GELECEĞİN DİJİTAL ASİSTANLARI: CHATGPT'NİN SİRİ VE DİĞER UYGULAMALAR İLE ENTEGRASYONUNDA VERİ GÜVENLİĞİ VE DİĞER HUKUKİ SORUNLAR

1. ChatGPT ve Apple Entegrasyonu

Apple Inc. ("**Apple**"), 10 Haziran 2024'te düzenlenen *Worldwide Developers Conference* etkinliğinde, iPhone, iPad ve Mac cihazları için yeni kişisel yapay zekâ sistemi olan Apple Intelligence'ı tanıtmıştır. Apple Intelligence, ChatGPT'nin Apple işletim sistemleri ve dijital asistanı Siri ile entegrasyonu aracılığıyla, OpenAI yapay zekâ teknolojisini geniş bir kullanıcı kitlesine sunmayı ve yapay zekâ destekli hizmetlerin günlük hayatta daha yaygın hale gelmesini amaçlamaktadır. Bu sistem ile ChatGPT, Apple'ın mesajlar, e-posta, sağlık, cüzdan gibi uygulamalarına entegre olarak kullanıcı verilerine erişebilecek ve bu veriler ChatGPT'nin öğrenme ve yanıt üretme süreçlerinde kullanılacaktır. Bu entegrasyonun başarılı bir şekilde uygulanması, yapay zekâ teknolojilerinin günlük hayatta daha yaygın hale gelmesi ile kullanıcı deneyimini ve etkileşimini artırma potansiyeline sahip olsa da veri güvenliği ve gizlilik konularında dikkatli bir şekilde yönetilmesi gereken çeşitli zorlukları da beraberinde getirecektir.

Bu makalede, entegrasyonun yaratabileceği potansiyel güvenlik riskleri ve bu risklerin hukuki boyutları incelenecektir.

2. Apple Intelligence'ın Veri Gizliliği Yaklaşımı

Apple, kullanıcı gizliliğini korumayı taahhüt eden bir teknoloji devi olarak, yapay zekâ teknolojilerini ürünlerine entegre ederken, kullanıcı verilerinin koruması amacıyla bu verilerin işlenmesinde (i) yerel işleme, *on-device processing* ve (ii) özel bulut işleme, *private cloud compute* şeklinde iki ana yaklaşım benimsemiştir.

Apple, yerel işleme teknolojisi ile verilerin doğrudan kullanıcı cihazlarında tutulmasını ve işlenmesini vadederek kullanıcı verilerinin güvenliği ve gizliliği için güçlü bir koruma mekanizması sunmaktadır. *Örneğin, Apple'ın Neural Engine ve M serisi çipleri, yapay zekâ işlemlerinin çoğunu yerel olarak gerçekleştirme kapasitesine sahip olup, metin işleme, yüz tanıma ve diğer makine öğrenimi görevleri cihaz üzerinde hızlı ve güvenli bir şekilde gerçekleştirilebilmektedir.* Özel bulut işleme teknolojisi ise kullanıcı verilerinin şifrelenmiş bir biçimde gönderilerek Apple'ın güvenli bulut sunucularında işlenmesini sağlamaktadır. Apple, bu sunucuların güvenliğini ileri düzey güvenlik önlemleriyle korumayı taahhüt etmektedir. Bulut sunucularında veriler işlenirken, kullanıcıların kimliğini belirleyici bilgiler ayrılarak anonimleştirilmiş veriler kullanmaktadır. Böylece, kullanıcıların kişisel bilgileri korunmakta ve veri işleme sürecinde gizlilik sağlanmaktadır.

Apple her iki yaklaşımda da kullanıcı verilerinin gizliliğini ve güvenliğini korumak amacıyla gelişmiş şifreleme yöntemleri ve güvenlik protokolleri kullanmaktadır. Yerel işleme, verilerin cihazda kalmasını sağlayarak dış tehditlere karşı korunma sağlarken, özel bulut işleme ise yüksek işlem gücü gerektiren görevlerin güvenli bir şekilde gerçekleştirilmesine olanak tanımaktadır. Bu sayede, kullanıcı verileri hem yerel cihazlarda hem de bulut ortamında güvenli bir şekilde işlenmekte, kullanıcı mahremiyeti ve veri bütünlüğü en üst seviyede korunmaktadır.

Apple, her ne kadar verilerin yerel cihazlarda işlenmesi ve şifrelenmiş biçimde özel bulut sunucularında tutulması konusunda katı politikalar izlese de ChatGPT'nin OpenAI tarafından geliştirilmiş bir yapay zekâ modeli olduğu ve bu modelin işleyişinin veri paylaşımı gerektirebileceği dikkate alındığında, ChatGPT'nin çalışması için kullanıcı verilerinin OpenAI sunucularına aktarılması söz konusu olabilecektir. Bu noktada, kullanıcı verilerinin işlenmesi sırasında gizlilik ve güvenlik riskleri söz konusu olabilecektir.

