

ChatGPT'nin Gölgesinde Kişisel Verilerin Korunması

Ahmet, DEMİRTAŞ
Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü Doktora Öğrencisi
ademirtas@solakpartners.com
ORCID ID : 0009-0001-6200-0714

ÖZ

ChatGPT ve benzeri yapay zekâ teknolojilerinin hayatımıza bu derece hızlı girdiği günümüzde meselenin hukuki uyum yönü yine tartışmalara sebep olmuştur. Çok büyük miktarda kişisel veri işleyen bu yapay zeka teknolojileri özellikle kişisel verileri koruma hukukunun temel prensipleriyle doğrudan çelişebilmekte ve bu prensipleri ihlal edebilmektedir. ChatGPT gibi diyalog modelleri özünde bir yazılım olmakla birlikte, bu yapay zeka teknolojisinin diğer yazılımlardan belki de ayrılan en önemli özelliği düzenli ve güncel bir şekilde veri ile eğitilmesi gerekesidir. Başka bir deyişle, veri ChatGPT'nin enerji kaynağıdır ve verilerin bu derece fazla kullanılmadığı bir durumda ChatGPT verimli olmaktan çok uzak olacaktır. İşlenen veriler arasında kişisel veriler de büyük yer tuttuğundan, doğal olarak hukuk birtakım sınırlamalar ve güvenceler öngörecektir ve kişileri koruyacaktır. Fakat her zaman olduğu gibi yine teknoloji çok hızlı yol alırken, yasa koyucular meseleyi düzenlerken gecikmektedir. Tam da bu durumda hukukun temel prensipleri en azından asgari korumaları sağlayacak güvenceler içermektedir. Özellikle, sınırlı amaçla veri işleme, veri minimizasyonu ilkesi ve şeffaflık prensibi adeta ChatGPT için tasarlanmış gibi muhtemel veri koruma hukuku ihlallerini engelleyici bir role sahiptir. Kişisel veri koruma otoritelerine bu noktada önemli görevler düşmekte ve yapay zekâ teknolojilerinin artlarından mahrum kalmadan, hukuki uyumu sağlayacak tedbirler alınmalıdır. Aksi halde kişiliğin bir parçası olan kişisel verilerin korunması hakkı ChatGPT gibi yapay zekâ teknolojilerinin faydaları karşısında toplumun ve bu teknolojileri üreten şirketlerin gözünde harcanabilir bir hak olarak görülür.

Anahtar Kelimeler: ChatGPT, Yapay Zeka, Kişisel Veri Koruma Prensipleri

Protecting Personal Data In The Shadow Of The ChatGPT

ABSTRACT

In today's world, where artificial intelligence technologies like ChatGPT have rapidly entered our lives, the legal aspect of the issue has once again sparked debates. These artificial intelligence technologies processing a massive amount of personal data are particularly in direct conflict with the fundamental principles of data protection law and violate these principles. While models like ChatGPT are fundamentally software, a distinguishing feature of this artificial intelligence technology is the necessity for regular and up-to-date training with data, setting it apart from many other types of software. In other words, data is the fuel for ChatGPT, and if the model is not regularly exposed to a significant amount of data, ChatGPT will be far from efficient. Given the substantial presence of personal data within the processed information, legal frameworks naturally anticipate a set of limitations and safeguards for the protection of individuals. Nonetheless, in the ever-quickenning realm of technology, legislators often find themselves trailing behind in the regulatory landscape. It is precisely in such instances that the foundational principles of law incorporate assurances, albeit minimal, to ensure essential safeguards. In particular, the principle of data limitation, data minimization and the transparency play a role seemingly designed

for preventing potential data protection law violations in the case of ChatGPT. At this juncture, significant responsibilities fall upon the data protection authorities, and measures should be taken to ensure legal compliance with artificial intelligence technologies' benefits without deprivation. This includes securing a balance between harnessing the advantages of these technologies and upholding legal standards. Otherwise, the right to the protection of personal data, an integral part of one's personality, might be perceived as a dispensable right in the eyes of both society and the companies which developing technologies like ChatGPT, when weighed against the benefits of artificial intelligence technologies.

Keywords: ChatGPT, Artificial Intelligence, Principles of Data Protection

Atıf Gösterme

Demirtaş, A., (2024). ChatGPT'nin Gölgesinde Kişisel Verilerin Korunması, *Kişisel Verileri Koruma Dergisi*. 6(1), 14-27.

1. GİRİŞ

ChatGPT (“GPT-4”) karmaşık talimatları yerine getirebilen, bir yazılım için kod yazabilen, araştırma yapabilen, daha önce kendisine sorulan soruları da gözeterek geniş çaplı cevaplar verebilen bir yapay zekadır. (Sun, 2022: 2) Elbette ChatGPT'nin yapabilecekleri yukarıda yer alan özellikler ile sınırlı değildir. ChatGPT bir akademik makaleyi tek başına yazabilecek kapasiteye sahiptir. (Osmanovic-Steingrimsson, 2022: 6) Yazı yazma kabiliyeti dışında GPT-4 finans, ticaret hatta hukuk dahil olmak üzere birçok alanda kayda değer tavsiyelerde bulunmaktadır. (Dowling-Lucey, 2023: 2) Bazı yazarlar gayet mümkün olabileceğini belirterek GPT-4'ün ABD’de baro sınavına girse, önemli ölçüde başarılı olacağını bile iddia etmişlerdir. (Bommarito-Katz, 2022: 9) Üstelik belki insana özgü olduğu düşünülen yaratıcı içerik üretme bakımından da ChatGPT önemli bir yol kat etmiştir. (Karakoç Keskin, 2023: 124) Örneğin, ChatGPT yazmış olduğunuz bir elektronik postayı oldukça süslü kelimelerle ifade edilen bir versiyona kolaylıkla çevirebilir. Ek olarak, ChatGPT, kişisel danışman gibi sizin son derece subjektif problemlerinizi dahi ilgilenen bir dostunuz bile olabilir. (Karakoç Keskin, 2023: 127) Kanımızca ChatGPT kullanıcılarının kişisel gereksinimlerine optimum çözümler sunabilme kabiliyetini sürekli ve güncel verilerle eğitilerek elde etmektedir. Dolayısıyla, veriler ChatGPT'nin verimli olması için olmazsa olmaz kaynaktır.

