenmesi sırasında hem de işleme faaliyeti sırasında, ilgili kişilerin haklarının korunması için uygun teknik ve organizasyonel önlemleri almalı ve gerekli tedbirleri veri işleme sürecine entegre etmelidir. İşte bu entegrasyon çoğu zaman, kişisel verilerin korunmasını ve gizliliğini güvence altına almayı hedefleyen MATlar geliştirilmesi ve kullanılmasıyla hayata geçirilir (Oualha, 2025). Nitekim MATlar, veri sisteminin işlevselliğinden ödün vermeksizin mahremiyeti koruduklarından, tasarım yoluyla mahremiyeti sağlamak (Kindt, 2013) ve ilgili kişilerin hak ve çıkarlarını korumak için kullanılabilecek önemli araçlardır (Borking, 2002; Borking ve Raab, 2001).

MATların Sınıflandırılması

Tıpkı MATların tanımı gibi sınıflandırılması konusunda da bir görüş birliği bulunmamaktadır. Buna karşılık, MATların sınıflandırılmasına ilişkin en temel ölçütlerden bir tanesi bunların işlevlerini (anonimleştirme, gizlilik, şeffaflık vb.) dikkate alarak yapılan sınıflandırmadır (Rubinstein, 2011). Bu bağlamda, MATların doğrudan mahremiyeti korumaları veya verilere müdahale etmeksizin gizlilik politikaları yaratarak ya da kullanıcı izinlerini belirleyerek mahremiyeti korumaları mümkündür (AEPD, 2019). Keza bu teknolojiler genellikle tasarımcıları (yazılımcıları) ya da son kullanıcıları tarafından mevcut sistemlere entegre edilmekte (Rubinstein, 2011; AEPD, 2019), donanım veya yazılım yoluyla, kurum içinde ya da bulut ortamında çalışabilmektedir (d'Aliberti vd., 2024).

MATlar literatürde, geleneksel ve yeni nesil olmak üzere iki ana gruba ayrılmaktadır. Geleneksel MATlar şifreleme, tokenizasyon ve k-anonimlik gibi yöntemleri içerirken; yeni nesil MATlar arasında homomorfik şifreleme, güvenilir yürütme ortamları, güvenli çok taraflı hesaplama, diferansiyel gizlilik ve federe veri işleme sistemleri bulunmaktadır (Bada et al., 2023). Bu teknolojilerden bazıları, yapay zekâ sistemlerinin geliştirilmesi ve kullanımı bakımından özel bir önem taşımaktadır (Information

Commissioner's Office, 2023). Zira bunlar, yüksek hacimli ve hassas verilerin işlenmesini mümkün kılarken, aynı zamanda veri koruma hukukunun öngördüğü sınırlamalarla uyumlu çözümler sunmaktadır. Aşağıda, bu bağlamda öne çıkan MAT türleri ayrı ayrı ele alınacaktır.

Sentetik Veriler

Sentetik veriler, gerçek dünyadaki verileri taklit eden yapay olarak oluşturulmuş verilerdir (Information Commissioner's Office, 2023). Gerçek dünya verileri, gözlemlenen (sosyal, ekonomik, biyolojik, fiziksel) olgulardan doğrudan elde edilirken (D'Acquisto, 2024), sentetik veriler, algoritmalar, simülasyonlar veya üretken modeller kullanılarak, gerçek verilerin istatistiksel özelliklerini taklit eden yöntemlerle belirli kullanım senaryoları için üretilir (James vd., 2021; Kosinski, 2025). Bunun anlamı, sentetik veriler kullanılarak yapılan analizler ile gerçek veriler kullanılarak yapılacak analizlerin çok benzer sonuçlar ortaya koymalarıdır (Information Commissioner's Office, 2023); AEPD 2023). Böylelikle, gerçek verilerin kullanılmasına bağlı mahremiyet riskleri ile karşı karşıya kalınmaksızın, gerçek verilerin kullanılmasından beklenen fayda ve sonuçlar elde edilebilmektedir.

Nitekim uygulamada da sentetik verilerin bu potansiyelinden sıklıkla yararlanıldığı görülmektedir. Örneğin, Curai adlı girişim geliştirdiği tıbbi teşhis modelini 400.000 simüle edilmiş tıbbi vaka üzerinden eğitmiştir (Fragkouli vd., 2024); Kurapati ve Gilli, 2023). Bu örnek, sentetik verilerin özellikle yapay zekâ sistemlerinin geliştirilmesinde ve test edilmesinde mahremiyet dostu bir alternatif sunduğunu açık biçimde ortaya koymaktadır.

Bununla birlikte, sentetik verilerin kullanımının mahremiyetin korunmasına ilişkin mutlak bir çözüm sunduğunu söylemek mümkün değildir. Nitekim, gerçek kişilere ait ve doğruluğu yüksek verilere ihtiyaç duyulan hallerde sentetik verilerden faydalanılamamaktadır (CIPL, 2025). Zira sentetik veriler, her ne kadar istatistiksel olarak gerçeğe yakın olsa da, belirli bir gerçek kişinin bireysel özelliklerini birebir yansıtmaz. Bu nedenle, sentetik verilerin hangi kullanım senaryoları bakımından uygun olduğu, her somut olay bakımından ayrıca değerlendirilmelidir.

Homomorfik Şifreleme (Homomorphic Encryption)

Homomorfik şifreleme, kişisel veriler şifreli durumdayken bu veriler üzerinde hesaplama ve işlem yapılmasına imkân tanıyan bir şifreleme yöntemidir (Information Commissioner's Office, 2023; Szekely, 2022). Bu halde, verilerin iletilmesi, işlenmesi ve muhafazası süreçlerinde verilerin şifresi çözülmez. İşlem sonucunda elde edilen çıktı ise yalnızca gizli anahtara sahip olan veri sorumlusu tarafından deşifre edilir. Böylelikle, veriler şifresiz olarak işlenmiş olsaydı hangi sonuç ortaya çıkacak idiyse, homomorfik şifreleme kullanılarak yapılan işlemler sonucunda da işlevsel olarak aynı çıktıya ulaşılması mümkün olur (Lukas, 2023; Information Commissioner's Office, 2023).

