Yapay Zekâ Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme

Araştırma Makalesi/Research Article

Fatma BAŞKAYA*, Hacer KARACAN

Bilgisayar Mühendisliği, Gazi Üniversitesi, Ankara, Türkiye
fatma.baskaya@gazi.edu.tr, hkaracan@gazi.edu.tr

(Geliş/Received:07.01.2022; Kabul/Accepted:24.10.2022)
DOI: 10.17671/gazibtd.1053803

***Özet*—** Günümüz gelişen teknolojisiyle birlikte yapay zekâ kullanımı artmıştır. Bu durumun çoğunlukla faydaları üzerine konuşulsa da kişisel veri mahremiyetine ve güvenliğine olumsuz etkisi göz ardı edilmemelidir. Çünkü yapay zekâ için ham madde olan veriler, kişilerin mahremiyet haklarına aykırı durumlara neden olabilmektedir. Bu doğrultuda ilgili çalışmada; genel olarak yapay zekânın kişisel veri mahremiyeti açısından oluşturduğu risklere, bu risklerin giderilmesi için önerilen bazı yöntemlere ve bu yöntemlerden biri olan federe öğrenme metodu ile ilgili detaylara yer verilmiştir. Ayrıca günümüzde çeşitli sektörlere ait uygulamalarda sıklıkla kullanılan yapay zekâ ürünü, sohbet robotları (chatbot) ile ilgili bir inceleme ve anket çalışması yapılmıştır. Bu anlamda; sohbet robotlarının kullanımı ve yapısının kişisel veri güvenliğine uygunluğu ile ilgili detaylara ve önerilere yer verilirken anket çalışmasında ise kişilere yöneltilen dört adet soru ile kişilerin, sohbet robotu kullanma boyutunu ve sohbet robotu kullanımının kişisel verilere etkisine yönelik farkındalığını ölçmek amaçlanmıştır. Anket sonuçları, sohbet robotlarının en fazla bankacılık işlemleri için kullanıldığını ve bireylerin %62,1'inin ise bu servislerin kişisel verileri kaydedip işleyebileceğini bilmediğini göstermiştir.

***Anahtar Kelimeler*—** yapay zekâ, kişisel veri güvenliği, KVKK, GDPR, federe öğrenme, sohbet robotları.

The Impact of Artificial Intelligence-Based Systems on Personal Data Privacy: A Study on Chatbots

***Abstract*—** Use of artificial intelligence has increased with the developments in technology. Although the benefits of this situation have mostly been discussed, its negative impacts on personal data privacy and security shouldn't be overlooked. Artificial intelligence-based systems can cause antithetical situations in terms of the privacy rights of individuals because of the fact that data is the raw material for artificial intelligence. Accordingly, the risks posed by artificial intelligence, some methods recommended to overcome these risks, and one of these methods, federated learning, were covered in the current study. Moreover, a study and survey were conducted on chatbots which are artificial intelligence products and are frequently used in applications applied on various sectors. In this sense, some details and recommendations regarding the use of chatbots and the compatibility of their structure with personal data security were included. In the survey with four questions, it was aimed to understand the extent of using chatbots and the awareness on the effects of chatbot using personal data. The survey results showed that chatbots are mostly used for banking transactions and 62.1% of individuals do not know that these services can save and process personal data.

***Keywords*—** artificial intelligence, data privacy, KVKK, GDPR, federated learning, chatbots.

1. GİRİŞ (INTRODUCTION)

Günümüzün teknolojik gelişimiyle birçok alanda yer bulan yapay zekânın en önemli faydalarından birkaçı; verileri, insan gücünden daha kısa sürede daha hızlı analiz etmeleri ve bu verileri işlerken öğrenme sürecine girmeleridir. Tüm faydaları düşünüldüğünde; son yıllarda yapay zekâ ve yapay zekânın alt dallarına ait kollarda, literatüre yeni

algoritmalar ve yöntemler kazandırılmış ve kazandırılmaya devam etmektedir.

Bu gelişmeler yapay zekâ dünyası için yeni öngörülerin ve yeni kapıların açılmasına olanak sağlamaktadır. Yapay zekâ uygulamalarına; tahmin, ses ve/veya görüntü tanıma, öneri ve tespit sistemleri, sohbet robotları, vb. gibi birçok uygulama ve sistem örnek olarak verilebilir [1].

Yapay zekânın hammaddesini oluşturan kaynak büyük veridir ve yapay zekâ teknolojisini kullanan sistemlerde, toplanan büyük miktarda verinin işlenmesi durumu söz konusudur [2]. Bu anlamda, kişisel veriler ve yapay zekâ iki taraflı ve birbirini besleyen bir ilişki içindedir. Bir yandan kişisel veriler yapay zekâ teknolojilerini beslerken öte yandan yapay zekâ teknolojileri de çıkarımlar yaparak daha fazla kişisel veri üretir [3].

Büyük veri ihtiyacı karşılanırken toplanan verilerin mahremiyeti, dikkat edilmesi gereken önemli konulardan biridir [1]. Bu durum, yapay zekânın sahip olduğu faydalar yanında çeşitli riskleri de barındırdığı anlamına gelmektedir. Örneğin; hastalık teşhisi için kullanılan yapay zekâ sistemlerinde, veri olarak kullanılan kan testlerinin işlenmesi kişisel veri mahremiyeti ilkesine aykırı durumlara sebebiyet verebilmektedir. Öte yandan, doktorların elinde bulunacak büyük miktardaki örnek test, derin öğrenme yöntemleri ile hastalık teşhisini kolaylaştırabilmektedir [1]. Anlaşıldığı üzere yapay zekâ, bahsedilen riskler düşünüldüğünde vazgeçilen bir alan olmamalı; tam aksine gerekli ve doğru bir şekilde kullanılarak faydasından en doğru şekilde istifade edilen bir alan olmalıdır.

Tüm bu açıklamalardan yola çıkarak; bu çalışmada, genel olarak yapay zekâ tabanlı sistemlerin kişisel veri güvenliğine olan olumsuz etkileri, kullanıcıların karşı karşıya kalabileceği riskler ve bu risklerin nasıl aşılabileceğine yönelik öneriler anlatılmıştır.

Belirtilen amaç ile ilgili yapılan literatür taramasında, yapay zekâ tabanlı sistemlerin hangi önlemler alınarak tasarlanması gerektiği ve böylece kişisel veri güvenliğinin nasıl sağlanabileceği ile ilgili hem akademik hem de ulusal ve uluslararası otoriteler tarafından yapılan çalışmalar incelenmiştir. Bu bağlamda çalışmada; Genel Veri Koruma Yönetmeliği'ne *(General Data Protection Regulation - GDPR)* ve 6698 sayılı Kişisel Verileri Koruma Kanunu'na (KVKK) da yer verilmiştir.

İncelenen çalışmalar neticesinde, gizlilik prensibine uygun sistemler tasarlamaya imkân sağlayan *Federe Öğrenme* yönteminin son birkaç yıldır literatürde yer etmeye başladığı görülmüştür. Yapay zekâ tabanlı sistemlerde, federe öğrenme yöntemi kullanarak kişisel verilere saygılı tasarımlar yapmanın mümkün olabileceği anlatılmıştır. Ayrıca yine yapay zekâ tabanlı bir sistem olan ve günümüzde özellikle elektronik ticaret sektörü başta olmak üzere birçok sektörde sıklıkla kullanılan sohbet robotları (chatbot) hakkında inceleme çalışması yapılmış ve bu çalışmaya ait detaylara yer verilmiştir. Kişisel verileri koruma hakkında yayımlanan kanun ve yönergelere uygun sohbet robotları tasarlamak için hangi şartların sağlanması gerektiği anlatılmıştır.

Çalışma kapsamında; literatür taramasına, öncelikli olarak insanların kişisel veri mahremiyeti farkındalığına ve bilincine ne düzeyde sahip olduğunu araştıran bir çalışma incelenerek başlanmıştır. Bu kapsamda; Eroğlu [4] tarafından yapılan çalışmada, günlük hayatlarında çoğunlukla dijital ortam ile etkileşim içinde olan öğrencilerin farkındalığı analiz edilmiştir. Bunun için 34 sorudan oluşan web tabanlı bir anket yapılarak 280 öğrenciye gönderilmiş ve ilgili anket 151 öğrenci tarafından yanıtlanmıştır.