3. Entegrasyonun GDPR ve KVKK Açısından İncelenmesi: Veri Koruması için Alınabilecek Önlemler ile Mevzuat Uyum Süreçlerinin Gerekliliği

Bilindiği üzere, Türk Hukuku kapsamında kişisel verilerin korunması, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK"**) ile sağlanmaktadır. KVKK'da yapay zekâya veya onu kullanan sistemlere ilişkin ayrı bir hüküm bulunmamakla birlikte, genel veri koruma ilkeleri, ikincil nitelikli düzenlemeler ve Kişisel Verileri Koruma Kurulu ("**Kurul**") kararları, yapay zekâ aracılığı ile kişisel verilerin işlenmesine de uygulanmaktadır.

Apple ve OpenAI, ChatGPT entegrasyonunun hukuki boyutlarını dikkate alarak kullanıcı verilerinin korunmasını sağlamak için Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği ("**GDPR**") ve KVKK mevzuatlarına uyum içerisinde bir dizi önlem almalıdır. Bu önlemlerden bazıları şu şekildedir:

i. Verilerin toplanması ve işlenmesi için kullanıcıların açık ve bilinçli onaylarının alınması gereklidir. Kullanıcılara, hangi verilerinin toplandığı ve nasıl kullanılacağı hususunda açık ve anlaşılır bir şekilde bilgilendirme yapılmalıdır *(KVKK m. 4).*
ii. Kullanıcıların verilerinin ne kadar süreyle saklanacağı açık bir şekilde belirlenmeli ve bu sürenin sorunda verilerin güvenli bir şekilde imha edilmesi sağlanmalıdır.
iii. Veri işleme faaliyetlerinin ilgili yasal düzenlemelere uygunluğu sağlanmalı ve kullanıcıların verilerinin güvenli bir şekilde işlenmesi için tasarım aşamasında dahi gerekli teknik ve organizasyonel önlemler alınmalıdır *(KVKK m. 12).* Veri şifreleme, erişim kontrolü, güvenlik duvarları gibi mekanizmalar bu kapsamda değerlendirilebilecektir.
iv. Üçüncü taraf hizmet sağlayıcılarla (OpenAI) yapılan anlaşmada, bu sağlayıcıların da veri koruma düzenlemelerine uyumlu hareket etmeleri sağlanmalıdır.
v. Kişisel verilerin işlenmesi sırasında veri minimizasyonu ilkesine uyulmalı ve yalnızca gerekli veriler, belirtilen amaç doğrultusunda ve orantılı olacak şekilde toplanarak işlenmelidir. Gereksiz veri toplanmasından kaçınılmalıdır.
vi. Söz konusu durumda Apple ve OpenAI'dan her birinin veri sorumlusu olduğu düşünüldüğünde, yurt dışında mukim iki veri sorumlusu arasında gerçekleştirilen sonraki aktarımlar da yurt dışı aktarım olarak değerlendirildiğinden, söz konusu aktarımlar KVKK m. 9 kapsamında belirtilen yurt dışı aktarım mekanizmalarına uygun bir şekilde gerçekleştirilmelidir.
vii. Kullanıcıların, verilerine erişim, düzeltme, silme ve işleme itiraz etme haklarını kullanabilmeleri için uygun mekanizmalar oluşturulmalıdır. Olası bir veri ihlali durumunda ise, ihlalin yetkili ulusal otoriteye veya sınır ötesi bir ihlal söz konusu olduğunda ilgili otoriteye bildirilmesi ve ihlalin, kişisel verileri ihlalden etkilenen ilgili kişilere ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle iletilmesi gerekmektedir.
viii. Yapay zekâ kullanan sistem ve araçların kişisel veri elde etme amaçlarının, her bir veri işleme faaliyeti için ayrı ayrı belirtilmesi gerekmektedir.
ix. Veri koruma önlemlerinin etkin bir şekilde sürdürülmesi için en güncel ve etkili yöntemler kullanılarak sürekli olarak denetlenmesi ve iyileştirilmesi gerekmektedir. Apple ve OpenAI'ın veri işleme politikalarının düzenli olarak gözden geçirilmesi ve değerlendirilmesi gerekmektedir.