Bu derece faydalı bir yapay zekâ teknolojisi acaba 6698 Sayılı Kişisel Verileri Koruma Kanunu (“KVKK”) ve Avrupa Genel Veri Koruma Tüzüğü (“GVKT”) ile ne derece uyumludur? Veriler ChatGPT dahil olmak üzere birçok yapay zekâ teknolojisinin belkemiğini oluşturmaktadır. (Herve, 2021: 196) Zira yapay zeka teknolojileri onlara yüklenen güncel veriler sayesinde bu derece doğru analizler gerçekleştirebilmektedir. (Stiennon-Ouyang vd. , 2020: 1) Bu verilerin hiç de azımsanamayacak bir kısmı ise kişisel veridir. Hal böyle olunca, ChatGPT'nin kişisel verileri koruma hukuku ile uyum içerisinde olması önem arz etmektedir. Zira GVKT m.25'te açıkça kişisel veri işleyen uygulamaların kişisel verileri koruyan teknik ve organizasyonel tedbirleri kapsayan şekilde tasarlanması gerektiği belirtilmiştir (*privacy by design*). (Jezova, 2020: 5) Yapay zekâ uygulamalarının kişisel verileri koruma hukukunda veri minimizasyonu, sınırlı amaçla veri işleme ve şeffaflık gibi ilkelere ne derece uyumlu olduğu değerlendirilmeye muhtaçtır. Çünkü çok fazla miktarda kişisel veri işleyen ve son derece geniş şekilde her türlü gereksinimi gidermeyi amaçlayan bu yapay zeka teknolojisinin gerçek manada KVKK m.4'te yer alan genel ilkelere uygun olması kolay gözükmemektedir. Bu makale başta ChatGPT

olmak üzere yapay zekâ teknolojilerinin kişisel verileri koruma hukukunu nasıl sarstığını ve temel veri koruma prensiplerini ne derece ihlal ettiğini ortaya koyacaktır.

2. KVKK VE GVKT'NİN YAPAY ZEKÂ TEKNOLOJİLERİNE KARŞI SAĞLADIĞI HUKUKİ GÜVENCELER

KVKK'da ve GVKT'de yer alan prensipler, yapay zekâ teknolojilerinin kullandığı kişisel verilerin korunması amacıyla birçok hukuki koruma içermektedir. (Kesa-Kerikmae, 2020: 70) İlk olarak, kişisel veri ve veri işleme kavramları her iki mevzuatta da çok geniş şekilde tanımlanmıştır. (Herve, 2021: 199) Bu sayede kişiyi belirli veya belirlenebilir kılan her türlü veri kişisel veri olarak değerlendirilecek ve KVKK veya GVKT geniş bir uygulama alanı bulacaktır. (Purtova, 2018: 40) Bunun dışında, bilhassa yapay zeka teknolojilerine yönelik GVKT m.22 kişilere salt algoritmik kararlara tabi olmama hakkı tanımaktadır. Benzer korumanın KVKK'da hiç yer almaması öğretilerde haklı olarak eleştirilmiştir. (Büyüksağış, 2021: 539)

Fakat salt algoritmik karara tabi olmama hakkı sanıldığından dar bir uygulama alanına sahiptir. Örneğin, hükmün uygulanması için salt otomatik yollarla veri işleyen yapay zekâ teknolojisi olmalıdır. (Falletti, 2020: 5) Dolayısıyla, insan müdahalesinin de karar alma sürecinde etkili olduğu kararlar bakımından GVKT m.22 uygulama alanı bulmaz. (Pehrsson, 2018: 10) Ayrıca bu hakkın kullanılması için doğrudan belirli bir kişiye yönelik karar alınmış olması gereklidir. (Pehrsson, 2018: 15) Mesela, İstanbul'un Ataşehir ilçesindeki insanların suç işleme eğilimini gösteren bir karar alma süreci hükme göre GVKT m.22 kapsamındaki hakkın kullanılmasını engeller, zira kişiye yönelik değil topluluğa ya da bir grup insana yönelik karar alma gerçekleşmiştir. Ayrıca hakkın kullanımı için kişi hakkında alınan kararın hukuki veya benzer nitelikte önemli sonuç doğurması gerekmektedir. (Binns-Veale, 2021: 319) Kişinin ekonomik durumunu, sağlığını, davranışlarını etkileyen kararların önemli olduğu düşünülmektedir fakat bu konuda bir belirsizlik olması da ayrıca eleştiriye açıktır. (Tosoni, 2021: 2) Ayrıca GVKT m.22/f.2 hükmü bazı hallerde bu hakkın kullanımına istisna getirmektedir. Karar alma sürecinin sözleşmenin kurulması veya ifası için zorunlu olması, üye devlet hukukunun izin vermesi yahut karar alma sürecinin açık rıza ile işlenmesi hallerinde de bu hak kullanılamaz. Görüldüğü üzere GVKT m.22 bu belirsiz ve etkin olmayan haliyle yeterli korumayı sağlamamaktadır.

Kişisel verisi işlenen kişiler ("ilgili kişi") GVKT m.22/f.3 kapsamında insan müdahalesi talep etme, kendi fikirlerini açıklama ve karara itiraz etme hakkına sahiptir. Fakat GVKT ilgili kişinin kendi fikrini açıklaması yahut itiraz etmesi halinde yapay zekâ tarafından alınmış olan kararın tekrar kim tarafından inceleneceğini veya bu kararın hukuken geçersiz olup olmayacağı ile ilgili hiçbir hüküm içermemektedir. (Aksoy, 2022: 79) Bu sebeple biz de birçok yazar gibi maddedeki belirsizliklerin ortadan kaldırılması gerektiğini ve hakkında salt algoritmik yollarla karar alınan kişinin itirazı halinde, hakkında alınan kararın önemli ölçüde insan müdahalesi ile tekrar değerlendirilmesinin etkin korumayı sağlayacağı kanaatindeyiz. (Hert-Lazcoz, 2021, < <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/> > Erişim Tarihi: 01.03.2024) Zira bu belirsizlikler ve hakkın kullanımı için gerekli ön şartların fazla olması hakkın uygulanma ihtimalini oldukça azaltmaktadır.