Çalışma sonucunda ise öğrencilerin 72'si kişisel veriyi bildiğini, 19'u ise kişisel veri kavramını bilmediğini belirtmiştir. Ayrıca, öğrencilerin çoğunlukla kimlik numarasını kişisel veri olarak nitelendirdiği görülmüştür. Bunun dışında; kredi kartı bilgileri, ad, soyadı ve doğum tarihi verilerini içeren kimlik bilgileri ve ev adresi verilerinin de öğrenciler tarafından kişisel veri olarak nitelendirildiği görülmüştür.

Kişisel veri ve yapay zekâ birlikteliğine gelindiğinde ise Mitrou yaptığı çalışmada [3], yapay zekâ ve makine öğrenmesi kavramlarına yer vermiş ve bu kavramların kişisel veriler üstündeki etkilerine değinmiştir. Mitrou, kişisel veri ve yapay zekâ arasında çift taraflı bir yol olduğunu, kişisel verilerin yapay zekâyı beslediğini ve buna karşılık yapay zekânın da daha fazla kişisel veri ürettiğini belirtmiştir.

Kamarinou ve arkadaşları [5], GDPR'a göre veri sahiplerinin profillenmesi için makine öğrenimi algoritmalarının kullanılmasının etkilerinin bir analizini sunmuşlardır. Veri koruma hak ve yükümlülüklerini, makine öğrenmesi sistemlerinin geliştirilmesinin sonuçlarını ve kişisel verilerin nasıl toplandığını ve kullanıldığını araştırmışlardır.

Li ve arkadaşları [6], endüstriyel alanlar ve bilişim dünyası uygulamaları açısından federe öğrenmeyi incelemiş ve mobil cihazlar, sağlık uygulamaları, sektör uygulamaları alanında federe öğrenme yöntemini kullanan uygulama örnekleri ile ilgili bir araştırma çalışması yapmışlardır.

Chandiramani ve arkadaşları [7], 2016 yılında Google tarafından önerilen federe öğrenme modeli üzerine bir çalışma yapmıştır. Çalışmada; klasik makine öğrenmesi, dağınık öğrenme modeli ve federe öğrenme yaklaşımları üzerine analiz ve karşılaştırmalar yapılmıştır. Üç modelin doğruluk oranlarında önemli bir fark olmadığı ancak modellerin oluşturulması için geçen sürede fark olduğu görülmüştür. Temel makine öğrenimi sınıflandırıcısının eğitilmesi 25,4 saniye sürerken federe öğrenme sınıflandırıcısının 16,7 saniye; dağıtılmış makine öğrenimi sınıflandırıcısının ise 14,1 saniye sürdüğü gözlemlenmiştir. Böylece en kısa süreye federe öğrenme modeli ile erişildiği

gözlemlenmiş ve fazla veriyle çalışırken verileri dağıtmanın ve küçük görevlere ayırmanın performans artırımı için bir avantaj olduğu görülmüştür. Bu nedenle; üç model arasından federe öğrenmenin, modelleri eğitirken gizliliği korumak için en iyi model olduğu anlaşılmıştır.

Wang ve arkadaşları [8]; kullanıcı görüşlerinin, duygularının ve e-postaların yer aldığı üç farklı hazır veri seti üzerinde metin madenciliği yöntemini uygulamıştır. Model, federe öğrenme yöntemi ile birleştirilen Gizli Dirichlet Ayırımı (Latent Dirichlet Allocation) algoritması kullanılarak eğitilmiş ve kullanıcıların veri gizliliğinin korunduğu görülmüştür.

Ülkemizde de son yıllarda özellikle 6698 sayılı KVKK ile birlikte mahremiyet kavramına verilen önem artmış ve bu alanda yapılan çalışmalara büyük ilgi olduğu gözlemlenmiştir. Süzen ve Kayaalp [1] yaptıkları çalışmada; klasik makine öğrenmesi uygulamaları için federe öğrenme yöntemini incelemiş ve federe öğrenmenin gizlilik açısından faydaları olsa da problemlere uygulanması sırasında karşılaşılacak zorluklarının olduğunu belirtmişlerdir. Bununla birlikte yeni algoritmalar ve bu alandaki araştırma çalışmalarının artması ile bu zorlukların aşılabileceği ve gizlilik ve güvenlik ilkelerine uygun sistemler geliştirilebileceği belirtilmiştir.

Süzen ve Şimşek [9], sağlık alanında yapılan uygulamalar için makine öğrenmesi modellerinin uygulanışını incelemişlerdir. Sağlık verilerinin işlenmesinde, gizlilik ilkesine uyumu yakalamak adına model içine federe öğrenme yöntemlerinin entegre edilmesi gerektiğini belirtmişlerdir.

Sağıroğlu ve Canbay [10] yapmış oldukları çalışmada, büyük veride yapay zekâ teknolojilerini kullanırken mahremiyet ihlallerinin önüne geçmek amacıyla yeterli önlemlerin alınması gerektiğini belirtmişlerdir. Bunun için, KVKK ve GDPR gibi yasal mevzuatlara uygunluğun önemli olduğunu belirtmişler ve mahremiyeti yakalamak için kullanılan anonimleştirme konusunun üstünde durmuşlardır.

Tüm bu çalışmaların yanı sıra Türkiye'de yapay zekâ ve kişisel veri mahremiyeti konusunun kamu idareleri tarafından da önemli ölçüde dikkate alındığını gösteren örneklerle karşılaşmak mümkündür. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yapılan "AçıkVeri" projesinde [11], federe öğrenme yöntemi gibi yenilikçi yöntemler ile gizliliği korunan kişisel veriler konusuna vurgu yapılmıştır. Ayrıca, Kişisel Verileri Koruma Kurumu tarafından Eylül 2021 tarihinde "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" [12] isimli rehber çalışması yayımlanmış ve bu çalışmada önemli tavsiyelere yer verilmiştir. Bu tavsiyeler; yürürlükte bulunan yasal mevzuatlar doğrultusunda, yapay zekâ sistemini geliştiren, üreten, bu sisteme servis sağlayan gerçek veya tüzel kişiler ile karar alıcıları kapsamıştır. Bu duruma yönelik benzeri önerilerin bulunduğu çalışmalar her geçen gün artmaktadır. Hem akademik düzeyde hem de kamu eli ile desteklenen bu alan, yenilikçi yöntemlerin keşfi ile gelecek vadeden alanlardan biri haline gelmiştir.

2. YAPAY ZEKÂ VE KİŞİSEL VERİ MAHREMİYETİ (ARTIFICIAL INTELLIGENCE AND PERSONAL DATA PRIVACY)

Bu bölümde; kişisel veri kavramının ne olduğu ve hangi türlerden oluştuğu, yapay zekânın kişisel verilerle olan ilişkisi ve bu sistemlerin veri toplama ve işleme faaliyetlerinde kişisel veri güvenliği açısından ne tür riskler oluşturabileceği anlatılmıştır.

Kişisel veri kavramı, 6698 sayılı KVKK Madde-3/1'de *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi…"* [13] olarak tanımlanmıştır. Bu tanımdan hareketle kişilere ait, ad, soyad, telefon numarası, adres, banka hesap numarası, resim, vb. gibi kişiyi tanımlayabilen ya da kişi ile ilişkilendirilebilen [14] tüm verilerin kişisel veri olduğunu söylemek mümkündür. Tüm bunların yanı sıra, KVKK'da *"Özel Nitelik Kişisel Veri"*; GDPR'de ise *"Hassas Veri"* olarak ifade edilmiş olan veriler bulunmaktadır. Bu veriler, bir başkası tarafından öğrenildiğinde kişinin mağduriyet yaşayabileceği veya ayrımcılığa maruz kalabileceği [14] durumlara neden olabilecek verilerden oluşmaktadır. KVKK Madde-6/1'de özel nitelikli kişisel veriler, "K*işilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri…*" olarak ifade edilmiş ve kanunda bu verilerin işleme şartları ayrı bir madde ile (Madde-6) ele alınmıştır.