Homomorfik şifreleme, özellikle yapay zekâ sistemleri bakımından önemli imkânlar sunmaktadır. Zira bu yolla yapay zekâ modelleri, şifreli veriyi açmadan öğrenebilir veya çıkarımlarda bulunabilir. Bu durum, özellikle kişisel verilerin üçüncü taraflarla paylaşılması veya bulut bilişim altyapılarında işlenmesi gereken senaryolarda, veri güvenliği ve mahremiyet bakımından önemli bir avantaj sağlar. Örneğin bir hastane, hasta verilerini homomorfik olarak şifreledikten sonra, bu verileri bulut tabanlı bir yapay zekâ modeline aktarabilir. Yapay zekâ modeli, verilerin içeriğini hiçbir zaman görmeden, şifreli veriler üzerinde kanser teşhisine yönelik bir tahmin algoritmasını eğitebilir veya çalıştırabilir. Bu süreçte, hastalara ait hassas veriler hiçbir aşamada şifresiz hâle gelmediği için, veri ihlali ve kötüye kullanım riski önemli ölçüde azaltılmış olur.

Bununla birlikte, günümüzde homomorfik şifreleme hâlâ oldukça yüksek zaman ve bellek gereksinimleri doğuran bir teknolojidir. Şifreli veriler üzerinde yapılan hesaplamalar, şifresiz verilere

kıyasla çok daha uzun sürede tamamlanmakta ve ciddi hesaplama maliyetleri yaratmaktadır (Lukas, 2023). Bu nedenle, homomorfik şifrelemenin büyük ölçekli veri setleri ve karmaşık modeller söz konusu olduğunda pratik bir çözüm sunduğunu söylemek güçtür (d'Aliberti vd., 2024). Bu çerçevede, yapay zekâ bağlamında homomorfik şifrelemeye başvurulması, çıkarım süresinin uzamasının kabul edilebilir olduğu durumlarda, daha küçük modeller üzerinde güvenli çıkarım (inference) yapılmak istenen hallerde pratik açıdan mümkündür (Information Commissioner's Office, 2023). Bununla birlikte, zaman ve alan gereksinimlerinin azaltılmasına yönelik çalışmaların devam etmesi, homomorfik şifrelemenin yakın gelecekte çok daha verimli hale gelmesini sağlayabilir (d'Aliberti vd., 2024).

Farklılaştırılmış Gizlilik (Differential Privacy)

Farklılaştırılmış gizlilik, verilere "gürültü" eklenerek ilgili kişilerin tespit imkanını ortadan kaldıran veya son derece güç hale getiren teknik bir mahremiyet arttırıcı çözümdür. Bu yöntemin amacı bir yandan mahremiyeti korurken diğer yandan verilerden genel, istatistiki bilgiler elde edilmesini mümkün kılmaktır (Auñón, 2024; Lukas, 2023). Örneğin, Apple, iPhone kullanıcılarının genel yazım eğilimlerini —örneğin belirli kelimelerin ne sıklıkla kullanıldığını— analiz edebilmek için, her kullanıcının verisine rastgele ve küçük hatalar (gürültü) eklemektedir. Bu sayede Apple, hiçbir kullanıcının bireysel olarak ne yazdığını bilmeden, kullanıcı kitlesinin genel davranışlarına ilişkin istatistiksel çıkarımlar yapabilmektedir. Keza, farklılaştırılmış gizlilikten faydalanılarak farklı kişilerin tıbbi verileri arasındaki istatistiki korelasyon tespit edilebilir ve bu bulgular ışığında yeni tedavi yöntemleri de geliştirilebilir (Lukas, 2023).

Farklılaştırılmış gizliliğin önemli bir özelliği, eklenen gürültüye rağmen, modellerin topluluğun geneli hakkında yeterli doğrulukta çıkarım yapabilmesine imkân tanımasıdır. Bu nedenle söz konusu yöntem, özellikle derin öğrenme ve federe öğrenme gibi modern yapay zekâ yaklaşımlarında da yaygın biçimde kullanılmaktadır (Auñón, 2024). Bu halde model, tek tek bireyler hakkında değil; genel eğilimler ve dağılımlar hakkında öğrenme gerçekleştirdiği için, kişisel verilerin açığa çıkma riski önemli ölçüde sınırlandırılmaktadır.

Bununla birlikte, farklılaştırılmış gizlilik kaçınılmaz bir doğruluk–mahremiyet dengesi sorununu da beraberinde getirir. Verilere eklenen gürültü arttıkça, ilgili kişilerin tespit edilmesi zorlaşır; ancak aynı zamanda elde edilen sonuçların doğruluk düzeyi de düşer (Lukas, 2023). Bu nedenle, istatistiksel olarak anlamlı ve güvenilir sonuçlara ulaşılabilmesi için genellikle geniş veri setlerine ihtiyaç duyulur (Szekely, 2022). Küçük ölçekli veri setlerinde, eklenen gürültü analiz sonuçlarını işlevsiz hâle getirebilir.

Son olarak, aynı kişiden uzun süre boyunca ve tekrar tekrar veri toplanması hâlinde, farklılaştırılmış gizliliğin mahremiyeti koruyucu etkisinin zayıflayabileceği de kabul edilmektedir (Szekely, 2022). Bu nedenle yöntemin etkinliği, gürültü seviyesi, veri toplama sıklığı ve veri minimizasyonu ilkeleriyle birlikte değerlendirilmelidir.

Federe Öğrenme (Federated Learning)

Geleneksel olarak, yapay zekâ modelleri üzerinde iş birliği yapılması, taraflar arasında yüksek düzeyde güven gerektirir. Zira model tarafından kullanılacak verilerin paylaşımı, her bir tarafın diğerlerinin hassas bilgilerine erişebilmesi anlamına gelir. Federe öğrenme ise bu güven ihtiyacını önemli ölçüde azaltır: tarafların verilerini paylaşmadan ortak bir model oluşturmasına, böylece hem yapay zekâ geliştirme sürecinin ilerlemesine hem de kişisel verilerin korunmasına hizmet eder (d'Aliberti vd., 2024). Bu durum özellikle, finans ve sağlık gibi yoğun şekilde regüle edilen ve siber güvenlik gibi hassas verilerin işlendiği alanlarda federe öğrenmenin önemini arttırmaktadır (OECD, 2025).