GVKT m.22'de yer alan itiraz etme gibi hakların etkin kullanılabilmesinin bir diğer şartı ise ilgili kişinin kendisi hakkında alınan kararın hangi kriterlerle verildiği konusunda basit ve anlaşılabilir bir şekilde aydınlatılması gerekliliğidir. (Mitrou, 2018: 70) Bu husus öğretilerde "**açıklama talep etme hakkı**" (*right*

to explanation) olarak anılmaktadır. Açıklama talep etme hakkı, yerine getirilmesi hem açık rızaya dayalı kişisel veri işleyen yapay zekâ teknolojilerinde rızanın bilgilendirmeye dayalı olma şartını gerçekleştirilmesi bakımından gereklidir hem de hakkın kendisi şeffaflık ilkesinin bir yansımasıdır. Bu noktada bazı yazarlar açıklama talep etme hakkının fikri mülkiyet hakkını ihlal edebileceği kanısındadır. (Kaminski, 2019: 200) Fakat kişisel verisi işlenen kişileri bilgilendirmek için fikri mülkiyet hakkına konu kodun veya ürünün detayları açıklanmak zorunda değildir. (Brkan, 2018: 23) Hal böyle olunca, fikri mülkiyet hakkına konu olacak bilgiler açıklanmadan da açıklama talep etme hakkının gerekleri yerine getirilebilir. Açıklama talep etme hakkına yönelik ikinci eleştiri ise, bu hakkın teknik olarak mümkün olmaması olarak ileri sürülmektedir. (Brkan, 2018: 18) Biz bu görüşe de katılmıyoruz. Zira teknik detayları en ince ayrıntısına kadar ilgili kişiye açıklamadan basit bir şekilde salt algoritmik karara konu kıstaslar açıklanabilir. Dolayısıyla, açıklama talep etme hakkı yapay zekaya karşı önemli bir koruma sağlamaktadır ve hakkın kullanıma yönelik itirazlar isabetsizdir.

Bu korumaların dışında GVKT m.5 ve KVKK m.4'te yer alan kişisel verilerin işlenmesine ilişkin temel prensipler ChatGPT gibi yapay zekâ teknolojilerinin kişisel verileri işlerken uyması gereken ilkelerdir. Özellikle, sınırlı amaçla veri işleme, veri minimizasyonu, verilerin sınırlı süreyle verilerin muhafaza edilmesi ve şeffaflık gibi kişisel verileri koruma prensipleri yapay zekâ teknolojileri tarafından sıklıkla ihlal edilebilecek nitelikte gözükmektedir. Tam da bu prensiplerin ihlali endişesiyle yakın zamana kadar İtalya'da ChatGPT yasaklanmış idi. (Yakışır, 2023: 1) ChatGPT'yi geliştiren OpenAI şirketinin verdiği taahhütler sonucunda yasak kaldırılmıştır. Bu taahhütler arasında “kişisel verilerin hangi amaçla işlendiğinin ilgili kişilere açıklanması”, “bireysel karar alma süreçlerine ilgili kişilerin itiraz etmesi için mekanizmalar oluşturulması” ve “verilerin silinmesi talebinin kolaylıkla ileri sürülmesi” dahil edilmiştir. (Yakışır, 2023: 4)

Görüldüğü üzere, temel veri koruma prensipleri yapay zekâ teknolojilerinin kişisel verileri koruma hukukunu ihlal etmesini engelleyecek nitelikte geniş bir hukuki koruma sağlamaktadır. Üstelik temel veri koruma prensiplerini ihlal halinde GVKT m.83/f.5 toplam cironun %4'ü (yüzde dördü) veya 20.000.000 (yirmi milyon) Euro'ya kadar olan -hangisi fazlaysa- caydırıcı bir yaptırım mekanizması öngörmektedir. Bu caydırıcı yaptırım mekanizması yapay zekâ teknolojilerinin temel veri koruma hukuku prensiplerine uyması bakımından önemli bir ittirici güçtür. KVKK'nın benzer caydırıcılıkta yaptırım öngörmesinin de gerekli olduğunu belirtelim zira şu anki haliyle idari para cezaları her yıl artsa da GVKT'ye oranla oldukça düşüktür. Sonuç itibarıyla hem KVKK hem de GVKT yapay zekâ teknolojilerini üretenlerin ve geliştirenlerin kişisel verileri koruma hukukuna uygunluk bakımından çeşitli önlemleri almasını zorunlu kılmaktadır.

3. CHATGPT KİŞİSEL VERİLERİ KORUMA HUKUKUNU NASIL SARSIYOR?

Yukarıda vurguladığımız üzere yapay zekâ teknolojileri birçok temel veri koruma hukuku prensibini ihlal edebilecek niteliktedir. (Cate-Dockery, 2019: 13) Bu bölümde çeşitli veri koruma hukuku prensipleri ile ChatGPT'nin nasıl çelişebileceğini ortaya koyacağız.

3.1. Hukuka Uygun Veri İşleme Prensibi

GVKT m.5/f.1 ve KVKK m.4/f.2 (a) hükmü uyarınca kişisel veriler hukuka uygun şekilde işlenmelidir. Bu ilkeyi kişisel verilerin ancak bir hukuka uygunluk sebebinin varlığı halinde işlemenin mümkün olduğu şeklinde yorumlamak gerekir. (Yücedağ, 2019: 48) Hukuka uygunluk sebepleri GVKT m.6'da

ve KVKK m.5'te detaylı şekilde açıklanmıştır. Dolayısıyla, bu maddelerde yer alan açık rıza, kanunlarda veri işlemenin öngörülmesi, sözleşmenin kurulması veya ifası gibi hukuka uygunluk sebeplerinden birinin varlığı halinde kişisel veri işlenmesi mümkün olacaktır. “*TK v. Asociatia*” davasında vurgulandığı üzere mevzuatta yer alan hukuka uygunluk sebepleri dışında hiçbir hukuka uygunluk sebebi türetilemez. (TK v. Asociatia de Proprietari bloc M5A-ScaraA”, Case C-708/18, (2019) <https://curia.europa.eu/juris/document/document.jsf?jsessionid=06D4F3D7477DBD926540522FD69EB1C1?text=&docid=221465&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=5981253> Erişim Tarihi: 03.03.2024) Başka bir deyişle, hukuka uygunluk sebepleri sınırlı sayıdadır. Bu aşamada ChatGPT'nin hangi hukuka uygunluk sebeplerine dayanarak kişisel veri işleyebileceğini değerlendirmek gerekmektedir.

