KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

SOHBET ROBOTLARI (CHATGPT ÖRNEĞİ) HAKKINDA BİLGİ NOTU

1- Sohbet Robotu (Chatbot) Nedir?

Sohbet robotu, kullanıcının bir arayüz aracılığı ile kendisine verdiği görevleri/direktifleri yerine getirmeye çalışan, son kullanıcıyla insan konuşmasını simüle eden bir yazılım olarak tanımlanabilir. Kullanıcıların sohbet robotuyla kurduğu iletişim sesli, yazılı vb. yöntemler ile olabilir. Kullanıcı, sohbet robotu ile iletişime geçtiğinde sohbet robotunun, kullanıcı tarafından verilen girdileri anlaması gerekir. Bu girdilerle, kullanıcı tarafından verilen direktifleri analiz edip buna göre bir işlem gerçekleştirmekte, sorulara ve isteklere anında yanıt vererek kullanıcıların bilgiye ulaşmasını kolaylaştırmaktadır. Sohbet robotları, kullanıcıların girdilerini anlamak için doğal dil işleme (Natural Language Processing-NLP) tekniklerinden faydalanır.

Yapay zekâ uygulamaları ile desteklenmesiyle karşımıza çıkan "yapay zekâ sohbet robotları" kullanıcıların girdileri doğrultusunda sadece talebi anlamakla kalmayıp bağlam, niyet, duyguyu da anlamlandırmakta ve gerçekleştirilen her bir konuşma ile kullanıcı hakkında bilgi elde etmesi kendisini daha akıllı kılmaktadır[1]. Özellikle, yapay zekâ sohbet robotlarının, kullanıcılarla önceki etkileşimlerinden elde ettikleri bilgi ile süreklilik arz eden öğrenme ve gelişme sürecine sahip olmaları, onları diğer sohbet robotlarından ayırmaktadır.

[1]Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, https://cbddo.gov.tr/SharedFolderServer/Genel/21.Chatbot-Uygulamas%C4%B1-ve-ChatGPT-%C3%96rne%C4%9Fi-De%C4%9Ferlendirme-Raporu.pdf, s 13

2- Yapay Zekâ Sohbet Robotları Ne İşe Yarar?

Yapay zekâ sohbet robotları; doğal dil işleme (NLP) teknolojisiyle birlikte genellikle; alt dalları olan doğal dil anlama (NLU) ve doğal dil üretimi (NLG) teknolojilerinden faydalanmaktadır.
Bu teknolojilerle;

- İnsan dilinin anlamlı bir şekilde yorumlanması,
- Kullanıcı girdisi doğrultusunda niyetin anlamlandırılması,
- İçeriğin belirlenerek oluşturulan cümlelerle çıktının ortaya konulması sağlanmaktadır.

Yapay zekâ sohbet robotları;

- Müşteri destek,
- Soru cevaplama,
- Kod oluşturma ve programlama,
- Bilgi arama,
- Metinleri kontrol etme ve gözden geçirme,
- İçerik oluşturma,
- Çeviri yapma
- Duygu analizi gerçekleştirme

gibi işlevler ile insan ihtiyacını en alt seviyeye indirerek ve zaman, maliyet ve performans açısından fayda sağlayarak kullanıcıların, kısa zamanda bilgi, çözüm veya sonuç elde etmesi mümkün kılınmaktadır.

Özellikle, OpenAI'ın ChatGPT, Apple'ın Siri, Amazon'un Alexa ve Google'ın Gemini gibi tüketicilere yönelik iyi bilinen akıllı sanal asistanların örnek gösterileceği üzere pek çok yapay zekâ sohbet robotu uygulamalarının, günlük hayata gitgide adapte olduğunu görmekteyiz. Bununla birlikte, kurumsal anlamda, müşterilere ve çalışanlara yardımcı olmak için yapay zekâ sohbet robotu uygulamalarının kullanımının günden güne arttığı görülmektedir.

3- Hangi Kişisel Veriler İşlenir?

Yapay zekâ destekli sistemler, en iyi performansla çalışabilmek için doğası gereği çeşitli ve büyük miktarlarda veriye ihtiyaç duymaktadır. Bu çerçevede, uygulamanın kullanıldığı yere ve amaca bağlı olarak işlenen veriler farklılık arz etmekle beraber, hizmet sağlamak, yönetmek, sürdürmek ve/veya analiz etmek, daha iyi bir kullanıcı deneyimi sağlamak, hizmetleri geliştirmek, kullanıcılar ile iletişime geçmek, bilgi teknolojileri sistemlerinin güvenliğini sağlamak, yeni programlar ve hizmetler geliştirmek, yasal yükümlülüklerin yerine getirilmesi ve veri sorumlularının meşru menfaatlerinin korunması gibi birçok amaçla işlenebilmektedir.