Gelişen dünya ile yapay zekâ gibi veriye ihtiyaç duyan ve veri ile beslenen teknolojiler ortaya çıkmıştır. Yapay zekâ, makinelere insansı özellikler kazandırarak karmaşık problemlere çözüm üretmeyi amaçlayan önemli konulardan biridir. Bir insanın karar verebilme gücünü taklit etmeyi amaçlayan bu sistemler, çeşitli algoritmalar aracılığı ile modellenir. Böylece, insan gücü ile yapılacak işler daha kısa sürede daha başarılı bir şekilde çözüme ulaşır [15].

Yapay zekâ teknolojisinin günümüz kullanım alanlarına bakıldığında; yapay zekânın sağlıktan elektronik ticarete, ulaşımdan pazarlamaya değin birçok alanda kullanıldığını görmek mümkündür. Hastalıkları, bilişim sistemlerine yapılan saldırıları [15], seri üretim bandı hatalarını, dolandırıcılığı tespit edebilen sistemler ile kişisel asistanlar, suç analizi, duygu analizi, fikir tespiti, vb. gibi çalışma alanları, yapay zekâ konusunun birer ürünüdür. Yapay zekâ teknolojisi ise tüm bu işlemler için yüksek miktarda veriyi işlemekte ve kendini eğitmektedir. Görüldüğü üzere yapay zekânın hemen her alanda hayatımızın içinde oluşu verilerin de aynı oranda yaygın bir şekilde işlenmesi sonucuna neden olmaktadır.

Veri ve yapay zekâ ise birbirinden beslenen kavramlardır. Bu durumu somutlaştırmak için gündelik hayatta sıklıkla karşılaşılan durumlardan örnek vermek gerekirse; arama motorunda daha önce aradığımız kelimelerle ilgili olan reklamların daha sonra karşımıza çıkarılması, aynı şekilde önceden izlediğimiz bir videoyla benzer konuları barındıran videoların öneri listemize gelmesi veya sosyal medya platformlarının arkadaş listemiz veya beğendiğimiz sayfalardan yola çıkarak kişi veya sayfa önermesi yapay zekânın verileri işleyerek ürettiği durumlardan sadece birkaçıdır [2]. Kısacası; çözmek istenilen probleme yönelik uygun veriye sahip olan sistemler, akıllı yaklaşımlar üretebilmektedir. Yapay zekâ için bir nevi besin olan bu veriler, her alanda her türlü sektör veya kurumdan elde edilebilmektedir.

Yapay zekânın birçok probleme başarılı çözümler üretmesinin yanı sıra tüm bu işlemleri gerçekleştirirken kaynağı olan veriyi ne şekilde aldığı, nasıl kullandığı ve koruduğu soruları da üzerinde düşünülmesi gereken önemli konulardandır. Tüm bunlar son yıllarda önem verilen konular olsa da maalesef yapay zekânın faydalarının yanında görece göz ardı edilmektedir. Bu durum ise zamanla yapay zekâyı; kişisel verileri, kanunlara aykırı bir şekilde işleme potansiyeli olan platformlar haline getirmektedir. Kişisel verileri kanunlara aykırı toplayan, işleyen ve saklayan uygulamalar; kötü niyetli kişilerce veri sahiplerini zor durumda bırakacak şekilde kullanılabilmektedir.

Dolayısıyla bir yapay zekâ sisteminin veri işleme görevini yerine getirirken veri mahremiyeti ilkesini gözetmesi için bazı zorunluluklara uyması gerekmektedir. Aksi halde işlenen veriler; veri sahibi konumundaki kişi veya kurumları, kişisel verilerin ifşa edilmesi, yetkisiz üçüncü kişilere aktarılması, fidye amacıyla kullanılması ve daha birçok şekilde zor duruma düşürebilmektedir.

3. ÖNERİLEN YÖNTEMLER (PROPOSED METHODS)

Yapay zekâ veriden bağımsız düşünülemez. Özellikle günümüz gelişen teknolojisiyle adeta yenidünya düzeni oluşturan teknolojiler, hayatın her alanına ve her sektöre girmişken bundan kaçmak imkânsız ve yanlıştır. O halde, yapılması gereken yapay zekâdan kaçmak değil; yapay zekâyı en etkili şekilde kullanıp hizmetlerinden en maksimum faydayı elde etmek ve ancak bunu gerçekleştirirken veri koruma ilkesine sadık kalarak kişisel verilerin korunmasını sağlamaktır.

Kişisel verilerin otomatik işlenmesi ile ilgili çalışmalar yapan Avrupa Konseyi, 108 numaralı Kişisel Verilerin Otomatik İşleme Danışma Komitesi *(Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)* tarafından Ocak 2019'da hazırlanan rehber çalışmasında [16]; yapay zekâ teknolojisine dayanan sistemlerde, kişisel veri işleme faaliyetinde bulunurken hangi hususların göz önünde bulundurulması gerektiği ile ilgili bilgilere yer verilmiş ve aşağıda belirtilen hususlara değinilmiştir:

- Verilerin işlenmesi ve teknolojinin gelişimi aşamasında veri koruma ilkeleri esas alınmalıdır. Ayrıca, ilgili kişi hakları gözetilmelidir.
- Veri işleme faaliyeti sırasında gerekli risk analizleri yapılmalı, bu analizler yapay zekâ teknolojisinin özellikleri göz önüne alınarak hassas bir şekilde yapılmalıdır.
- İlgili kişilere, açık, doğru ve anlaşılır bir şekilde gerekli bilgilendirmeler yapılmalıdır.
- Veri minimizasyonu ilkesi gözetilmeli, gereksiz ve aşırı veri işleme faaliyetinden kaçınılmalıdır.
- Amaç dışı veri işleme faaliyetinde bulunulmamalıdır.

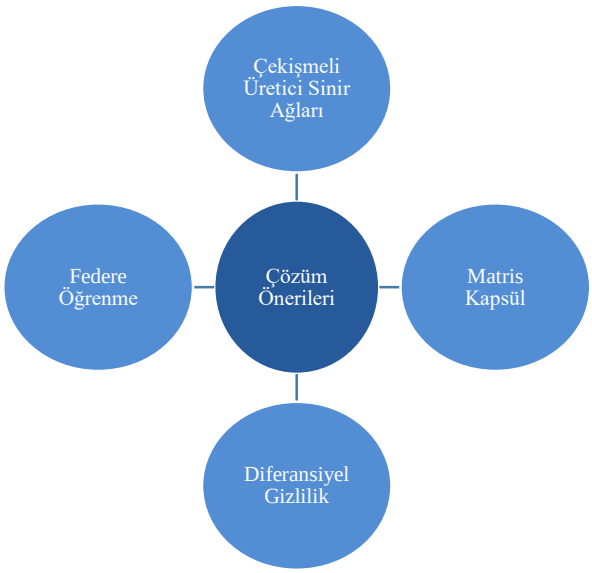
Bahsi geçen bazı temel veri işleme politikaları GDPR Madde-5 ve 6698 sayılı KVKK Madde-4 ile düzenlenmiştir. KVKK Madde-4'te yer alan hükümler aşağıda bulunmaktadır [13]:

"...(1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir. (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:
a) Hukuka ve dürüstlük kurallarına uygun olma.
b) Doğru ve gerektiğinde güncel olma.
c) Belirli, açık ve meşru amaçlar için işlenme.
ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme..."

Bu hükümler içinde belirtilen amaçla sınırlı olma ilkesi, kişisel verilerin belirli, açık ve meşru amaçlarla toplanması gerektiğini; veri minimizasyonu prensibi ise kişisel verilerin işleme için gerekli olduğu kadar, amaçla ilgili ve ölçülü bir biçimde işlenmesi gerektiğini ifade etmektedir [17]. Bu duruma örnek vermek gerekirse; seyahat için bilet alınmak istendiğinde, kişiden kan grubu bilgisinin istenmesi verinin amaçla ilgili olmadığı anlamına gelmektedir.