GPT-4'ü kullanan kişiler bakımından akla ilk gelen hukuka uygunluk sebebi açık rızadır. Fakat bu konuda ChatGPT kullanımına henüz başlanmadan, önceden işaretli olmayan (*opt-in*) bir kutucuğun işaretlenmesi suretiyle kullanıcılardan açık rıza alınması gerektiğinin altını çizmek isteriz. Aksi halde aktif davranışla rıza almadan, kişiler sırf uygulamayı kullanıyor diye bu pasif davranışı kullanıcıların kişisel verilerinin işlenmesine rıza vermesi olarak değerlendirmek hukuka aykırı olacaktır. (Braun, 2018: 28)

ChatGPT bakımından asıl hukuka aykırılık problemi, özellikle kullanıcı olmayan kişilerin kişisel verilerin işlenmesi bakımından ortaya çıkmaktadır. Acaba bu noktada kişisel verilerin ilgili kişi tarafından aleni hale getirilmesi bir hukuka uygunluk sebebi olabilir mi? Kanımızca ChatGPT'de kullanılan kişisel veriler çoğu zaman alenileştirme amacıyla kullanılmayacağından, verilerin aleni olması hukuka uygunluk sebebi olarak değerlendirilemez. Kişisel Verileri Koruma Kurulu'nun (“**Kurul**”), 2019 tarihli bir kararında aleni hale getirilen kişisel verilerin alenileştirilme amacı dışında kullanılması halinde veri işlemenin hukuka aykırı olduğu yönündeki kararı da bu tezimizi güçlendirmektedir. (Kişisel Verileri Koruma Kurulu (2019), <https://kvkk.gov.tr/Icerik/6623/2019-331> > Erişim Tarihi:03.03.2024)

Peki yapay zekayı eğitirken kullanılan bu kişisel verileri işlemek, veri sorumlusunun veya üçüncü kişilerin meşru menfaati kapsamında işlenmesi zorunlu olan veriler olarak görülebilir mi? Bu hususta Latin Amerika ülkelerinde, veri sorumlusunun meşru menfaatinin hukuka uygunluk sebebi olarak kabul eden bazı ülkeler bulunmaktadır. (Kramcsak, (2023), <https://www.sciencedirect.com/science/article/abs/pii/S026736492200108X> Erişim Tarihi: 03.03.2024) Veri sorumlusunun veya üçüncü kişilerin meşru menfaati gerekçesiyle kişisel veri işlenebilmesi, ilgili kişilerin temel hak ve hürriyetleri ile veri sorumlusunun veya üçüncü kişilerin meşru menfaati arasında bir denge kurulmasını gerektirir. (Ferretti, 2014: 14) Veri sorumlusunun veya üçüncü kişilerin meşru menfaatinin hukuka uygunluk sebebi olabilmesi için, kişisel veri işlemenin meşru menfaat için gerçekten **gerekli** olması gerekir. (Mitrou, 2018: 41) Kanımızca ChatGPT hem veri sorumlusuna ekonomik menfaat sağlamakta hem de toplumun bilgi ihtiyacına yönelik önemli çözümler sunmaktadır. Örneğin bugün bazı iş modelleri ChatGPT kullanarak ve eğiterek sundukları hizmetleri ve ürünleri daha cazip kılmak için adımlar atmaktadır. Dolayısıyla ChatGPT'nin veri sorumlusuna sağladığı ekonomik menfaatin dışında kullanıcılarına sağladığı tartışılmaz faydalar söz konusudur. Üstelik bu faydalar güncel ve sürekli eğitilen yapay zekâ sayesinde mümkün olduğundan, kişisel veri işlemenin katı şekilde gerekli olduğu da söylenebilir. Fakat buradaki fayda kişisel verilerin korunması hakkının özünü ihlal etmeyi meşru kılmaz. Ayrıca çok büyük oranda kişisel veri işleyen ChatGPT'nin gerekli teknik ve organizasyonel tedbirleri daha sıkı alması zorunludur. Ancak bu şartla veri sorumlusunun meşru

menfaati hukuka uygun görülebilir. Oysa yakın tarihte OpenAI şirketi gerekli teknik ve organizasyonel tedbirleri almadığı için kişisel veri ihlali yaşandığını kabul etmiştir. (OpenAI March 20 ChatGPT Outage Here's What Happened, (2023) < <https://openai.com/blog/march-20-chatgpt-outage> > Erişim Tarihi:03.03.2024)

3.2. Sınırlı Amaçla Veri İşleme Prensibi

Sınırlı amaçla veri işleme prensibi, veri sorumlularının en geç veri işleme anında veri işleme amacını belirlemesi ve bu amaç dışında başkaca bir amaç için veri işlememesi anlamına gelmektedir. (Grafenstein, 2018: 5) Ayrıca bu amacın belirli, açık ve meşru olması zorunludur. (Costa, (2013) 'Big Data, Open Data and Purpose Limitation: How Are They Linked?' < <https://www.lexology.com/library/detail.aspx?g=ab2dd08f-3e32-4e31-8447-69b658b86399> > Erişim Tarihi: 03.03.2024) Başka bir deyişle, genel bir amaçla kişisel veri işlenemez. (Koning, 2020: 58) Oysa ChatGPT gibi yapay zekâ teknolojilerinde, kişisel verilerinin toplandığı andaki amacın çok dışında kullanılabilirdiğini görmekteyiz. (Chalubinska Jentkiewicz- Nowikowska, 2022: 188) Çünkü ChatGPT eğitilerek farklı hizmetler de sunabildiğinden, kişisel verileri asıl programlanma amacının dışında da kullanılabilir. (Chalubinska Jentkiewicz- Nowikowska, 2022: 188) Hal böyle olunca, ChatGPT'nin sınırlı amaçla veri işleme prensibine uygun olduğunu söylemek güçtür. Esasen, eğitilerek kendini geliştiren ve fonksiyonunu artıran hiçbir yapay zekâ uygulamasının sınırlı amaçla veri işleme prensibine tam anlamıyla uygun davranması beklenemez. Peki veri sorumluları bu durumda nasıl bir yol izlemelidir? Her yeni amaç ortaya çıktığında yeniden rıza mı almalıdır? GVKT ve KVKK bu soruya evet cevabını vermektedir. Yine de bu durum iş hayatının gereksinimlerini gözeten bir yükümlülük değildir. Zira birçok farklı amaçla kişisel veri işlenmekte olduğundan sürekli olarak yeni bir hukuka uygunluk sebebi gerekecektir. Bu durum ise kullanıcı dostu olmadığından doğal olarak iş hayatının tercih ettiği bir yol değildir.