Federe öğrenme, veriler tek bir merkezde toplanmadan, birden çok cihaz veya kurumun kendi verileri üzerinde model eğitimi yaptığı ve diğer paydaşlarla ham veriyi değil, model güncellemelerini paylaştığı bir dağıtık yapay zekâ yöntemidir (Auñón, 2024). Bu yöntemde, yapay zekayı eğitecek algoritmalar her bir kurumun/kullanıcının, kendi cihazına yüklenmektedir. Keza işlenecek veriler de her bir kullanıcının kendi cihazı içinde kalmaya devam eder. Böylelikle, hiçbir katılımcı diğerinin verisine erişmeksizin, her katılımcı kendi yerel veri setiyle modelini eğitmekte ve ardından eğitilmiş modeli —ve modeli eğitmekte kullandığı veri miktarına ilişkin bilgiyi— merkezi sunucuya göndermektedir. Sunucu ise, bu modelleri birleştirmekte ve ortaya çıkan birleşik modeli tüm katılımcılarla paylaşmaktadır. Böylelikle, birden fazla veri sorumlusu verilerini yerel olarak tutarken ortak bir yapay zekâ modeli geliştirebilmektedir (d'Aliberti vd., 2024).

Örneğin, Google, Google Asistan hizmetini çalıştıran konuşma modellerini eğitmek için federe öğrenme yönteminden yararlanmaktadır. Bu kapsamda, kullanıcıların ses verileri Google'ın merkezi sunucularına aktarılmak yerine, doğrudan kullanıcıların kendi cihazlarında saklanmakta, bu veriler üzerinde, modelin nasıl geliştirilebileceğini öğrenmek üzere yerel eğitim algoritmaları çalıştırılmaktadır. Daha sonra, bu yerel eğitimden elde edilen öğrenme çıktılarının özetleri Google'ın sunucularına gönderilmekte ve burada diğer cihazlardan gelen güncellemelerle birleştirilerek yeni ve daha gelişmiş bir konuşma modeli oluşturulmaktadır (Google, 2025).

Bununla birlikte, federe öğrenme mutlak bir mahremiyet garantisi sunmamaktadır. Taraflardan birisinin, paylaşılan model güncellemelerinden hareketle, orijinal veri setlerinde yer alan kişisel verilere ilişkin çıkarım yapabilmesi teorik olarak mümkündür. Bu nedenle, verilerin yeniden tanımlanması (de-anonymization) riskini tamamen ortadan kaldırmak için federe öğrenmenin, farklılaştırılmış gizlilik veya homomorfik şifrelem gibi başka bir gizliliği artırıcı teknolojiyle birlikte uygulanması önerilmektedir (Information Commissioner's Office, 2023; d'Aliberti vd., 2024; Lukas, 2023).

Güvenli Çok Taraflı Hesaplama (Secure Multi-Party Computation)

Güvenli çok taraflı hesaplama, birden fazla tarafın elindeki gizli verileri birbirleriyle paylaşmadan birlikte hesaplama yapmasına imkân tanıyan bir protokoldür (Information Commissioner's Office, 2023). Bu yöntem, taraflar arasındaki güven eksikliği, veri koruma hukukuna uyum ihtiyacı veya verileri birlikte işlemek isteyen taraflarca karşılaşılan teknik engellere çözüm olarak geliştirilmiştir (Szekely, 2022). Bu bağlamda, federe öğrenmeye benzemekle birlikte, federe öğrenmeden temel farkı, veriler üzerinden ortak bir yapay zekâ modelinin eğitilmesini amaçlamaması; fakat tarafların gizli verileri paylaşmaları gerekmeksizin önceden tanımlanmış bir hesaplama sonucuna ulaşılmayı hedeflemesidir.

Bu yöntemin temel mantığı, kişisel verilerin tek bir merkezde toplanmasını gereksiz kılmasıdır (Szekely, 2022). Zira her taraf yalnızca kendi elindeki veriler üzerinde işlem yapar; hesaplama süreci boyunca ham veriler hiçbir aşamada diğer taraflara açılmaz. Taraflar arasında paylaşılan tek unsur ise hesaplamanın sonucudur (Lukas 2023; Information Commissioner's Office, 2023). Örneğin iki banka, müşteri verilerini birbirleriyle paylaşmaksızın, ortak bir dolandırıcılık tespit modeli geliştirmek isteyebilir. Bu senaryoda her banka, kendi müşteri verileriyle hesaplamaya katılır; sistem, tarafların bireysel verilerine erişmeden yalnızca ortak bir risk skoru veya tahmin sonucu üretir ve bu sonucu taraflara sunar. Böylece veri setleri ifşa edilmeden ve bundan doğabilecek güvenlik risklerine maruz kalınmadan iş birliği mümkün hâle gelir.

Güvenli çok taraflı hesaplama kişisel verileri ileri düzeyde korumaktaysa da pratik kullanım açısından bazı sınırlamalar da barındırmaktadır. Özellikle, iletişim maliyetleri ve hesaplama yönteminin kompleks niteliği nedeniyle sınırlı işlem kapasitesi olan hallerde ve büyük ölçekte hızlı hesaplama ihtiyacı olan durumlarda bu yöntemin kullanılması pratik açıdan güçtür (Lukas, 2023; Auñón, 2024). Bununla birlikte, bu yöntemin kişisel verileri yalnızca hesaplama yapılırken koruduğu da gözden

kaçırılmamalıdır. Zira hesaplama sonucunda elde edilen çıktı, belirli bir kişiyle ilişkilendirilebilir nitelikteyse, bu sonucun kendisi de kişisel veri veya hatta özel nitelikli kişisel veri niteliği taşıyabilir (Lukas, 2023; Information Commissioner's Office, 2023).

Güvenilir Yürütme Ortamı (Trusted Execution Environment)

Güvenilir yürütme ortamı, bir bilgisayar sisteminin işlemcisi içinde yer alan, sistemin geri kalanından ayrı, güvenli ve izole bir donanım alanıdır. Güvenilir yürütme ortamı dışındaki uygulamalar bu ortamdaki verilere erişemez, bu verileri değiştiremez ve silemez. Ayrıca, bu güvenli alanda veriler şifrelenmeksizin ve gürültü eklenmeksizin işlenebilir (Information Commissioner's Office, 2023).

Bu özellikleri nedeniyle güvenilir yürütme ortamları, büyük ölçekli veri analizi ve makine öğrenimi uygulamaları bakımından da önemli bir potansiyele sahiptir. Özellikle yapay zekâ modellerinin eğitimi ve çalıştırılması sırasında hem veri gizliliğinin korunması hem de hesaplama performansından ödün verilmemesi gereken senaryolarda güvenilir yürütme ortamları tercih edilmektedir. Örneğin bir sağlık uygulaması, hasta verilerini bulut ortamında çalışan bir yapay zekâ modeline gönderebilir. Bu senaryoda veriler, yalnızca güvenilir yürütme ortamı içinde açılır ve işlenir; bulut hizmet sağlayıcısı dâhil olmak üzere, hiçbir üçüncü taraf bu verilere erişemez. Böylece, hassas sağlık verileri üzerinde yüksek doğrulukta analizler yapılırken, veri ihlali ve yetkisiz erişim riskleri önemli ölçüde azaltılmış olur.