Norveç Veri Koruma Otoritesi tarafından Ocak 2018'de hazırlanan yapay zekâ ve gizlilik raporunda [18], GDPR'de yapay zekâ ile veri işlemenin hususlarına değinilmiştir. Temel olarak yasallık, şeffaflık, amaçla sınırlı kalma, veri minimizasyonu, amaca bağlılık ilkelerinden söz edilmiştir. Bunun yanı sıra veri sorumlularının, ilgili kişi konumundaki veri sahiplerine karşı hesap verilebilirlik ilkesi gereğince hareket etmeleri gerektiği belirtilmiştir. Bu bilgilendirmeler ışığında; bahsi geçen raporda ilgili otorite, kişisel veri mahremiyetine önem veren yapay zekâ tabanlı sistemlerin teknik alt yapıları hususunda bazı çözüm önerilerinden bahsetmiştir. Bu çözüm önerileri Şekil 1' de belirtilmiştir.

Belirtilen çözüm önerilerine kısaca değinmek gerekirse, Çekişmeli Üretici Sinir Ağları (Generative Adversarial Networks) modeli, 2014 yılında Google araştırmacısı *Ian Goodfellown* tarafından geliştirilmiştir. Bu modelde, üretici ağ ve ayırt edici ağ olmak üzere iki türlü ağ bulunmaktadır. Üretici ağ gerçeğe yakın veriler üretirken ayırt edici ağ, verinin gerçek mi sahte mi olduğunu anlamaktadır [18].



Şekil 1. Otoritenin çözüm önerileri [18]
(Solutions of the authority)

Matris kapsül yöntemi ise sistemi eğitmek için kullanılan yapay sinir ağları temelli bir modeldir [18]. Diferansiyel Gizlilik (Differential Privacy) modelinde ise veriye gürültü ekleme işlemi yapılmaktadır [19, 20].

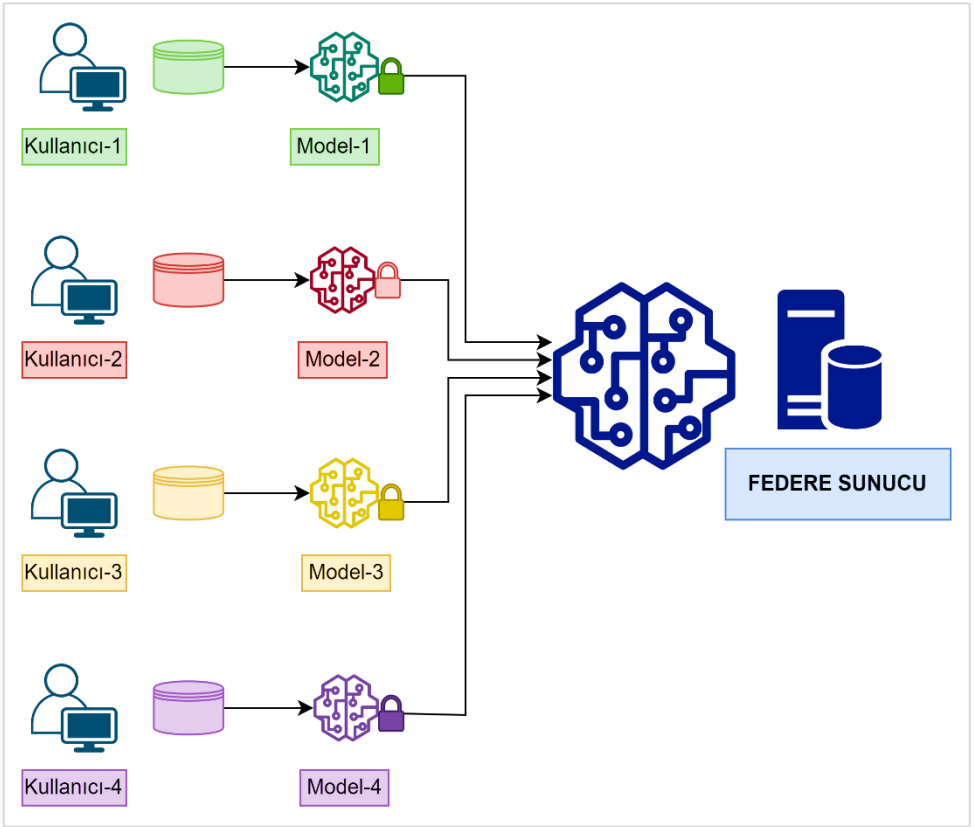
Bu çalışmada, önerilen yöntemlerden biri olan federe öğrenme konusu ile ilgili detaylara yer verilmiştir.

3.1. Federe Öğrenme (Federated Learning)

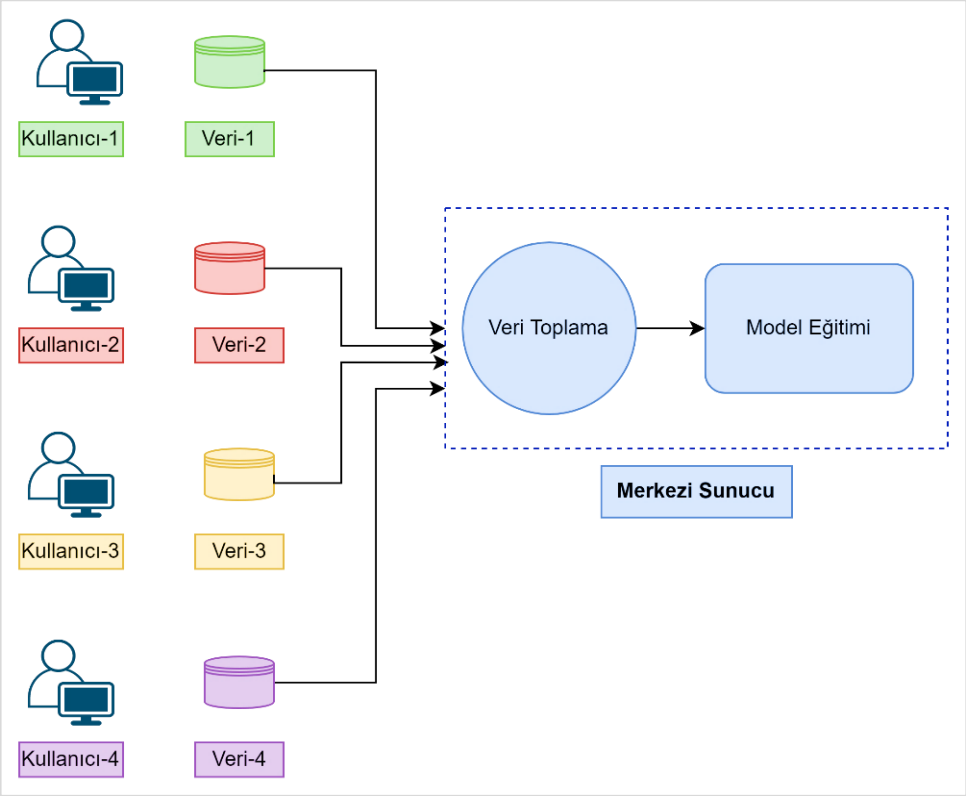
Federe öğrenme, kullanıcıların verileri paylaşmadan sistemi eğittiği bir makine öğrenmesi biçimidir. Bu öğrenme metodunda her kullanıcı kendi verileri ile yerel modelini oluşturur ve tüm model ağırlıkları birleştirilerek federe sunucuda bulunan ana modelin ağırlıkları oluşturulur [21]. Federe öğrenme, makine öğrenmesindeki eğitim sürecinin sistemdeki kullanıcılar arasında paylaştırıldığı işbirlikçi bir yöntemdir [18].