3.3. Şeffaflık Prensibi

Şeffaflık prensibi, kişisel veri işleme sürecinin ve işlenen verilerin kolaylıkla ulaşılabilir olması, anlaşılabilir olması ve basit bir dille ilgili kişilere aktarılması anlamına gelmektedir. (Spagnuolo-Ferreira vd., 2019: 115) GVKT m.15'te yer alan verilere erişim hakkı ilgili kişilerin veri işleme amacı, mantığı ve muhtemel sonuçlarıyla ilgili bilgi almasını mümkün kılan önemli bir hukuki korumadır. (Seizov-Wulf, 2020: 623) Şeffaflık ilkesi yapay zekâ teknolojisinin karar alma süreci hakkında açıklama talep etme hakkını da güvence altına almaktadır. Buna karşın, yakın tarihli "*Uber Drivers v. Uber B.V.*" davasında, Uber sürücülerini müşterileriyle nasıl eşleştiklerine ilişkin bilgi almak için şirkete talepte bulunmuş, Amsterdam Yerel Mahkemesi ise bu karar alma sürecinin ilgili kişiler bakımından hukuki veya önemli sonuç doğurmaması nedeniyle talebi reddetmiştir. (Uber Drivers v. Uber B.V.", Amsterdam District Court, 2021, para.4.66 < <https://ekker.legal/wp-content/uploads/2021/03/Uber-drivers-v.-Uber-transparency-requests-.docx> > Erişim Tarihi: 03.03.2024) Bizce yapay zekâ teknolojisinin karar alma süreciyle ilgili bilgi almak için alınan kararın hukuki veya önemli sonuç doğurması gerekmemelidir. Oysa hukuki veya önemli sonuç doğurma GVKT m.22'de yer alan salt algoritmik karara tabi olmama hakkının kullanılması için zorunlu bir ön koşul olarak tasarlanmıştır. Dolayısıyla da kişilerin bu hakkı kullanarak bilgi alma imkanı önemli ölçüde engellenmiştir.

ChatGPT bakımından, bu teknoloji de her yapay zekâ teknolojisi gibi ortaya çıkardığı çıktıları, hangi verileri kullanarak ve hangi ölçütleri dikkate alarak oluşturduğunu izah edebilmelidir. Fakat bu konuda da ChatGPT'nin, KVKK'nın ve GVKT'nin öngördüğü şeffaflık standartlarını sağladığını iddia etmek güçtür. Zira ChatGPT'nin oluşturduğu çıktıların hangi veriler kullanılarak ortaya konulduğu oldukça belirsizdir. Belirtelim ki şeffaflık prensibi diğer birçok hakkın kullanılması için bir ön koşul niteliğinde olduğundan, bu hakkın ihlali ilgili kişiler için büyük zararlara yol açabilir. Örneğin ChatGPT'yi işe alımda kullanan bir şirkette, bir adayın özgeçmişinin yeterli bulunmaması sebebiyle reddedilmesi senaryosunda, ChatGPT'nin kararının dayanağını bilmeyen adayın, bu karara itiraz etmesi de olanaksız olacaktır.

3.4. Veri Minimizasyonu Prensibi

Veri minimizasyonu ilkesi yeterli, ilgili ve amaçla bağlantılı kişisel verilerin dışında başka bir kişisel verinin işlenmemesi esasına dayanır. (Biega-Finck, 2021: 44-61) Elbette bu ilkenin doğal sonucu olarak işlenen veri miktarında bir azalma gerekmektedir. (Biega-Finck, 2021: 56) Veri minimizasyonu ilkesi Avrupa Birliği Adalet Divanı'nın yakın tarihli "*Norra Stockholm v. Per Nycander*" kararında da vurgulandığı üzere bir "**orantılılık**" değerlendirmesi yapmayı gerektirir. (C-268/21 "*Norra Stockholm Bygg v. Per Nycander*", 2023, para.45. < <https://curia.europa.eu/juris/document/document.jsf?text=&docid=270823&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2078240> > Erişim Tarihi: 03.03.2024) Acaba ChatGPT'nin gerçekleştirmek istediği amaçlar için bu kadar büyük miktarda kişisel veri işlemesi gerekir mi? Bu kadar büyük ölçekte veri işlemeden sağlanmak istenen amaç gerçekleştirilemez miydi? Bu sorular teknik değerlendirmeler gerektirmekle birlikte ChatGPT benzeri yapay zekâ teknolojilerinde hangi verilerin yeterli, ilgili ve amaçla bağlantılı olduğunu tahmin etmek çok zor olduğu gibi yapay zekanın eğitildikten sonra hangi verileri öğreneceğini öngörmek de olanaklı değildir. (Cate-Dockery, 2019: 15) Hal böyle olunca, ChatGPT'nin özellikle de eğitildiği aşamada kullanılan büyük miktarda kişisel veri işleme faaliyetinin ve eğitilen yapay zekanın ürettiği yeni kişisel verilerin, veri minimizasyonu ilkesiyle bağdaştığını ileri sürmek oldukça zor görünmektedir. Zira gelecekte bir şekilde verilerin kullanılacağı düşüncesiyle ilgili olabilecek ve ilgisiz tüm veriler ChatGPT'nin eğitim aşamasında işlenmektedir.