MATLARIN YAPAY ZEKÂ EKOSİSTEMİNDEKİ ROLÜ VE UYGULAMA SINIRLARI

MAT'lar, yapay zekâ yaşam döngüsünün farklı aşamalarında sundukları çeşitli işlevlerle tasarımdan itibaren mahremiyet ilkesinin uygulanmasında önemli bir araç niteliği taşımaktadır. Bununla birlikte, tüm potansiyellerine rağmen bu teknolojilerin geniş ölçekte benimsenmesini sınırlayan yapısal, ekonomik ve hukuki engeller de mevcuttur. Bu nedenle, aşağıda, önce mahremiyetin korunmasını esas alan bir yapay zekâ ekosistemi bakımından MAT'ların işlevleri ele alınacak; ardından bu teknolojilerin geliştirilmesi ve yaygınlaştırılmasının önünde duran başlıca sorunlar incelenecektir.

Veri Koruma Hukuku ile Yapay Zekâ Çatışmasında MATların İşlevleri

Yapay zekâ sistemleri, yüksek doğrulukta sonuçlar üretebilmek için geniş ve çeşitli veri setlerine ihtiyaç duymakta, bu durum ise mahremiyet, veri güvenliği ve bireylerin kişisel verileri üzerindeki hâkimiyeti bakımından ciddi riskleri beraberinde getirmektedir. Bunun neticesinde, inovasyonun sürdürülmesi ile mahremiyetin korunması arasında zorunlu bir tercih yapılması gerektiği düşüncesi gündeme gelmektedir. Bu fikre karşı çıkan, Cavoukian, mahremiyet ile inovasyon arasında mevcut olduğu varsayılan gerilimin aslında zorunlu olmadığını, bu ikisi arasındaki dengenin sağlanmasının ve özellikle yapay zekâ teknolojilerine ilişkin kamu güveninin tesis edilmesinin yolunun "tasarımdan itibaren mahremiyet" yaklaşımı olduğunu savunmaktadır (Borealis AI, 2020). MATlar ise tasarımdan itibaren mahremiyet ilkesinin gerçek dünya sistemlerine entegre edilmesinde önemli bir rol üstlenmektedir.

Cavoukian'ın, tasarımdan itibaren mahremiyete ilişkin olarak ortaya koyduğu yedi ilke arasından, "tam işlevsellik – sıfır toplam değil, pozitif toplam" ilkesi çalışmamız bakımından özellikle önemlidir. Zira bu ilke, veri koruma hukukuna uygun inovasyonun önünü açan temel bir varsayıma dayanır: Mahremiyetin korunması, sistemin işlevselliğinden veya performansından zorunlu olarak feragat edilmesini gerektirmez (Cavoukian, 2009). Başka bir deyişle, bu ilke "mahremiyet ve güvenlik" ya da "mahremiyet ve işlev" arasında bir tercih yapılması gerekmediğini ve her ikisine de sahip olmanın sadece arzu edilen değil, aynı zamanda mümkün bir sonuç olduğunu vurgulamaktadır (Cavoukian, 2009). Bu bağlamda, doğru teknik araçlar kullanıldığında, hem yüksek işlevsellik hem de güçlü mahremiyet koruması eş zamanlı olarak mümkün olabilecektir. İşte MATlar tam da bu pozitif toplam yaklaşımını teknik düzeyde hayata geçiren çözümler sunmaktadır.

Bu yaklaşımın yapay zekâ teknolojilerinin gelişimi bakımından taşıdığı önem, makine öğrenimi algoritmalarının doğasıyla doğrudan bağlantılıdır. Zira algoritmalar, anlamlı örüntüler ve güvenilir tahminler üretebilmek için genellikle geniş ve zengin içerikli veri setlerine ihtiyaç duyar. Bu veri setleri ise çoğu zaman isim, adres, yaş, cinsiyet, sağlık durumu ve finansal bilgiler gibi kişisel verileri ve hatta özel nitelikli verileri içermektedir. Ne var ki, yapay zekâ modellerinin eğitilmesi için çoğu durumunda bu verilere ihtiyaç bulunmamaktadır. Bu modellerin başarısı çoğu durumda, temel veri kümesindeki kişiye özel ayrıntılardan ziyade, genel dağılımlar, ilişkiler ve istatistiksel kalıplar üzerinden şekillenmektedir. MAT'lar, bu noktada, kişiye özgü ayrıntıları maskeleyerek, yapay zekâ modellerinin eğitilmesini mümkün kılmaktadır (Dulberg, 2021). Ayrıca, bu teknolojiler, farklı kurum ve sektörler arasında verilerin daha geniş ölçekte ve daha güvenli biçimde paylaşılmasını mümkün kılarak, yapay zekâ çözümlerinin benimsenmesini, yaygınlaşmasını ve gelişmesini de teşvik etmektedir (CNIL, 2025).

Bu yaklaşım, düzenleyici kurumlar tarafından da giderek daha açık biçimde benimsenmektedir. Örneğin, Birleşik Krallık Bilgi Komiserliği'nin (ICO) yakın tarihli çalışmalarında, MATların kişisel veri kullanımını en aza indirdiği, bilgi güvenliğini üst düzeye çıkardığı ve ilgili kişilerin verileri üzerindeki hâkimiyetini güçlendirdiği özellikle vurgulanmaktadır. Buna göre MATlar, bir yandan kişilerin mahremiyetinin korunmasını sağlarken, diğer yandan veri kümelerine erişimi ve bu verilerden değerli içgörülerin çıkarılmasını mümkün kılmaktadır (Information Commissioner's Office, 2023).