Federe öğrenmede, koordinatör rolüne sahip bir sunucu [22] ve sunucu tarafından belirlenen kullanıcılar bulunmaktadır. Koordinatör rolündeki federe sunucu bu kullanıcıları, kullanıcının erişilebilir olup olmadığı ve model eğitimine izin verip vermediği gibi kıstasları göz önünde bulundurarak belirlemektedir. Belirlenen kullanıcılar verilerini paylaşmadan kendi modellerini oluşturup ağırlıkları federe sunucuya aktarırlar. Şekil 2'de [7, 18, 23] görüldüğü gibi federe sunucu koordinatör rolü ile tüm kullanıcılardan gelen ağırlıkları birleştirir ve nihai modeli oluşturur [21].

Federe öğrenmede mevcut durumda eğitilmiş bir model bulunuyorsa bu modelin ağırlıkları ve parametreleri, bahsi geçen kriterlere göre seçim yapılarak belirlenen kullanıcılar ile paylaşılır. Her kullanıcı, gelen modeli kendi verisi ile oluşturduğu yerel modelin ağırlıkları ile günceller ve güncellenmiş ağırlıkları federe sunucuya iletir.



Şekil 2. Federe öğrenme [7, 18, 23]
(Federated learning)



Şekil 3. Klasik makine öğrenmesi modeli [7]
(General machine learning model)

Klasik makine öğrenmesi modelinde Şekil 3'te görüldüğü üzere kullanıcıların verileri paylaşması söz konusudur. Merkezi sunucu rolündeki koordinatör, kullanıcılardan gelen verileri toplayarak modeli eğitir [7] ve sonrasında geleneksel makine öğrenmesi adımları izlenir. İlk aşamada veri, ön işlemeden geçirilerek yapısal formata dönüştürülür. İkinci aşamada, makine öğrenmesi modeli oluşturulur. Bir sonraki aşamalarda ise model eğitilir ve test edilir.

Federe öğrenmenin kullanıldığı çeşitli alanlara ait uygulama ve sistemler bulunmaktadır. Bunlardan biri olan Google Klavye (Gboard),kullanıcının yazdıklarına erişerek kullanıcı için otomatik metin düzeltme, bir sonraki kelimeyi tahmin etme ve kelimeyi tamamlama gibi özellikler içeren sanal bir klavyedir [24] ve federe öğrenmeyi kullanarak kullanıcı gizliliği önem vermiştir.

Çin'de Google'un yasaklanmasıyla birlikte Baudi şirketi, yapay zekâ ürünlerine dâhili olarak uygulamak amacıyla federe öğrenme tekniğini kullanarak PaddleFL platformunu geliştirmiştir [25].

Bir başka örnek olarak Owkin isimli bir Fransız tıp-biyoloji şirketi hastalık tanıları ile ilgili etkili bir çalışma yapmak amacıyla sağlık kurumları ve ilaç firmalarıyla ortaklık yürüterek federe öğrenmeye dayalı bir makine öğrenmesi modeli oluşturmuştur. Böylece, hasta mahremiyeti korunurken kuruluşlar ve araştırmacılar arasında veri paylaşımı yapılmıştır [1].

NVIDIA şirketi, GDPR'de hassas nitelikli kişisel veri olarak da ifade edilen (6698 sayılı Kişisel Verileri Koruma Kanunu'nda da özel nitelikli kişisel veri) sağlık verilerinin hastane içinde kalmasını sağlayan ClaraFL geliştirmiştir [1]. Bazı üst düzey sağlık hizmeti sunan kurumlarda bulunan radyologlar tarafından kullanılmaya başlanan ClaraFL, önceden eğitilmiş modelleri kullanmaktadır. Öğrenme tekniklerini aktarırken radyologlara etiketleme konusunda yardımcı olmaktadır.

Intel şirketi, Mayıs 2020'de Pensilvanya Üniversitesi ile yaptığı işbirliği neticesinde beyin tümörlerini tespit eden yapay zekâ teknolojisi üzerine çalışmaya başladıklarını açıklamıştır [26]. Geliştirilecek sistemde, 29 tıp merkezinden alınacak hasta verileri için kişisel veri gizliliğini sağlamak adına federe öğrenme yönteminin kullanılacağı belirtilmiştir.

Federe öğrenme, yapay zekâ sistemlerinde kişisel veri mahremiyetini korumak için uygun bir çözümdür ancak yanında getirdiği bazı teknik zorluklar ve riskler bulunmaktadır. İlki, tasarlanacak federe öğrenme sisteminin karmaşıklığıdır. Sistemi iyi tasarlamak ve karmaşıklığı azaltacak çözümler üzerine çalışmak gerekmektedir. Bir diğer zorluk, federe sistem koordinasyonundan sorumlu olan sunuculara iş yükü yüklemektir. Bu durumun sunucuları yoracağı düşünüldüğünden sistemin, bu dezavantaj düşünülerek inşa edilmesi gerekmektedir.

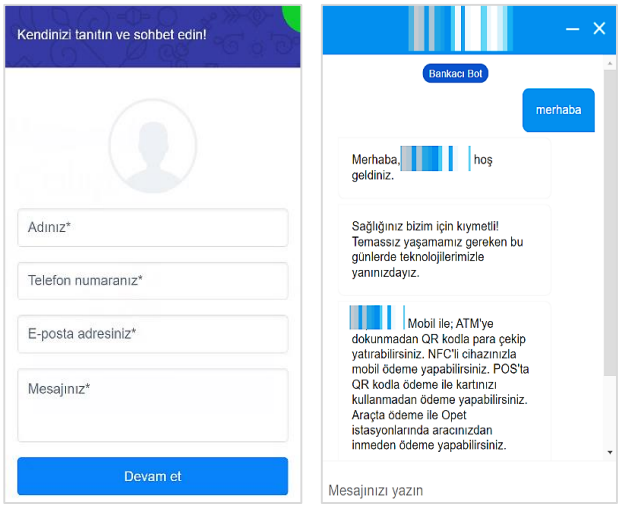
4. SOHBET ROBOTLARI (CHATBOTS) ÜZERİNE İNCELEME ÇALIŞMASI (STUDY ON CHATBOTS)

Bu bölümde, yapay zekâ tabanlı uygulamaların ne sıklıkla ve çoğunlukla hangi işlemler için kullanıldığıyla ilgili genel yargı çıkarımı yapmak amacıyla yapay zekâ tabanlı uygulama olan sohbet robotları özelinde deneysel bir çalışma yapılmıştır. Yapay zekâ tabanlı uygulama olan sohbet robotlarının ne olduğu, nerelerde kullanıldığı, hangi tür verilere ihtiyaç duyduğu ve veri toplama faaliyetini yürütürken barındırdığı riskler anlatılmıştır. Kişisel veri mahremiyeti ve buna yönelik kanun, yönerge ve rehberlere uygun sohbet robotları tasarlamak için nelere dikkat edilmesi gerektiği konuları üstünde durulmuştur.

4.1. Sohbet Robotu (Chatbot)

Chatbot kellimesi, sohbet anlamına gelen *Chat* ve robot anlamına gelen *Bot* sözcüklerinin birleşiminden meydana gelmiştir [27]. Sohbet robotu olarak bilinen bu uygulamalar, kullanıcı ile birebir etkileşimde bulunarak daha önceden belirlenmiş bazı durumlar üzerine kullanıcının isteğine göre cevaplar üreten ve bunu kullanıcıya ileten yapay zekâ ürünleridir [28]. Yapay zekâ teknolojisi ile geliştirildiklerinden dolayı ile kullanıcı ile yaptıkları her ikili konuşma neticesinde bir öğrenim sürecine girerler. Bu durum; sohbet robotlarına, karşılaştıkları yeni durumlar için kullanıcı isteğine cevap üretme imkânı sağlamıştır [29].

Sohbet robotlarının; kesintisiz erişebilir olmaları, basit sorunlar için kısa sürede çözümler oluşturması, sipariş işlemlerini yönetmesi, zaman ve maliyet anlamında etkin sonuçlar doğurması, vb. gibi birçok faydası bulunmaktadır [28]. Tüm bu faydaları ile her sektörün kullanmak istediği bu interaktif araç, müşteri deneyimine yeni bir bakış açısı kazandırmış; her an her yerde kullanıcı karşısına çıkmaya başlamıştır.