3.5. Sınırlı Süreyle Verilerin Muhafaza Edilmesi Prensibi

Sınırlı süreyle verilerin muhafaza edilmesi ilkesi kişisel verilerin işleme amacı için gerekli olan süreden daha uzun bir süre depolanmamasını gerektirir. (Council of Europe: Handbook on European Data Protection Law 2018, s.129 < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > Erişim Tarihi:03.03.2024). Başka bir deyişle, amacını gerçekleştiren ve artık bir amaca hizmet etmeyen veriler silinmelidir. (Case-136/17 "*G.C. v. Others*", 2019, para.74 < <https://curia.europa.eu/juris/document/document.jsf?docid=218106&doclang=EN> > Erişim Tarihi: 03.03.2024)

"*Digi*" kararında vurgulandığı üzere kişisel veriler sonraki işleme faaliyetlerinde ilgili kişilerin beklentilerine uygun şekilde işlenmeli aksi halde ya yeni bir hukuka uygunluk sebebine sahip olunmalı ya da artık veri silinmelidir. (Case-77/21 "*Digi v. Nemzeti*", 2022, para.50 < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CJ0077> > Erişim Tarihi: 03.03.2024)

ChatGPT bakımından ilkeyi değerlendirmek gerekirse, OpenAI şirketinin veri koruma politikasını açıkladığı metinde, kullanıcıların geçmişteki konuşmalarının aksi yönde rıza açıklanmadığı sürece 30 gün sonra silineceği belirtilmiştir. (OpenAI Data Controls FAQ < <https://help.openai.com/en/articles/7730893-data-controls-faq> > Erişim Tarihi:03.03.2024) Buna karşın mevcut konuşmaların ise süresiz kaydedileceğini ve aksi yönde aksiyon alınıncaya kadar bunların model eğitimlerde dahi kullanılabilmesi belirtilmiştir. Bizce devam eden konuşmadaki verileri model eğitimlerde kullanmayı mümkün kılan bir hukuka uygunluk sebebi yoktur. Zira burada rıza aktif bir davranışla verilmediğinden tereddüde yer bırakmayacak şekilde açık olduğu söylenemez. Kaldı ki devam eden konuşmaların sonsuza dek depolanması da sınırlı süreyle verileri muhafaza etme ilkesiyle bağdaşmaz. Bu konuşmalar kullanıcılar tarafından kaydedilmesi yönünde rıza gösterilmesi halinde depolanmalı, aksi halde silinmelidir.

3.6. Verilerin Doğru ve Gerektiğinde Güncel Olması Prensibi

Verilerin doğru ve gerektiğinde güncel olması prensibi bilerek veya ihmalle ilgili kişiler hakkında yayılan yanlış veya yanıltıcı bilgilerin engellenmesini sağlayan bir hukuki araçtır. (Hallinan-Borgesius, 2020: 2) Bu ilke uyarınca yanlış ve yanıltıcı bilgilerin derhal silinmesi veya düzeltilmesi gerekmektedir. (Council of Europe: Handbook on European Data Protection Law 2018 < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > Erişim Tarihi:03.03.2024) Belirtelim ki bilgiler her zaman doğru veya yanlış diye ayrılamayabilir. Özellikle fikirler ve yorumlar bu iki kavramın dışında bir alanda konumlanabilir. (Hallinan-Borgesius, 2020: 5) Bizce bu durumda ilgili kişilerin düzeltmeye ilişkin talepleri dikkate alınmalıdır. Bu ise önceki yorumun silinmesini gerektirmeyebilir. ChatGPT'yi incelediğimizde, ChatGPT'ye Türkiye'deki IP adresleriyle yapılan girişlerde yanlış veya yanıltıcı verilerin silinmesini veya düzeltilmesini sağlayan bir forma yahut linke rastlanmamaktadır. Dolayısıyla ChatGPT'nin anılan ilkeyi de ihlal ettiği kanaatindeyiz.

4. SALT OTOMATİK KARARA TABİ OLMAMA HAKKININ CHATGPT'NİN ALDIĞI KARARLAR BAKIMINDAN UYGULANABİLİRLİĞİ MESELESİ

4.1. Veri Sorumlusu'nun Tespiti

Veri sorumlusu GVKT m.4/f.7'de tanımlandığı üzere, veri işleme amaçlarını ve yöntemini belirleyen gerçek veya tüzel kişi, kamu kurumu yahut başkaca kuruluşlardır. ChatGPT bakımından veri sorumlusunun kullanıcılar mı yoksa OpenAI şirketi mi olduğu tartışılabilir. Örneğin X şirketi çalışanlarının bilgilerini ChatGPT'ye girip bu bilgiler ışığında verimlilik değerlendirmesi yapmasını istiyorsa, burada acaba hem ChatGPT'yi üreten OpenAI şirketi hem de X şirketi müşterek veri sorumlusu mu olmalıdır? Kanımızca OpenAI şirketi her halükârda veri sorumlusudur. Zira bu yapay zekâ sistemini tasarlayan, saf haldeki verileri sisteme entegre ederek ve yapay zekâyı eğiterek sistemi kullanıma hazırlayan ve kullanıcıların hangi amaç ve yöntemle veri işleyebileceğinin çerçevesini çizen OpenAI şirkettir. Kullanıcılar bakımından ise başkalarının kişisel verilerini ChatGPT'ye aktarıp, bu verilerin işleme amacının belirlenip belirlenmediğine göre somut olay değerlendirilmelidir. Yukarıda verdiğimiz çalışan bilgilerinin girilerek ChatGPT'den verimlilik değerlendirilmesi yapılması istenen farazi örnek bakımından hem OpenAI şirketini hem de X şirketini müşterek veri sorumlusu olarak kabul etmek gerekir.