Gerçekten de MATlar, verinin kendisine erişimi olmayan kişilerin dahi, kişisel verilerden anlamlı ve faydalı çıkarımlar elde edebilmelerini sağlamaktadır (Macgillivray, 2022). Bu kişiler, temel veri kümesindeki kişiye özel ayrıntılara değil, geniş veri modellerine ve bu veriden elde edilen sonuca eriştiklerinden, ilgili kişilerin mahremiyetinin zarar görmesi riski önemli ölçüde azalmaktadır. Bu bağlamda, MATların vaat edildiği şekilde çalıştığı bir senaryoda, araştırmacıların, doktorların ve bilim insanlarının kişisel verinin kendisine erişmeden de bilimsel ve toplumsal açıdan değerli içgörüler elde etmeleri mümkün olacaktır. ICO'nun da ifade ettiği üzere, böyle bir yapı, kişisel veri kullanımını asgari seviyeye indirirken, veri güvenliğini en üst düzeye çıkaracak ve bireylere kendi verileri üzerinde daha fazla kontrol imkânı tanıyacaktır.

MATların, mahremiyetin koruması dışında birtakım dolaylı işlevleri de bulunmaktadır. Mahremiyeti daha tasarım aşamasında sistemlerine entegre eden kuruluşlar, mahremiyeti korurken aynı zamanda ekonomik değer yaratma imkânına da sahip olmaktadır (Cavoukian vd., 2010). Keza tasarımdan itibaren mahremiyet yaklaşımı, ilgili kişilere verileri üzerinde daha güçlü bir hâkimiyet sağlarken, veri işleyen kuruluşlara da güven temelli bir rekabet avantajı sunar (Nampiina, 2020; PDPC, 2024). Bunun yanında MATlar, kamu verilerinin erişilebilirliğini artırmak ve güvenlik ile gizlilikten ödün vermeksizin özel sektör veri paylaşımını teşvik etmek bakımından da önemli işlevler üstlenmektedir (Obermeyer, 2021).

Bununla birlikte, farklı MAT türlerinin yapay zekâ yaşam döngüsünde farklı işlevlere sahip olduğu ve her MATın her ihtiyaca yanıt vermediği özellikle vurgulanmalıdır. Örneğin, sentetik veri ve farklılaştırılmış gizlilik, ilgili kişiye erişimi güçleştirmeyi amaçlayan MATlardır. Bu nedenle, belirli bir hastaya özgü teşhis ve tedavi sunmayı hedefleyen bir hastanenin, sentetik verilerden doğrudan yararlanması mümkün olmayabilir. Zira, hastanın kimliğinin bilinmemesi, doğru ve bireyselleştirilmiş bir tedavinin uygulanmasını engel olacaktır. Buna karşılık, aynı hastane, bir hastalığın tedavisine ilişkin genel bilimsel araştırmalar yürüten araştırmacılara veri sağlamak istediğinde, sentetik veriler son derece işlevsel bir araç hâline gelebilir (Information Commissioner's Office, 2023). Bu durum, MAT seçiminde ihtiyaca ve bağlama duyarlı bir değerlendirme yapılmasının zorunlu olduğunu göstermektedir. Dolayısıyla işletmelerin, veri akışlarını, potansiyel riskleri ve üçüncü taraflarla olan ilişkilerini dikkate alarak, kendileri için en uygun MAT kombinasyonunu belirlemeleri gerekmektedir (Srouji ve Mechler, 2020).

Bu bağlamda, çalışmamızda ele alınan MATların yapay zekâ yaşam döngüsündeki işlevleri aşağıdaki tabloda özetlenmektedir:

Tablo 1: MATların Yapay Zekâ Yaşam Döngüsünde İşlevleri (CIPL, 2025):

	İŞLEV					
	Veri Kaynağı	**Model Eğitimi**	**Güvenlik**	**İşbirliği**	**Model Doğrulama**	**Model Dağıtımı**
Sentetik veri	X	X			X	
Homomorfik Şifreleme		X	X	X	X	X
Farklılaştırılmış Gizlilik		X	X	X	X	X
Federe Öğrenme		X	X	X		X
Güvenilir Yürütme Ortamı		X	X	X	X	X
Güvenli Çok Taraflı Hesaplama		X	X	X	X	

Son olarak, MATların tüm mahremiyet ve veri koruma sorunlarını tek başına çözecek bir "sihirli değnek" olarak görülmemesi gerekir. Örneğin, MAT'lar, orijinal veri setlerinde mevcut olan önyargıların ortadan kaldırılmasına doğrudan katkı sunmazlar. Aynı şekilde, MAT kullanımı, bu veriler üzerine inşa edilen tüm bilgi teknolojileri sistemlerinin bütünüyle güvenli olduğu anlamına da gelmez (OECD, 2023). Bu nedenle MAT'lar, hukuki, kurumsal ve organizasyonel önlemlerle birlikte ele alınması gereken tamamlayıcı araçlar olarak değerlendirilmelidir.

MATların Yaygınlaşması ve Kullanımı Önündeki Sorunları

MATların potansiyeli giderek daha geniş çevrelerde kabul görmesine rağmen, bu teknolojilerin yaygın ve sürdürülebilir bir biçimde benimsenmesi önünde önemli engeller bulunmaktadır. Bunların başında, MATların geliştirilmesine ilişkin yüksek maliyetler gelmektedir. Birçok MAT ileri düzey uzmanlık, ciddi araştırma kapasitesi ve uzun Ar-Ge süreçleri gerektirdiğinden, kuruluşlar açısından önemli bir yatırım yükü doğurur. Bu maliyetler, özellikle küçük ve orta ölçekli işletmeler için MAT geliştirmeyi veya mevcut sistemlere entegre etmeyi zorlaştırmaktadır.

Bir diğer temel sorun ise talep eksikliğidir. Ekonomik teşviklerin yetersiz olduğu ortamlarda özel sektörün MATlara yönelme motivasyonu zayıflamaktadır. Geliştiriciler, kısa vadede doğrudan gelir yaratmayan bu teknolojilere yatırım yapma konusunda isteksiz davranabilmektedir. MATların sağlayacağı uzun vadeli faydalar ise çoğu zaman yeterince görünür olmadığı için piyasa talebi doğal olarak oluşmamakta, bu da inovasyonun hızını yavaşlatmaktadır.

Son olarak, hukuki belirsizlik MATların benimsenmesini ciddi ölçüde sınırlayan bir diğer önemli faktördür. Mevzuatta MAT kullanımına ilişkin açık ve yönlendirici hükümler bulunmadığı için, veri sorumluları hangi teknolojinin, hangi şartlar altında hukuki riskleri azaltacağını net biçimde öngörememektedir. Örneğin, belirli bir şifreleme tekniğinin veri koruma yükümlülüklerini ne ölçüde karşıladığı veya sorumluluğu ne ölçüde azaltacağı konusunda rehberlik eksikliği, yatırım kararlarını doğrudan etkilemektedir. Bu nedenle, hukuki çerçevenin belirsizliği hem geliştiriciler hem de kullanıcılar yönünden ihtiyaç duyulan teşviki sağlamamakta, MATların pratikte yaygınlaşmasının önünde önemli bir engel oluşturmaktadır.