Şekil 4. Örnek sohbet robotu uygulamaları
(Examples for the chatbot apps)

Telefonlarda kullanılan kişisel asistanlardan bankaların kişisel asistanlarına ve elektronik ticaret sitelerinin çevrimiçi destek servisine kadar her alanda hizmet verebilir niteliğe ulaşmıştır. Her sektörde boy gösteren yapay zekânın ve bunun bir yansıması olan sohbet robotlarının, kullanıcı deneyimi için artık bir devrim niteliğinde olduğu yadsınamaz bir gerçektir. Şekil 4'te ülkemizde, bankacılık ve elektronik ticaret sektöründe hizmet veren iki firmanın web sitelerinde kullandıkları sohbet robotlarına ait örnekler verilmiştir.

Sohbet oturumu sonrasında robot; elde ettiği verileri, CRM *(Customer Relationship Management)* adı verilen müşteri ilişkileri yönetimi veya benzer teknolojilerle bağlantılı duruma getirmek için saklamaktadır. Böylece bu durum; çıkarım yapmak, gelecek stratejileri belirlemek veya satış raporları oluşturmak için firma tarafından kullanılmaktadır [30].

Tüm bu özellikler ve toplanan veriler, sohbet robotlarının kullanım özeline göre (hangi uygulama ve hangi sektörde olduğu) değişiklik gösterse de temel olarak yukarıda anlatılan prensibin kullanıldığını söylemek mümkündür. Görüldüğü üzere bir sohbet robotu uygulaması, müşteri verilerini toplamakta büyük bir potansiyele sahiptir. Her ne kadar kullanıcı ile etkileşimli sistem oluşumu içinde onlara efektif bir hizmet sunmayı amaçlasa da amaç dışı sonuçlara da sebep olabilmektedir.

Kişiler; söz konusu bu uygulamadan faydalandıkları sırada paylaştıkları kişisel verilerin kaydedilmesi, işlenmesi ve aktarılması gibi sonuçlarla karşı karşıya kalabilmektedirler [31]. Öyleyse bu uygulamaların, bireyin kişilik haklarına aykırı bir durum teşkil etmeden tasarlanması gerekmektedir. Bunun yanı sıra veri sahibi konumundaki kişiler de yasal haklarını bilerek hareket etmelidirler.

4.2. Deneysel Çalışma (Experimental Study)

Bu çalışma kapsamında, Gazi Üniversitesi Etik Komisyonunun 27.01.2022 tarih ve E.274489 sayılı yazısı ile etik kurul izni alınan bir anket çalışması yapılmıştır. Yapılan anket çalışmasında; kişilerin, sohbet robotu kullanma boyutunu ve sohbet robotu kullanımının kişisel verilere etkisine yönelik farkındalığını ölçmek amaçlanmıştır. Bu amaçla, *Google Formlar* [32] aracı ile kişilere Tablo 1'de belirtilen dört adet soru yöneltilmiştir.

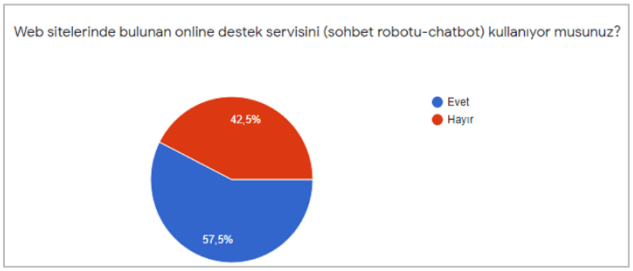
Anket soruları ve soru seçeneklerinin belirlenmesinde, kişilerin; sohbet robotlarını kullanımı ve kişisel veri farkındalığı bilincini ölçmek için temel olarak nitelendirilebilecek, cevaplaması fazla zaman almayan ve katılımcıları yormayan öz metinlerin belirlenmesi amaçlanmıştır.

Tablo 1. Katılımcılara yöneltilen anket soruları ve seçenekleri
(Questions and options)

Sorular	Anket Soruları	Seçenekler
Soru-1	Web sitelerinde bulunan online destek servisini (sohbet robotu-chatbot) kullanıyor musunuz?	• Evet • Hayır
Soru-2	Kullanıyorsanız çoğunlukla hangi işlemleriniz için kullanırsınız?	• Bankacılık İşlemleri • E-ticaret (sipariş işlemleri) • Müşteri Hizmetleri/Destek • Kişisel Asistanlar • Kullanmıyorum
Soru-3	Bu servislere güveniyor musunuz?	• Evet, güveniyorum • Emin değilim • Hayır, asla güvenmiyorum
Soru-4	Bu servislerin kişisel verilerinizi kaydedip işleyebileceğini biliyor musunuz?	• Evet • Hayır

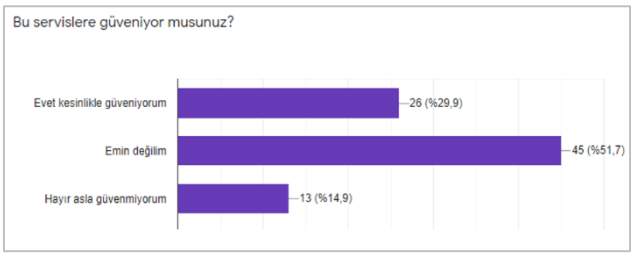
Tablo 1'de belirtildiği üzere; Soru-1 ile sohbet robotlarının kullanılma düzeyi; Soru-2 ile hangi işlemler için kullanıldığı, Soru-3 ile kullanılan uygulamalara olan güven ve Soru-4 ile sohbet robotu uygulamasının kişisel veri işlediğinin ne düzeyde bilindiği ölçülmüştür. Soru-2'nin seçenekleri belirlenirken fazlaca kişisel veri işleyen uygulamaların seçeneklerde yer alması hususu göz önünde bulundurulmuştur.

Yapılan anket çalışması 100 katılımcı tarafından yanıtlanmıştır. Şekil 5'te görüldüğü gibi Soru-1 için verilen cevaplarda, katılımcıların %57,5'i sohbet robotlarını kullandığını; %42,5'i ise kullanmadığını ifade etmiş ve sohbet robotlarının kullanım oranının azımsanmayacak boyutta olduğu sonucuna varılmıştır. Katılımcıların Soru-2'ye vermiş oldukları yanıtlarda, %21,4 oranı ile sohbet robotu uygulamalarının en fazla bankacılık işlemleri için kullanıldığı görülmüştür. Banka faaliyetlerinde bulunan, kimlik doğrulama, kişisel bankacılık hizmetleri, vb. gibi operasyonlarda sohbet robotlarının kullanım oranının fazla olması, bu uygulamaların kişisel veri güvenliği konusunda hassas olması gerektiği sonucunu doğurmuştur. Şekil 6 ile bankacılık işlemlerini sırasıyla, e-ticaret ve müşteri hizmetleri işlemlerinin takip ettiği görülmektedir. Anket sonuçlarına ait Şekil 7'de verilen grafiksel öğede ise Soru-3 için katılımcıların verdiği yanıtlara ait sonuçlar görülmektedir. Buna göre, katılımcıların %45'i bu uygulamaların güvenilirliği konusunda emin olmadığını düşünürken, %26'sı bu uygulamalara güvendiğini, %13'ü ise güvenmediğini belirtmiştir. Soru-3 için ulaşılan bu yanıtlar ile katılımcılar, çoğunlukla bankacılık işlemlerinde kullandıkları sohbet robotu uygulamalarına büyük oranda güvenmediklerini ifade etmişlerdir.