Bununla birlikte, Apple cihazları üzerinden gerçekleştirilecek sesli komut, yüz tanıma ve parmak izi kullanımı gibi işlemler sonucunda işlenecek özel nitelikli kişisel veri niteliğindeki biyometrik verilerin güvenliğine ilişkin ek önlemlerin alınması ayrıca önem arz etmektedir. Zira özel nitelikli kişisel veriler, o kişiye özgü, benzersiz fizyolojik ya da davranışsal özellikleri içererek bizzat kişinin kimliğinin tanımlanmasını sağlamakta ve doğası gereği ilgili kişilerin hak ve özgürlüklerine özgü spesifik riskleri barındırmaktadır. Bu doğrultuda Kurul tarafından hazırlanan Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber ile Kurul'un 31/01/2018 tarihli ve 2018/10 sayılı *Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler Kararı* dikkate alınarak ek güvenlik tedbirlerinin alınması gerekmektedir. Buna göre, yukarıdakilere ek olarak, Apple ve OpenAI tarafından özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedür belirlenmeli; ölçülülük ilkesi kapsamında bu verilerin işleme faaliyetleri, işleme amacıyla bağlantılı olarak ölçülü olmalı ve amacı aşan işleme faaliyetlerinden kaçınılması gerektiğinden minimum düzeyde veri işleme ilkesine (veri minimizasyonu) uyulmalıdır.

Bu doğrultuda söz konusu önlemler, ChatGPT entegrasyonunda kullanıcı verilerinin korunmasını sağlayarak GDPR ve KVKK gibi mevzuatlara tam uyumlu, güvenli ve şeffaf bir veri işleme süreci oluşturmak için büyük önem arz etmektedir. Zira yapay zekâ teknolojilerinin entegrasyonu sırasında kullanıcı verilerinin korunmasına yönelik alınacak bu önlemler, yalnızca kullanıcı gizliliğini sağlamakla kalmayıp, aynı zamanda bu teknolojilerin güvenilirliğini ve etkinliğini artırarak kullanıcı güvenini de pekiştirecektir. Ancak, yapay zekâ sistemlerinin sunduğu geniş olanaklar ve beraberinde getirdiği potansiyel riskler dikkate alındığında, teknik önlemler tek başına yeterli olmayacaktır. Nitekim yapay zekâ teknolojileri hızla gelişmekte ve sürekli olarak yeni kullanım alanları ve işlevleri ortaya çıkmaktadır. Bu durum, teknik önlemlerin her zaman güncel ve etkili olamayabileceği anlamına gelmekle birlikte, yapay zekâ sistemlerinin karmaşıklığı ve öngörülemezliği, teknik önlemlerin ötesinde hukuki ve etik düzenlemelerin de gerekli olduğunu göstermektedir. Bu noktada veri koruma yasalarının ve ilgili düzenlemelerin, yapay zekâ teknolojilerinin dinamik doğasına uyum sağlayacak şekilde revize edilmesi ve bu düzenlemelerin sürekli olarak güncellenmesi önemlidir. Mevzuat uyum süreçlerinin etkin bir şekilde işletilmesi, yalnızca yasal sorumlulukların yerine getirilmesi açısından değil, aynı zamanda kullanıcı haklarının korunması ve kullanıcıların dijital dünyada kendilerini güvende hissetmeleri açısından da elzemdir.

Bu doğrultuda örneğin algoritmik kararlara tabi olmama hakkı gibi kullanıcı haklarının korunması, yapay zekâ uygulamalarının etik standartlara uygun olarak işletilmesi ve veri işleme süreçlerinin şeffaflığı, mevzuat uyum süreçlerinin merkezinde yer almalıdır. GDPR m. 22 kapsamında salt algoritmik kararlara tabi olmama hakkı, bireylerin tamamen otomatikleştirilmiş süreçlerle alınan kararlara karşı korunmasını sağlamaktadır. Bir diğer ifade ile bu hak insan denetimini zorunlu kılmakta ve ilgili kişiler hakkında yeni bir durum yaratan veya meydana getiren salt algoritmalar tarafından verilmiş kararların, doğrudan uygulanmasını ilgili kişinin açık rızası bulunmadıkça yasaklamaktadır. Bu doğrultuda GDPR, otomatik bireysel kararlar karşısında veri sorumlusu tarafından ilgili kişinin hak ve özgürlükleri ile meşru çıkarlarını güvence altına almaya yönelik uygun önlemler alınmasını, ilgili kişinin en azından bir insan müdahalesini isteme, görüşünü belirtme ve karara itiraz etme hakkını yerine getirmesini öngörmektedir.