TÜRK HUKUKU BAKIMINDAN MATLARA İLİŞKİN POLİTİKA ÖNERİLERİ

MATların yaygınlaştırılması ve etkin biçimde kullanılması, yalnızca teknik bir tercih değil, aynı zamanda hukuk politikası meselesidir. Nitekim, Avrupa Veri Koruma Denetmeni konuyla ilgili ön görüşünde, Avrupa Birliği kurumlarına ve üye devletlere, tasarımdan itibaren mahremiyet yaklaşımını ve MATların kullanımını - gerekli uygulama tedbirleri ve politika girişimleri yoluyla - teşvik etmeleri yönünde açık tavsiyelerde bulunmuştur (European Data Protection Supervisor, 2018).

Bununla birlikte, literatürde tasarımdan itibaren mahremiyetin muğlak bir kavram olduğu ve bu kavramsal belirsizliğin mühendislik pratiğine aktarım sırasında ciddi sorunlara yol açtığı sıklıkla dile getirilmektedir (Morales-Trujillo, 2019; Gustavsson, 2020; Gürses vd., 2007). Bu teknolojilerin son derece teknik yapısı, onları geliştiren mühendislerle bunların nasıl kullanılacağına yön verecek politika yapıcılar arasında ciddi bir "dil bariyeri" oluşturmakta ve böylece benimsenmelerini zorlaştırmaktadır (OECD, 2023). Benzer şekilde, veri sorumlularının, tasarımdan itibaren mahremiyet prensibine uyum sağlamak için somut olarak hangi adımları atmaları gerektiği konusunda yeterli yönlendirmeden yoksun oldukları ileri sürülmektedir (Rubinstein, 2018). Buna ek olarak, literatürde, tasarımdan itibaren mahremiyet yaklaşımının hayata geçirilmesini destekleyecek düzenleyici ve ekonomik teşviklerin yetersiz kaldığı, özellikle firmaları mahremiyeti koruyan teknolojilere yatırım yapmaya yönlendirecek etkili ekonomik mekanizmaların bulunmadığı yönünde güçlü eleştiriler dile getirilmektedir (Hustinx, 2010; Rubinstein, 2011; van Lieshout vd., 2011). Öte yandan, araştırmalar, mahremiyetlerinin korunmasına yönelik tüketici talebinin de düşük olduğunu göstermektedir (London Economics, 2010; van Rest, 2012). Keza, firmalar üzerindeki itibar kaybı baskısı da firmaları MATlara yatırım yapmaya itecek kadar zorlayıcı değildir (Rubinstein, 2011).

Bu eleştiriler, tüm dünyada yasa koyucuların ve veri koruma otoritelerinin, yapay zekâ teknolojisini kullanırken MATların kullanımını teşvik etmedeki rollerini daha etkin şekilde yerine getirmeleri gerektiğini göstermektedir. Nitekim, MATların yaygınlaşabilmesi ve bu teknolojilerden tam anlamıyla faydalanılabilmesi için, hukuki kesinlik sağlayan ve teşvik edici bir yasal zeminin oluşturulması gereklidir. Bu da soyut ilke ve hedeflerin ötesine geçilerek, somut politika araçlarının ve düzenleyici teşviklerin geliştirilmesini zorunlu kılmaktadır.

Kanımızca, ülkemizde MATların gelişimini teşvik etmek amacıyla atılması gereken ilk adım, Kişisel Verileri Koruma Kurumu tarafından konu hakkında bir düzenleyici rehber yayımlanması ve böylelikle hukuki öngörülebilirliğin sağlanmasıdır. Nitekim, MATlara yatırım yapılması ve bunların kullanımının yaygınlaşması için ilk olarak hukuki öngörülebilirliğe ve teşvike ihtiyaç vardır. Bu nedenle, MATları özellikle veri minimizasyonu ilkesi ve veri sorumlularının idari ve teknik tedbirler alma yükümlülükleri çerçevesinde ele alan bir rehber yayımlaması, uygulamayı doğrudan teşvik edici bir etki yaratacaktır. Keza, bazı MAT türlerinin kullanımının anonimleştirmeye eşdeğer sayılıp sayılmayacağı gibi kritik soruların açıklığa kavuşturulması, veri sorumlularının risk algısını önemli ölçüde şekillendirecektir (CIPL, 2023).

Buna ek olarak, MATları etkin şekilde kullanan kuruluşlara, olası bir ihlal durumunda daha düşük yaptırım uygulanması esasının benimsenmesi de bu araçların benimsenmesini teşvik edecektir. Bu tür düzenlemeler, yalnızca uyumu teşvik etmekle kalmayacak; aynı zamanda özel sektörün bu teknolojileri geliştirmeye yönelik temel ve uygulama odaklı araştırmalara yatırım yapmasını da özendirecektir (CIPL, 2025).

Ayrıca, MATların hesap verilebilirliğin somut bir unsuru olarak kabul edilmesi, veri sorumlularının uyum çabalarını güçlendirecek ve güven tesisine katkı sağlayacaktır. Zira, MAT kullanan kuruluşlar, bu yolla hem mahremiyeti korumaya yönelik taahhütlerini görünür kılabilecek hem de verinin yararlı

kullanımını sistemli, sürdürülebilir ve denetlenebilir bir çerçeve içinde gerçekleştirebilecektir (CIPL, 2025).

MATların mahremiyeti koruyucu etkisinden fiilen yararlanılabilmesi, bu teknolojilerin uygulamada kullanılabilir ve erişilebilir olmasına bağlıdır. MATlar, veri sorumluları tarafından yeterince bilinmediği, maliyetli olduğu veya pazarda erişilebilir olmadığı sürece, beklenen işlevlerini yerine getiremeyecektir. Bu nedenle politika yapıcıların, yalnızca hukuki çerçeveyi değil, aynı zamanda bu teknolojileri geliştirenler ile kullananların ekonomik ve pratik ihtiyaçlarını da dikkate alan bütüncül teşvik mekanizmaları oluşturması gerekir. Ancak, MATların yaygınlaşmasının serbest piyasa dinamiklerine bırakılması gerçekçi görünmemektedir. Zira bu alanda ne yeterli arz ne de güçlü bir talep mevcuttur. Bununla birlikte, teknolojinin hızlı evrimi dikkate alındığında, belirli MATların kullanımının doğrudan zorunlu kılınması da arzu edilen sonucu doğurmayabilir. Daha dengeli bir çözüm, geliştiriciler bakımından asgari teknik standartların belirlenmesi ve MAT kullanımını özendiren hukuki ve ekonomik teşviklerin birlikte tasarlanmasıdır (Hornung, 2013).