Şekil 5. Soru-1 için katılımcı yanıtları
(Responses to Question-1)

Şekil 6. Soru-2 için katılımcı yanıtları
(Responses to Question-2)



Şekil 7. Soru-3 için katılımcı yanıtları
(Responses to Question-3)

Şekil 8. Soru-4 için katılımcı yanıtları
(Responses to Question-4)

Şekil 8'e göre ise kullanıcıların %62,1'i bu servislerin kişisel verileri kaydedip işleyebileceğini bilmediğini; %37,9'luk kesim ise bildiğini belirtmiştir. Bu sonuçlardan anlaşıldığı üzere katılımcıların büyük bir kısmı sohbet robotu uygulamalarını bankacılık hizmetleri, vb. gibi veri güvenliği ve mahremiyetin önem arz ettiği operasyonlarda kullanırken bu uygulamalara güvenmediğini ifade etmiştir.

Yapılan anket çalışması, yapay zekâ tabanlı uygulamalardan sadece biri olan sohbet robotları temel alınarak gerçekleştirilmiştir ve anket sonuçlarından da anlaşılacağı üzere yapay zekâ tabanlı uygulamalar sıklıkla kullanılmaktadır. Hatta bu uygulamaların kişisel verileri işlediğini bilmeyen ve/veya bu uygulamaların güvenilirliğinden emin olmayan kişiler tarafından da kullanıldığı görülmektedir. Dolayısıyla yapay zekâ, insan hayatına değer katmayı amaçlasa da çıktı üretmesi için işlemesi gerekli olan veriyi en doğru şekilde ve kişisel veri mahremiyeti ve veri güvenliği ilkelerine bağlı kalarak kullanmalıdır.

Federe öğrenme modeli, bir önceki bölümde detaylıca anlatıldığı gibi mahremiyet korumalı yapay zekâ uygulamaları geliştirmek için kullanılabilecek önemli yöntemlerden biridir. Bununla beraber bir sonraki başlıkta önerilen özelliklerin de yapay zekâ uygulamalarını veri mahremiyeti konusunda güçlü kılacağı düşünülmektedir.

4.3. Öneriler (Recommendations)

Sohbet robotlarının, kişisel veri mahremiyeti ilkesine uygun geliştirilmesi, tasarlanması ve kullanılması için gerekli önlemlerin alınması gerekmektedir. Bununla ilgili olarak yasal mevzuatlarla ve tavsiye niteliğindeki bazı rehberler ile kişisel veri mahremiyetine uygunluk sağlanabileceği görülmüştür.

- *Privacy by Design* ilkesi ile sohbet robotu uygulamaları gizlilik prensipleri düşünülerek tasarlanmalıdır.
- *Amaca Bağlılık* ilkesi gereğince kişilere, verilerinin hangi amaçla alındığı kaydedildiği ve işlendiği açık ve doğru bir şekilde açıklanmalı ve amaçla bağdaşmayan türden veriler toplanılmamalıdır.
- *Veri Minimizasyonu* ilkesi ile kişisel bilgilerin toplanması, yasal olarak belirtilen amaçlar için gerekli olan kadarı ile sınırlı kalmalıdır. Kişisel olarak tanımlanabilir bilgilerin toplanması kesinlikle asgari düzeyde tutulmalıdır [33].
- *Silme hakkı* gereğince; veri sahipleri, işlenen verilerini silme talebinde bulanabilirler. Bu talepler karşılanmalı veya silinmesi talep edilen veriler, yasal dayanaklarda belirtilen uygun yöntemler ile anonim hale getirilmelidir.
- *Açık rıza* ilkesi ile sohbet robotunu kullanacak kullanıcının açık rızası alınmalıdır. Kullanıcıya, kişisel veri toplandığına, işlendiğine ve bunun hangi amaçla yapıldığına ilişkin bilgilendirmeler ışığında açık rıza isteği sorulmalıdır [13].
- *Aydınlatma metni* ilkesi gereğince veri sahipleri, hangi verilerinin hangi amaçla ve ne kadar süre işleneceğine dair bilgilendirilmelidir.

4.4. Privacy by Design

Privacy by Design ilkesi, geliştirilmesi planlanan uygulamanın tasarım ve mimari aşaması dâhil olmak üzere ürünün tüm yaşam döngüsü boyunca veri koruma kurallarının dikkate alınmasıdır. Bu ilke kapsamında *Kanada Ontario Bilgi ve Gizlilik Kurulu Başkanı Ann Cavoukian* tarafından yedi temel prensip yayımlanmıştır [33]:

- Çalışmaların önleyiciliği ilkesi gereğince bir uygulamanın kullanımı esnasında çıkabilecek mimari veya teknik veri koruma sorunlarının önceden tespit edilmesi ve ortaya çıkmalarının engellenmesi hedeflenmelidir.
- *Privacy by Default* ilkesi gereğince uygulamaların standart varsayılan ayarları kullanıcı gizliliğini koruyacak şekilde yapılandırılmalıdır.
- *Gizlilik ilkesi* tasarıma entegre edilmelidir. Gizlilik prensipleri, uygulamanın tasarlanması aşamasında dikkate alınmalı ve uygulama tasarımı bu temel üzerine inşa edilmelidir.
- Kullanıcı, gizlilik prensibi çerçevesinde estetikten mahrum bırakılmamalıdır.
- Verinin, uygulama içinde toplandığı andan itibaren geçirdiği tüm yaşam döngüsü süresince güvenliği sağlanmalıdır.
- Uygulamada, veri işlemi sırasındaki her aşama hakkında şeffaf olunmalı ve kullanıcılar bilgilendirmelidir.
- Kullanıcı çıkarları en üst seviyede tutulmalı ve kullanıcıya saygı ilkesi gereğince hareket edilmelidir.

5. SONUÇLAR (RESULTS)

Yapay zekâ ve veri birbirinden beslenen iki önemli kavramdır. Yapay zekâ için kaynak olan veriler, yapay zekâ teknolojilerine sahip sistemler için bir malzeme işlevi görür. Son yıllarda hem ülkemizde hem de dünyada kişisel veri mahremiyetine verilen önemin artmasıyla birlikte yapay zekâ konusu da kişisel verilerin mahremiyeti açısından önemli bir olgu haline gelmiştir. İnsanların kişisel veri mahremiyeti üstündeki bilinci ve farkındalık düzeyi artınca bu teknolojilerin mahremiyete etkisi üstünde daha kapsamlı çalışmaların karşımıza çıkacağı ise yadsınamaz bir gerçektir.

Bu çalışma kapsamında, genel olarak yapay zekâ tabanlı sistemlerin kişisel veri mahremiyeti üzerine etkisi anlatılmıştır. Yapay zekânın veri ile olan ilişkisine ve veri işlemenin kişileri mağdur edebilecek riskler taşıdığına değinilmiştir. Bu riskleri ortadan kaldırmak ve yapay zekâyı risklerinden arındırarak kişisel verilere saygılı sistemler haline dönüştürmek için ulusal ve uluslararası düzenlemelerde ve kanunlarda üstünde durulan ilkelere ve önerilere yer verilmiştir.

Yapılan literatür taramasında, bu alandaki çalışmaların büyük bir kısmının uygulama tabanlı çalışmalardan çok araştırma şeklinde olduğu görülse de son yıllarda uygulama çalışmalarına yönelik büyük bir artış yaşandığı da gözlemlenmiştir. Yapay zekânın kişisel verileri suiistimal etmesine engel olmak amacıyla özellikle veri koruma otoriteleri tarafından sunulan çözüm önerilerden en dikkat çeken ve üstünde durulan önerinin ise *Federe Öğrenme* yöntemi olduğu görülmüştür. Federe öğrenmenin karmaşık bir sisteme sahip olması, sunucuları yormaya yatkın olması gibi dezavantajları olsa da bu dezavantajlar, iyi tasarlanan sistemlerle ortadan kaldırılarak daha güvenli sistemler tasarlanabileceği görülmüştür.