4.2. ChatGPT Salt Algoritmik Karara Tabi Olmama Hakkının Kullanımına Uyumlu Hale Getirilebilir Mi?

Salt algoritmik karara tabi olmama hakkının detaylarını yukarıda açıklamıştık. Bu hakkın kullanımı bakımından OpenAI şirketine çeşitli yükümlülükler düşmektedir. Zira ChatGPT genellikle insan müdahalesi olmadan, salt algoritmik karar almakta ve kişilere yönelik bu kararlar hukuki veya önemli olabilecek sonuçlar doğurabilmektedir. Biz alınması gereken önlemlerin özellikle ChatGPT'yi iş modellerinde profesyonel amaçla kullanan şirketler bakımından daha etkili olacağı kanaatindeyiz. Çünkü bu şirketlerin ChatGPT'ye veri aktararak elde ettikleri kararların hukuki veya önemli sonuç doğurma olasılığı yüksektir.

İlk olarak ChatGPT'nin doğrudan kişilere yönelik karar alması istendiği takdirde, ChatGPT tarafından soruyu soran kişiye hatırlatma yapılarak GVKT m.22 kapsamında soruya konu olan öznenin salt algoritmik karara tabi olmama hakkı olduğu uyarısı verilebilir. Bu bilgilendirme kişilere yönelik karar elde etmek isteyen şirketlerin karara konu kişiden onay almaları gerektiği konusunda yönlendirici olacaktır.

İkinci olarak, doğrudan kişilerle ilgili soru sorulduğunda, algoritma bu sorunun hangi amaçla sorulduğunu teyit edecek şekilde geliştirilebilir. Böylece hukuki veya önemli bir sonuç doğuracak nitelikteki amaçlar bakımından soru cevaplanmayabilir ya da ChatGPT'nin kararının bağlayıcı olmaması gerektiği kararda vurgulanabilir.

Son olarak ChatGPT'nin GVKT m.22/f.3'te yer alan insan müdahalesi talep etme, kendi görüşünü açıklama ve itiraz etme hakkı gibi hakları mümkün kılan teknik altyapıyı oluşturması gerekmektedir. Böylece ChatGPT'nin aldığı karar sebebiyle hakkında hukuki veya önemli sonuç doğuran bir kişinin, bu sonucu engelleyecek aksiyonları alması mümkün olacaktır. Ayrıca ChatGPT'nin aldığı kararda hangi kıstasları ve verileri kullandığını açıklama talep etme hakkını kullanan ilgili kişilere açıklayabilecek şeffaflıkta olması da önem arz etmektedir. Aksi halde karara itiraz edebilmek pek de mümkün olmayacaktır. Özetle biz salt algoritmik karara tabi olmama hakkının ChatGPT'nin aldığı kararlar bakımından da uygulanmasının gerekli ve mümkün olduğu kanaatindeyiz.

5. SONUÇ

ChatGPT başta olmak üzere yapay zekâ teknolojileri hayatımızı tahmin ettiğimizden çok daha fazla etkileyebilecek çözümler ve kolaylıklar sunmaktadır. Biz yapay zekanın ticari hayatta ve iş modellerinde de kullanımının artacağından hiç kuşku duymuyoruz.

Zira Bill Gates'in de vurguladığı üzere yapay zekâ en az internet ve cep telefonu kadar önemli bir devrimdir. (Gates, Bill "The Age of AI Has Begun", 2023, s.1 < <https://www.gatesnotes.com/The-Age-of-AI-Has-Begun> > Erişim Tarihi:03.03.2024) Bununla birlikte; ChatGPT ve diğer yapay zekâ uygulamaları kişisel verileri koruma hukuku prensiplerini tamamen görmezden gelerek geliştirilemez. Teknolojideki gelişmeler her ne kadar regülasyondan çok daha hızlı gerçekleşse de temel ilkeler ve esaslar bu gelişim durumunda dahi yeterli korumayı sağlayacak şekilde kişisel verilerimizin korunmasını temin etmektedir. Bu makalenin yazıldığı tarih bakımından ChatGPT'nin kişisel verileri yeterli derecede koruduğunu iddia etmek mümkün gözükmemektedir.

ChatGPT'nin özellikle hukuka uygun veri işleme, sınırlı amaçla veri işleme ve şeffaflık ilkesini önemli ölçüde ihlal ettiği söylenebilir. Bu ihlalin engellenmesi hem yasa koyucuların hem de kişisel veri koruma otoritelerinin alacağı pro-aktif rol ve müdahale ile engellenebilir. Elbette bu müdahale İtalyan Veri Koruma Otoritesi Garante'nin kısa süreli de olsa uyguladığı yasakçı bir bakış açısıyla yapılmamalıdır. Bu ise kişisel verilerin korunmasının ChatGPT'nin gölgesinde yok olmasına seyirci kalmak anlamına da gelmez.

KAYNAKÇA

1. Kanunlar, İkincil Mevzuat ve Rehberler

2016/679 Sayılı Avrupa Genel Veri Koruma Tüzüğü

6698 Sayılı Kişisel Verileri Koruma Kanunu

Article 29 Data Protection Working Party Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679

2. Kitaplar ve Kitap Niteliğinde Tek Yazarlı Kitaplar

CATE Fred H. - DOCKERY Rachel (2019) “Artificial Intelligence and Data Protection: Observation on a Growing Conflict”.

CHALUBINSKA-JENTKIEWICZ, Katarzyna – NOWIKOWSKA, Monika (2022) “Artificial Intelligence v. Personal Data”, Polish Political Science Yearbook

GRAFENSTEIN, Max von (2018) “The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles and Private Standards as Elements for Regulating Innovation”.

HERVE, Alan (2021) “Data Protection and Artificial Intelligence”, The European Union’s Internal Approach and Its Promotion Through Trade Agreements, Cambridge University Press, s.193-214.

JEZOVA, Daniela (2020) “Principle of Privacy by Design and Privacy by Default”, Regional Law Review.

KESA, Aleksandr – KERIKMAE, Tanel (2020) “Artificial Intelligence and the GDPR: Inevitable Nemeses?”, Journal of European Studies.

KONING, Merel Elize (2020) “The Purpose and Limitations of Purpose Limitation”.

MÍTROU, Lilian (2018) “Data Protection, Artificial Intelligence and Cognitive Services: Is General Data Protection Regulation (GDPR) Artificial Intelligence Proof”.

OSMANOVIC, Thunström A. - STEINGRIMSSON, S. (2022) “Can GPT-3 Write an Academic Paper on Itself, with Minimal Human Input?”.