Bu çerçevede, kalite damgaları ve sertifikasyon mekanizmaları, MATların geliştirilmesi ve kullanımı bakımından etkili bir teşvik aracı olabilir (Hornung, 2013). Benzer şekilde, MAT odaklı araştırmalara yönelik kamu fonlarının artırılması (Hornung, 2013): 184; OECD, 2023), ödüllü yarışmalar düzenlenmesi (OECD, 2025) ve araştırmacılara araştırma fonu destekleri sağlanması (OECD, 2025), bu alandaki yenilikçiliği destekleyecektir. Ayrıca, düzenleyici kum havuzları (regulatory sandboxes) aracılığıyla teşebbüslere, hukuki yaptırımlara maruz kalmaksızın kontrollü bir ortamda MATları test etme imkânı tanınması da önem taşımaktadır (CNIL, 2025; OECD, 2025). [2]

Kamu alımlarında mahremiyeti koruyan ürün ve hizmetlerin tercih edilmesi de MAT ekosisteminin gelişiminde tamamlayıcı bir rol oynayacaktır (OECD, 2025). Keza, endüstri standartlarının oluşturulması, farklı MATların birbiriyle uyumlu ve birlikte çalışabilir hâle gelmesini sağlayacağından ve en iyi uygulamaları standartlaştırarak MATların teknik güvenilirliğini ve olgunluk düzeyini güvence altına alacağından önemlidir (CIPL, 2025).

Son olarak, bu sürecin başarısı akademi, sanayi, KOBİ'ler ve kamu otoriteleri arasında çok paydaşlı iş birliğinin kurulmasına bağlıdır. Nitekim, MATların gelişimi, farklı sektörlerden ve uzmanlık alanlarından gelen paydaşların kollektif uzmanlığı ve işbirliğinden faydalanılmasını gerektirmektedir (OECD, 2025; CNIL, 2025).

SONUÇ

Yapay zekâ teknolojisinin gelişimi, veri işleme kapasitemizde bir sıçrama yaratarak toplumsal refahın artması, bilginin yayılması ve ekonomik değer üretilmesi bakımından kayda değer bir potansiyeli ortaya çıkarmıştır. Ne var ki, temelde istatistiksel öğrenmeye dayanan bu sistemler, kendi kendine öğrenebilmek, çıkarım yapabilmek ve karar süreçlerini besleyebilmek için sağlık kayıtlarından finansal işlemlere uzanan geniş bir yelpazede yüksek hacimli veriye ihtiyaç duymaktadır.

Buna karşılık, yapay zekâ sistemlerinin işlediği verilerin önemli bir kısmı kişisel veri niteliği taşımakta ve bu durum, yapay zekâ temelli veri işleme faaliyetlerinin veri koruma hukukuna uygun yürütülmesini zorunlu kılmaktadır. Ancak yapay zekânın "veri açlığı" ile veri koruma hukukunun veri minimizasyonu başta olmak üzere temel ilkeleri arasındaki gerilim, yalnızca hukuki bir uyum problemine

[2] Farklı ülkelerde düzenleyici kum havuzlarının kullanımına ilişkin örnekler için bkz. OECD, 2023.

indirgenemeyecek ölçüde yapısal bir nitelik taşımaktadır. Bu gerilim aynı zamanda kamuoyu güvenini de doğrudan etkilemektedir.

Bu nedenle, kanun koyucuların ve veri koruma otoritelerinin, bireyin kişilik hakkının bir parçası olan mahremiyetten ödün vermeden yapay zekâdan yararlanmayı mümkün kılan bir çerçeve inşa etmeleri gerekmektedir. MATlar, tam da bu noktada, mahremiyeti ve güvenliği güçlendirirken inovasyonun önünü açabilen "pozitif toplamlı" çözümler sunmaktadır. Ancak MAT'ların vaat ettikleri faydanın gerçekleşmesi, bu teknolojilerin teknik imkânlarının ötesinde, hukuki kesinlik, düzenleyici rehberlik ve doğru teşvik mekanizmalarıyla desteklenen bir ekosistemin kurulmasına bağlıdır. Bu çalışma, Türk hukuku bakımından söz konusu ekosistemin inşasına katkı sunabilecek politika araçlarını görünür kılmayı amaçlamaktadır.

KAYNAKÇA

AEPD. (2019). *A Guide to Privacy by Design*. https://www.aepd.es/guides/guide-to-privacy-by-design.pdf Son erişim tarihi: 4 Haziran 2025.

AEPD. (2023). *Synthetic data and data protection*. https://www.aepd.es/en/prensa-y-comunicacion/blog/synthetic-data-and-data-protection Son erişim tarihi: 17 Mart 2025.

Aksoy, H. C. (2022). Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme. *Kişisel Verileri Koruma Dergisi*, 4(2).

Bada, M., et al. (2023). Supporting Small and Medium-Sized Enterprises in Using Privacy Enhancing Technologies. A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (ss. 274–289). Cham: Springer. https://doi.org/10.1007/978-3-031-35822-7_19

Borealis AI. (2020). *RESPECT AI: Privacy, by design*. https://www.borealisai.com/news/respect-ai-privacy-design/ Son erişim tarihi: 4 Haziran 2025.

Borking, J., & Raab, C. D. (2001). Laws, PETs and Other Technologies for Privacy Protection. *The Journal of Information, Law and Technology*, 2001(1).

Borking, J. (2002). The Status of Privacy Enhancing Technologies – (PET) Online and Offline. E. Nardelli, S. Posadziejewski & M. Talamo (Eds.), *Certification and Security in E-Services – From E-Government to E-Business*. Boston: Springer.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. UC Santa Cruz. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf Son erişim tarihi: 2 Haziran 2025.

Cavoukian, A., et al. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society*, 3(2), 405–413.

Cavoukian, A. (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf Son erişim tarihi: 2 Haziran 2025.

CIPL. (2025). *Privacy-Enhancing and Privacy-Preserving Technologies in AI: Enabling Data Use and Operationalizing Privacy by Design and Default*. Mart 2025.