KVKK kapsamında insan katılımı olmaksızın salt algoritma çıktıları ile alınan otomatik bireysel kararlar ile insan müdahalesi içeren kararlar arasında bir ayrım yapılmamış ve bu duruma KVKK tahtında spesifik bir hukuki sonuç atfedilmemiş olsa da Kurul'un rehberlerinde "*bireylerin münhasıran kendi görüşleri dikkate alınmaksızın otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetler tasarlanması*" gerekliliğine yer verilmektedir. Nitekim KVKK'nın 11. maddesi uyarınca da ilgili kişilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun doğmasına itiraz etme hakkı da unutulmamalıdır. Dolayısıyla, Siri ve ChatGPT entegrasyonu ile elde edilebilecek kullanıcıların ekonomik durumu, alışveriş alışkanlıkları, sağlık durumları, davranış biçimleri gibi genel nitelikli verilerinin otomatik olarak işlenmesi KVKK kapsamında açıkça yasaklanmamış olsa da Kurul'un rehberlerinde bu durumun önüne geçilmesi gerekliliğine yer verilmektedir ve ilgili kişilerin aleyhe sonuçlara itiraz etme hakkının mevcudiyeti KVKK'da açıkça düzenlenmektedir.

Bunlara ek olarak her ne kadar kişisel verisi işlenen ilgili kişiler, KVKK kapsamında kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin düzeltilmesini, silinmesini veya yok edilmesini isteme gibi haklara sahip olsa da kişinin bu haklarını nasıl kullanacağı, taleplerini kime yönelteceği, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması halinde kime itiraz edileceği konusunda bir kesinlik bulunmamaktadır. Bu sebeple söz konusu belirsizliklerin ortadan kaldırılması ve ilgili kişilerin haklarını kullanabilmesi için gerekli sistemlerin kurulması sağlanarak en azından ilgili kişi haklarının etkin korunması gerekmektedir. Zira bu belirsizlikler ilgili kişi hakkının uygulanma ihtimalini oldukça azaltmaktadır.

Belirtildiği üzere, Apple cihazları gibi işlemci sahibi cihazlar tarafından yazılım veya donanım özellikleri kullanılarak önceden hazırlanan algoritmalarla yapılan işlemlerde, insan müdahalesi olmadan kişisel verilerin işlenmesi sonucunda doğabilecek hak kayıplarının önüne geçilmesi amacıyla ilgili kişilerin münhasıran kendi görüşleri dikkate alınmaksızın otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetler tasarlanmaması öngörülmektedir. Bu nedenle söz konusu entegrasyon sonucu Apple cihazlarında kullanılan algoritmalarla yapılan veri işleme eylemleri sırasında kullanıcıların haklarının korunması hususunda ilgili mekanizmaların kurulmaması KVKK'ya aykırılık teşkil edebilecektir. Buna ek olarak, mevcut durum Anayasa'nın 17. maddesi ile güvence altına alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkının da ihlalini doğurabilecektir. Bu nedenle söz konusu entegrasyonun farklı hukuklarda yaratacağı hak ihlallerinin önüne geçilmesi amacıyla, Apple ve OpenAI'ın gizlilik politikalarını tüm bu unsurlar dikkate alınarak düzenlemeleri, farklı veri koruma mevzuatlarına sahip ülkelerin ise bu mevzuatlarını revize etmeleri gerekmektedir.

4. Sonuç

ChatGPT'nin Siri ve diğer Apple uygulamaları ile entegrasyonu, kullanıcı deneyimini zenginleştirirken aynı zamanda veri güvenliği ve gizlilik konularında önemli zorluklar yaratmaktadır. Apple her ne kadar yerel işleme ve özel bulut işleme yaklaşımlarıyla kullanıcı verilerinin gizliliğini korumayı taahhüt etse de kullanıcıların kişisel verilerinin güvenli bir şekilde işlenmesi açık rıza alınması, veri minimizasyonu, şifreleme, veri işleme sürelerinin belirlenmesi ve kullanıcı haklarının korunması gibi önlemlerle sağlanmalıdır. Apple ve OpenAI'ın, ChatGPT entegrasyonunda kullanıcı verilerinin korunması için GDPR ve KVKK gibi mevzuatlara uyum sağlaması da büyük önem arz etmektedir. Böylece, hem Apple ve OpenAI gibi teknoloji devleri hem de ulusal yasama organları, kullanıcıların veri güvenliğini ve gizliliğini en üst düzeyde koruyarak dijital asistanların ve yapay zekâ teknolojilerinin sorunsuz bir şekilde entegrasyonunu sağlayabilecektir.

***

Herhangi bir sorunuz olması halinde bizlerle her zaman iletişime geçebilirsiniz.

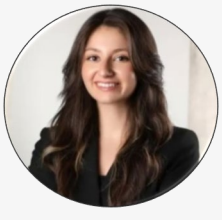
İletişim

Can Güner
Kurucu Ortak
can.guner@bicerguner.com

Burçak Kurt Biçer
Yönetici Ortak
burcak.bicer@bicerguner.com

Uğurkan Şeber
Yönetici Avukat
ugurkan.seber@bicerguner.com

Elif Şatır
Kıdemli Avukat
elif.satir@bicerguner.com



İrem Efe
Avukat
irem.efe@bicerguner.com