PEHRSSON, Emily (2018) “The Meaning of the GDPR Article 22”, European Union Law Working Papers, Stanford-Vienna Transatlantic Technology Law Forum.

SEİZOV, Ognyan - WULF, Alexander J. (2020) “Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU”, European Law Review.

SPAGNUELO, Dayana – FERREIRA, Ana – LENZINI, Gabriele (2019) “Accomplishing Transparency within the General Data Protection Regulation”, s.114-125.

STIENNON, Nisan - OUYANG Long (2020) “Learning to Summarize from Human Feedback: OpenAI”.

SUN, Fei (2022) “ChatGPT: The Start of the New Era”, A Bright and Gloomy Future.

TOSONI, Luca (2021) “The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation”, Research Paper Series No.2021-07.

YAKIŞIR, Ceren (2023) “An Evaluation of the ChatGPT Decision Which Italy Blocked Access on the Grounds of Violation of the GDPR”.

3. Dergi Makaleleri

AKSOY, Hüseyin Can (2022) “Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme”, Kişisel Verileri Koruma Dergisi, Cilt No: IV, Sayı: 2, s. 69-87.

BIEGA Asia J./ FINCK Michele (2021) “Reviving Purpose Limitation and Data Minimisation in Data Driven Systems” Technology and Regulation.

BINNS Reuben/ VEALE Michael (2021) “Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR”, International Data Privacy Law, Volume: 11 Issue: 4, 319-332.

BOMMARITO Michael/ KATZ Daniel Martin (2022) “GPT Takes the Bar Exam”.

BRAUN AVCI, Cihan (2018) "Kişisel Verilerin İşlenmesinde Rıza", YÜHFD, C.XV, 2018/1 s.13-33.

BRKAN, Maja (2018) “Do Algorithms Rule the World? Algorithmic Decision Making in the Framework of the GDPR and Beyond”, International Journal of Law DOI; 10.1093/ijlit/eay017, s.91-121.

BÜYÜKSAĞIŞ, Erdem (2021) “Yapay Zekâ Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı”, YÜHFD, C. XVIII, 2021/2, S.529-541.

DOWLING, Michael – LUCEY, Brian, (2023) “ChatGPT for (Finance) Research: The Banarama Conjecture”.

FALLETTI, Elena (2020) “Automated Decisions and Article No.22 GDPR of the European Union: An Analysis of the Right to an Explanation”.

FERRETTI, Federico (2014) “Data Protection and the Legitimate Interest of Data Controllers: Much Ado Nothing or the Winter of Rights?”, *Common Market Law Review*, Volume:51, Number:3, s.843-863.

HALLINAN, Dara – BORGESIOUS, Frederik Zuiderveen (2020) “Opinions can be incorrect (in our opinion) On Data Protection Law’s Accuracy Principle”, *International Data Privacy Law*, DOI:10.1093/idpl/ipz025 .

KAMINSKI, Margot (2019) “The Right to Explanation, Explained”, *Berkeley Technology Law Journal*.

KARAKOÇ KESKİN, Elif (2023) “Yapay Zeka Sohbet Robotu ChatGPT ve Türkiye İnternet Gündeminde Oluşturduğu Temalar”, *DergiPark*, s.114-131.

YÜCEDAĞ, Nafiye (2019) “Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler”, *Kişisel Verileri Koruma Dergisi*, Cilt: 1, Sayı: 1, s.47-63.

4. Mahkeme ve Veri Koruma Otoritesi Kararları

“Digi v. Nemzeti”, Case-77/21, 2022.

“G.C. v. Others”, Case-136/17, 2019.

“İlgili Kişi Tarafından Alenileştirilen Kişisel Verinin Alenileştirme Amacı Dışında İşlenmesi” Hakkında Kurul’un 07.11.2019 Tarihli ve 2019/331 Sayılı Karar Özeti.

“Norra Stockholm Bygg v. Per Nycander”, C-268/21, 2023.

“TK v. Asociația de Proprietari bloc M5A-ScaraA”, Case C-708/18.

“Uber Drivers v. Uber B.V.”, C/13/687315, Amsterdam District Court, 2021.

5. Elektronik Kaynaklar

COSTA, Monica Oliveira (2013) “Big Data, Open Data and Purpose Limitation: How Are They Linked?” < <https://www.lexology.com/library/detail.aspx?g=ab2dd08f-3e32-4e31-8447-69b658b86399> > Erişim Tarihi: 03.03.2024.

COUNCIL OF EUROPE: HANDBOOK on European Data Protection Law (2018), < https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf > Erişim Tarihi: 03.03.2024.

DEMİRTAŞ, Ahmet (2023) “OpenAI-ChatGPT: Fikri Mülkiyet ve Veri Koruma Hukukunu Nasıl Sarsıyor?” < <https://solakpartners.com/openai-chatgpt/> >. Erişim Tarihi: 03.03.2024.

GATES, Bill, “The Age of AI Has Begun” (2023) < <https://www.gatesnotes.com/The-Age-of-AI-Has-Begun> > Erişim Tarihi: 01.03.2024.

HERT, Paul de - LAZCOZ Guillerme (2021) “Radical Rewriting of Article 22 of the GDPR on Machine Decisions in the AI Era” < <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/> > Erişim Tarihi: 01.03.2024.

KRAMCSAK, Pablo Trigo (2023) “Can Legitimate Interest be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Dataset?”, Computer Law & Security Review < <https://www.sciencedirect.com/science/article/abs/pii/S026736492200108X?via%3Dihub> > Erişim Tarihi: 01.03.2024

OpenAI’s explanation to train ChatGPT < <https://openai.com/blog/chatgpt> > Erişim Tarihi: 01.03.2024

OpenAI March 20 ChatGPT Outage: Here’s What Happened < <https://openai.com/blog/march-20-chatgpt-outage> > Erişim Tarihi: 01.03.2024

OpenAI Data Controls FAQ < <https://help.openai.com/en/articles/7730893-data-controls-faq> > Erişim Tarihi: 01.03.2024

PURTOVA, Nadezhda (2018) “The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law”, Law, Innovation and Technology 10(1).