Ayrıca çalışma kapsamında, bir yapay zekâ ürünü olan ve kullanımı her sektörde gittikçe artan sohbet robotları üzerine bir inceleme çalışması yapılmıştır. Sohbet robotlarının uygulamalarda kullanım yaygınlığı ve bir sohbet robotunun kullanıcı verilerini ne şekilde topladığı ve işlediği ile ilgili detaylara yer verilmiştir. Bu bağlamda; ülkemizde hem sohbet robotlarının kullanımını hem de kişilerin veri güvenliği ve mahremiyeti farkındalığını ölçmek için bir anket çalışması yapılmıştır. Yapılan anket çalışması 100 kişi tarafından yanıtlanmış ve bunların %57,5'i sohbet robotlarını kullandığını; %42,5'i ise kullanmadığını ifade etmiştir. Kullanıcıların sohbet robotlarını %21,4 oranı ile en fazla bankacılık işlemleri için kullandığı görülmüştür. Ayrıca, kullanıcıların %45'i bu uygulamaların güvenilirliği konusunda emin olmadığını düşünürken, %26'sı güvendiğini, %13'ü ise güvenmediğini belirtmiştir. Bunun yanı sıra kullanıcıların %62,1'i bu servislerin kişisel verileri kaydedip işleyebileceğini bilmediğini; %37,9'luk kesim ise bildiğini belirtmiştir. Bu durum bir bakıma, kişisel veri güvenliği farkındalığı konusunda toplumda eksikler olduğunu göstermektedir.

Tüm bunların yanında, sohbet robotlarını kişisel veri güvenliğini sağlayarak kanunlara uygun duruma getirmek için uygulanması gereken önemli ilkeler anlatılmış ve *Kanada Ontario Bilgi ve Gizlilik Kurulu Başkanı Ann Cavoukian* tarafından yayınlanan ve bugün birçok kesim tarafından kabul edilen *Privacy by Design* ilkesi ve buna ait yedi temel prensip anlatılmıştır.

Sonuç olarak, yapay zekâdan faydalanılması ve bu teknolojiler aracılığıyla çeşitli verilerin işlenmesi her ne kadar ticari ve sosyal açıdan önemli bir gelişme olarak kabul edilse de veri güvenliği açısından önemli riskleri içinde barındırmaktadır. Ancak, yapay zekâ riskleri düşünüldüğünde vazgeçilen bir alan olmamalı; tam aksine gerekli ve doğru bir şekilde korunmuş ve gizlenmiş verilerle beslenerek geliştirilmeli ve kullanılmalıdır.

KAYNAKLAR (REFERENCES)

[1] A. Süzen, K. Kayaalp, "Büyük Verilerde Gizlilik Tabanlı Yaklaşım: Federe Öğrenme", *International Journal of 3d Printing Technologies and Digital Industry*, 3(3), 297-304, 2019.

[2] İnternet: M.V. Dülger, Yapay Zekâ Teknolojileri ve Veri Koruma Hukuku, https://www.researchgate.net/publication/349552759, 14.12.2021.

[3] L. Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?", *SSRN Electronic Journal (3386914)*, 2018.

[4] Ş. Eroglu, "Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi", *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 35(2), 130-153, 2018.

[5] D. Kamarinou, M. Christopher, S. Jatinder, "Machine Learning with Personal Data", *Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016*, 2016.

[6] L. Li, F. Yuxi, M. Tse, K. Lin, "A Review of Applications in Federated Learning", *Computers & Industrial Engineering*, 149(5), 2020.

[7] K. Chandiramani, D. Garg, N. Mahesvari, "Performance Analysis of Distributed and Federated Learning Models on Private Data", *Procedia Computer Science*, 165, 349-355, 2019.

[8] Y. Wang, Y. Tong, D. Shi, "Federated Latent Dirichlet Allocation: A Local Differential Privacy Based Framework", *Proceedings of the AAAI Conference on Artificial Intelligence*, 34(04), 6283-6290, 2020.

[9] A. A. Süzen, M. A. Şimşek, "A Novel Approach to Machine Learning Application to Protection Privacy Data in Healthcare: Federated Learning" *Namık Kemal Tıp Dergisi*, 8(1), 22-30, 2020.

[10] Y. Canbay, Y. Vural, Ş. Sağıroğlu, "Mahremiyet Korumalı Büyük Veri Yayınlama İçin Kavramsal Model Önerileri", *Politeknik Dergisi*, 23(3), 785-798, 2020.

[11] İnternet: Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, AçıkVeri Projesi, https://cbddo.gov.tr/projeler/acik-veri/, 13.12.2021.

[12] İnternet: Kişisel Verileri Koruma Kurumu, Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zekâ-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler, 15.12.2021.

[13] İnternet: Kişisel Verileri Koruma Kanunu, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5, 14.12.2021.

[14] İnternet: Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf, 26.09.2022.

[15] O. Sarı, "Yapay Zekânın Sebep Olduğu Zararlardan Doğan Sorumluluk", *Türkiye Barolar Birliği Dergisi,* 147, 251-312, 2020.

[16] Council of Europe, **Guidelines on Artificial Intelligence and Data Protection**, Directorate General of Human Rights and Rule of Law, 01, Fransa, 2019.

[17] A. Akıncı, **Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti**, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı Uzmanlık Tezi, 2019.

[18] The Norwegian Data Protection Authority Committee, **Artificial Intelligence and Privacy Report**, Norwegian Data Protection Authority, Norwegian, 2018.

[19] O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, A. Das, "Differential Privacy-enabled Federated Learning for Sensitive Health Data", *arXiv:1910.02578*, 2020.

[20] M. Pettai, P. Laud, "Combining Differential Privacy and Secure Multiparty Computation", *Proceedings of the 31st Annual Computer Security Applications Conference*, 421-430, 2015.

[21] İnternet: M. A. Sarıkaya, Yapay Zekâ ve Mahremiyet, https://medium.com/@sarikayameh?source=post_page-45f8731736-, 11.12.2021.

[22] K. Hu, Y. Li, M. Xia, J. Wu, M. Lu, S. Zhang, L. Weng, "Federated Learning: A Distributed Shared Machine Learning Method", *Complexity*, 2021(2), 1-20, 2021.

[23] İnternet: R. Yeşil, Federated Learning, https://medium.com/datarunner/federe-%C3%B6%C4%9Frenme-federated-learning-8ad87791c0b5, 12.12.2021.

[24] T. Yang, G. Andrew, H. Eichner, H. Sun, W. Li, N. Kong, D. Ramage, F. Beaufays, "Applied Federated Learning: Improving Google Keyboard Query Suggestions", *arXiv:1812.02903*, 2018.

[25] İnternet: F. Hartman, Federated Learning for Firefox, https://florian.github.io/federated-learning-firefox/, 14.12.2021.

[26] İnternet: Intel Works with University of Pennsylvania in Using Privacy-Preserving AI to Identify Brain Tumors, https://newsroom.intel.com/news/intel-works-university-pennsylvania-using-privacy-preserving-ai-identify-brain-tumors/#gs.oak7q9, 01.02.2022.

[27] J. Vogel, **Chatbots: Development and Applications**, Yüksek Lisans Tezi, HTW Berlin University of Applied Sciences, International Media and Computing Faculty, 2017.

[28] Z. Seyitoğlu, **Türkiye'de Dijital Halkla İlişkilerde Değişen Müşteri Deneyimi: Chatbot Uygulamaları**, İstanbul Kültür Üniversitesi, Yüksek Lisans Tezi, Mayıs 2019.

[29] İnternet: Türkiye Cumhuriyeti Ticaret Bakanlığı, Chatbot Kurgusunun Yapılması, https://www.eticaret.gov.tr/cevrimiciegitim/chatbot-kurgusunun-yapilmasi-64, 10.12.2021.

[30] İnternet: H. Charatan, Chatbots vs. GDPR, https://chatamo.com/chatbots-vs-gdpr-interact/, 13.12.2021.

[31] İnternet: Yapay Zekâ Reklamcılığı ve Kişisel Verilerin korunması, https://cukurpartners.com/tr/yapay-zeka-reklamciligi-ve-kisisel-verilerin-korunmasi, 26.10.2022.

[32] İnternet: Google Formlar (Google Forms), https://www.google.com/intl/tr_tr/forms/about/, 31.01.2022.

[33] A. Cavoukian, **Privacy by Design**, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, Information & Privacy Commissioner, Canada, 2010.