Yapay zekâ sohbet robotları kullanılırken temel olarak;

- Bir hesap oluşturduğunuzda; adınız, iletişim bilgileriniz, hesap kimlik bilgileriniz, ödeme kartı bilgileriniz ve işlem geçmişiniz de dahil olmak üzere hesap bilgileri,
- Uygulamalar kullanıldığında sağlanan girdilere, dosya yüklemelerine veya geri bildirimlere dahil olan içerik bilgileri,
- Gönderilen mesajların içeriği ve iletişim bilgileri,
- Sosyal medya sayfaları ile iletişimde bulunulduğunda verilmesi seçilen sosyal medya bilgileri,
- Tarayıcının veya cihazın otomatik olarak gönderdiği İnternet Protokolü (IP) adresi, tarayıcı türü ve ayarları, erişim zamanları, bilgisayar veya mobil cihazın türü gibi bilgiler,
- Çerez bilgileri ile kişiler tarafından sağlanan (metin içeriği, konuşma ve ses verisi vb.) diğer veriler işlenebilmektedir.

4- Kişisel Veri Güvenliği Açısından Yapay Zekâ Sohbet Robotu Uygulamaları Nasıl Değerlendirilebilir?

Bu tür uygulamaları kullanırken öncelikli olarak kişilerin kullanım amaçları ve farkındalık düzeyleri önem arz etmektedir.

Kişisel veri güvenliği açısından yapay zekâ sohbet robotlarındaki şeffaflık konusu dikkate alınması gereken konulardan biridir. Bu tür uygulamaların, işlediği verilerin nasıl ve hangi amaçlar için kullanıldığı, kimlerle paylaşılacağı, hangi verilerin ne kadar süreyle saklanacağı, veri sorumlusunun ve varsa temsilcisinin kimliği ile ilgili kişinin hakları gibi hususlarda yeterli bilgilendirmeyi yapabilmesi, ilgili kişilerin kişisel verileri üzerindeki kontrolü sağlayabilmesi açısından dikkat etmesi gereken hususlardandır.

Bunun yanında ilgili kişilerin mahremiyetlerini riske atabilecek düzeyde bilgi paylaşması (aşırı paylaşım yapılması vb.) şeklinde kullanıcı farkındalık eksikliğinden kaynaklı problemler yaşanabileceği gibi sohbet robotu uygulamalarındaki teknik açıklıkların sömürülmesi sonucu siber olaylara konu olması sebebiyle de veri ihlalleri gibi birtakım problemlerin yaşanması riski söz konusudur. Çocuklara ilişkin yaş tespiti için yeterli önlemlerin alınmaması gibi problemler doğabilir.

5- Sohbet Robotu Uygulamaları Geliştirilirken Nelere Dikkat Etmelidir?

- Kişisel verileri işlemeye başlamadan önce risk değerlendirmesi yapılmalıdır.
- Uygulamalar oluşturulurken hesap verebilirlik ilkesine uygun hareket edilmelidir.
- Kişisel veri işleme faaliyetleri, kişisel verileri koruma mevzuatında belirlenen genel ilkelere uygun gerçekleştirilmelidir.
- Kişisel veriler 6698 sayılı Kişisel Verilerin Korunması Kanununun 5 inci ve 6 ıncı maddelerine uygun olarak işlenmelidir.
- Kişisel veriler işleniyorsa bunun yasal dayanağı açıkça belirtilmelidir.
- 6698 sayılı Kişisel Verilerin Korunması Kanununun 10. maddesi çerçevesinde veri sorumluları, kişisel verilerin elde edilmesi sırasında aydınlatma yükümlülüğünü yerine getirmelidir.
- Kişisel veri güvenliğine ilişkin gerekli teknik ve idari tedbirler alınmalıdır. Bu kapsamda;

Kişisel veri işleme faaliyeti söz konusu olan bu tarz uygulamaların mahremiyetin korunması ve veri güvenliğinin sağlanması adına uluslararası kabul görmüş belirli standartlara uygun olması, sertifikalarının bulunması ve başlangıçtan itibaren mahremiyet ve varsayılan mahremiyet yaklaşımlarının uygulamaların geliştirilmesi sürecinde her aşamada dikkate alınması önem arz etmektedir.

Veri iletişiminde metin, ses, konuşma ve görüntü gibi girdilerin barındırılacak ortamlara iletilmesine yönelik güvenli yöntemler tercih edilmelidir.

- Yapay zekâ alanında faaliyet gösteren geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar için Kişisel Verileri Koruma Kurulu tarafından belirlenen tavsiyelere dikkat edilmelidir[2].
- Veri sorumlusu ya da veri işleyen olarak kişisel verilerin korunması mevzuatı kapsamındaki yükümlülüklerin yerine getirilmesi gerekmektedir.
- Çocuklara yönelik olarak yaş tespitinin doğru ve güvenilir şekilde yapılması gerekmektedir.
- Özellikle çocukların olumsuz deneyimler yaşamasını engellemek için proaktif bir yaklaşım benimsenmelidir.

[2]https://kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Nasuh Akar Mahallesi, 1407. Sokak No:4 06520
Balgat-Çankaya/ANKARA // www.kvkk.gov.tr
Tel: 0 (312) 216 50 00 // Faks: 0 (312) 216 50 52