D'Acquisto, G. (2024). Synthetic data and data protection laws. *Journal of Data Protection & Privacy*, 6(3), 227–239.

d'Aliberti, L., et al. (2024). Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems. arXiv:2404.03509v1. https://arxiv.org/html/2404.03509v1

Dulberg, R. (2021). Privacy Enhancing Technologies and why they're vital for healthcare innovation. *Medium*. https://medium.com/codex/ai-privacy-and-why-you-should-care-1ef503a789b6 Son erişim tarihi: 4 Haziran 2025.

European Data Protection Supervisor. (t.y.). Glossary – Data Minimization. https://edps.europa.eu/data-protection/data-protection/glossary/d_en#data_minimization Son erişim tarihi: 5 Haziran 2025.

European Data Protection Supervisor. (2018). *Opinion 5/2018 – Preliminary Opinion on privacy by design*. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf Son erişim tarihi: 5 Haziran 2025.

Fragkouli, S. C., et al. (2024). Synthetic data: how could it be used in infectious disease research? *Future Microbiology*, 19(17), 1439–1444. https://doi.org/10.1080/17460913.2024.2400853

Google. (2025). Google, konuşma modellerini nasıl iyileştirir? https://support.google.com/assistant/answer/11140942 Son erişim tarihi: 5 Haziran 2025.

Gustavsson, S. (2020). *An Assessment of Privacy by Design as a Stipulation in GDPR* (Yayımlanmamış yüksek lisans tezi). Uppsala Universitesi, İsveç.

Gürses, S., Troncoso, C., & Diaz, C. (2007). *Engineering Privacy by Design*. Institute IMDEA Software. https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf Son erişim tarihi: 2 Haziran 2025.

Hornung, G. (2013). Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework. *Innovation: The European Journal of Social Science Research*, 26(1–2), 181–196.

Hustinx, P. (2010). Privacy by design: delivering the promises. *Identity in the Information Society*, 3, 253–255.

Information Commissioner's Office. (2023). *Privacy-enhancing Technologies (PETs)*. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/ Son erişim tarihi: 2 Haziran 2025.

James, S., Harbron, C., Branson, J., & Sundler, M. (2021). Synthetic data use: exploring use cases to optimise data utility. *Discover Artificial Intelligence*, 1(1). https://doi.org/10.1007/s44163-021-00016-y

Kindt, E. (2013). Best Practices for Privacy and Data Protection for the Processing of Biometric Data. P. Campisi (Ed.), *Security and Privacy in Biometrics*. London: Springer.

Kosinski, M. (2025). *Why Synthetic Data is the Future of AI: Exploring the Shift from Real-World Datasets*. https://www.1950.ai/post/why-synthetic-data-is-the-future-of-ai-exploring-the-shift-from-real-world-datasets Son erişim tarihi: 14 Mart 2025.

Kurapati, S., & Gilli, L. (2023). Synthetic Data: Convergence between Innovation and GDPR. *Journal of Open Access to Law*, 11, 1–12.

London Economics. (2010). *Study on the economic benefits of privacy-enhancing technologies (PETs)*. https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf Son erişim tarihi: 2 Haziran 2025.

Macgillivray, A. (2022). *Advancing a Vision for Privacy-Enhancing Technologies*. The White House. https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/ Son erişim tarihi: 2 Haziran 2025.

Morales-Trujillo, M. E., et al. (2019). A Systematic Mapping Study of Privacy by Design in Software Engineering. *CLEI Electronic Journal*, 22(1), 1–29.

Nampiina, E. (2020). *Privacy by Design – A qualitative study to explore privacy by design adaptation in reducing privacy breaches* (Yayımlanmamış yüksek lisans tezi). Lund University School of Economics and Management, İsveç.

Obermeyer, H. (2021). Privacy-Enhancing Technologies: Opening Data, Powering AI. *BSA TechPost*. https://techpost.bsa.org/2021/02/01/privacy-enhancing-technologies-opening-data-powering-ai/ Son erişim tarihi: 2 Haziran 2025.

OECD. (2023). *Emerging Privacy Enhancing Technologies – Current Regulatory and Policy Approaches*. OECD Digital Economy Papers, No. 351.

OECD. (2025). *Sharing Trustworthy AI Models with Privacy-Enhancing Technologies*. OECD Artificial Intelligence Papers, No. 38.

Oualha, N. (2025). SoK: Privacy-Enhancing Technologies in Artificial Intelligence. arXiv preprint arXiv:2506.14576.

PDPC (Personal Data Protection Commission – Singapore). (2024). *Privacy Enhancing Technology (PET): Proposed Guide on Synthetic Data Generation*. https://www.conformally.com/featured_item/privacy-enhancing-technology-pet-proposed-guide-on-synthetic-data-generation-by-pdpc/ Son erişim tarihi: 2 Haziran 2025.

Rossum, H. van, & Borking, J. J. (1995). *Privacy-enhancing Technologies: the path to anonymity*. The Hague: Registratiekamer.

Rubinstein, I. S. (2011). Regulating Privacy by Design. *Berkeley Technology Law Journal*, 26(3), 1409–1456.

Rubinstein, I. S. (2018). Procedural, Institutional, Technical and Management Devices: A U.S. Perspective. I. Pernice & J. Pohle (Eds.), *Privacy and Cyber Security on the Books and on the Ground*. Berlin: Alexander von Humboldt Institute for Internet and Society.

Srouji, J., & Mechler, T. (2020). How privacy-enhancing technologies are transforming privacy by design and default: Perspectives for today and tomorrow. *Journal of Data Protection & Privacy*, 3(3), 268–280.

Szekely, B. (2022). Mitigating the Privacy Risks of AI through Privacy-Enhancing Technologies. *Acta Universitatis Sapientiae: Legal Studies*, 11(2), 35–64.

The European Consumer Organization. (2020). *Artificial Intelligence: what consumers say*. https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf Son erişim tarihi: 6 Haziran 2025.

van Blarkom, G. W., et al. (2003). Chapter 3: PET. G. W. van Blarkom, J. J. Borking & J. G. E. Olk (Eds.), *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*. The Hague: College bescherming persoonsgegevens.

van Lieshout, M., et al. (2011). Privacy by Design: an alternative to existing practice in safeguarding privacy. *Info*, 13(6), 55–68.

van Rest, J., et al. (2014). Designing Privacy-by-Design. B. Preneel & D. Ikonomou (Eds.), *Privacy Technologies and Policy*. London: Springer.