SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 25.07.2024
Kabul | Accepted: 03.12.2024
doi 10.15337/suhfd.1522309

YAPAY ZEKA SİSTEMLERİ KULLANILARAK YAPILAN İŞLEME FAALİYETLERİNDE KİŞİSEL VERİLERİN KORUNMASI

Prof. Dr. Emel BADUR*

Öz

Günümüz şartlarında teknolojik gelişmelerin takip edilmesi güç bir hızla gerçekleştiği, dijital ortamın en az yüz yüze ilişkiler kadar günlük hayatın içine girdiği ve bunların sonucunda yapay zeka uygulamalarının hem günlük yaşantı hem de mesleki-ticari faaliyetler çerçevesinde giderek yaygınlaştığı yadsınamaz. Ya-pay zeka sistemleri tarafından toplanan, analiz edilen ve bir takım sonuçlara ulaşılmasını sağlayan -hatta deyim yerindeyse yapay zekayı besleyen- verilerin büyük bir kısmı gerçek kişilere aittir. Yapay zeka alanında yaşanan bu gelişme-ler, kişisel verilerin yapa zeka karşısında korunmasını gerekli kılmaktadır. Kişi-sel verilerin yapay zeka tarafından işlenmesi söz konusu olduğunda, ilgili kişi-nin profillenmesine ve onun hakkında otomatik karar alınmasına özenle yakla-şılması gerekmektedir. KVKK'nın ilgili kişinin haklarının düzenlendiği 11/1/g maddesinde herkesin "İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkına sahip olduğu düzenlenmiştir.

* Prof. Dr. Çankaya Üniversitesi Hukuk Fakültesi, Medeni Hukuk Ana Bilim Dalı, Ankara, Türkiye | Prof, Çankaya University, Faculty of Law, Department of Civil Law, Ankara, Türkiye.
badur@cankaya.edu.tr • ORCID 0000-0002-5133-8541

Atıf Şekli | **Cite As**: **BADUR,** Emel: "Yapay Zeka Sistemleri Kullanılarak Yapılan İşleme Faaliyetlerinde Kişisel Verilerin Korunması",SÜHFD, C. 32, S. 4, 2024, s. 2525-2560.

İntihal | **Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. | This article has been scanned via a plagiarism software and reviewed by at least two referees.

Anahtar Kelimeler

• Kişisel Verilerin Korunması Kanunu • Profilleme • Otomatik karar alma • Algoritmik karar alma • Genel Veri Koruma Tüzüğü

PROTECTION OF PERSONAL DATA DURING PROCESSING BY ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract

Nowadays, it's undeniable that technological developments are taking place at a pace that is difficult to follow, that the digital environment has entered into daily life at least as much as face-to-face relationships, and artificial intelligence applications have become increasingly widespread both in daily life and in professional-commercial activities. Most of the data collected and analysed by artificial intelligence systems, which provides certain results - or even feeds artificial intelligence- belongs to real persons. These developments make it necessary to protect personal data against artificial intelligence. When it comes to the processing of personal data by artificial intelligence, the profiling of the data subject and automated decision-making about him/her needs to be approached with care. Article 11/1/g of the PDPL, stipulates that everyone has the right to "object to the occurrence of a result to the detriment of the person himself/herself by analysing the processed data exclusively through automated systems".

Keywords

• Personal Data Protection Law • Profiling • Aautomated decision making • Algorithmic decision making • General Data Protection Regulation

GİRİŞ

Günümüzde yapay zeka sistemleri ve uygulamaları oldukça gelişmiş ve yapay zeka barındıran sistemler hayatın pek çok alanında insanı doğrudan etkiler hale gelmiştir. Yapay zekanın insan ve toplum yaşamını kolaylaştırıcı etkisi, onun gün geçtikçe hayatımızda daha çok yer kaplaması sonucunu doğururken; bu olumlu etki, yapay zeka kullanılırken kişilerin temel hak ve özgürlüklerinin göz ardı edilmesine sebep olmamalıdır. Konuya bu açıdan yaklaşıldığında yapay zeka sistemleri aracılığıyla yürütülen veri işleme faaliyetlerinde, kişisel verilerin korunmasına özellikle dikkat edilmesi gerektiği sonucu ortaya çıkmaktadır.

Kişiye, kişisel verilerinin korunmasına dair sağlanan hak, en temel haliyle, kişisel verilerin başkaları tarafından bilinir hale gelmesi ve hatta

bu kişilerin kontrolüne geçmesiyle, verilere sahip olan kişinin, kişisel verileri üzerindeki yitirdiği egemenliği tekrar kurmasına yönelik bir hak olarak değerlendirilebilir. Başka bir ifadeyle kişisel verilerin korunması, kişileri haklarındaki verilerin hukuka uygun olmayan şekillerde işlenmesinden kaynaklanan hak ihlallerinden ve zararlardan koruma amacına yönelmiş, temel ve evrensel ilkelerde somutlaşmış yasal, idari ve teknik önlemleri ifade eder.

Hukuk sistemleri, kişisel verilerin korunmasının hayata geçirilmesi kapsamında kişilerin, kendi verilerinin geleceğini bizzat kendilerinin belirlemelerini bir hak olarak kabul etmiştir. Kişisel verilerin korunması, sadece kişiler hakkındaki bilgilerin değil; bu bilgilerin ait olduğu kişilerin ve bu kişilerin haklarının korunmasını da sağlamaktadır. Bu korumanın insan onuru temel olmak üzere diğer birçok temel hakkın ve kişilik hakkının da korunması kapsamında olduğu gerçeği; kişisel verilerin korunmasının, insan haklarıyla olan ilgisini gösterir. Bir başka ifadeyle kişisel verilerin korunmasını hedefleyen hukuk sistemleri, aslında bizatihi ve soyut bir kavram olarak bilginin değil; bilginin ilişkili olduğu kişinin korunmasını amaçlamaktadırlar.

I. KİŞİSEL VERİ, İŞLEME VE VERİ SORUMLUSU KAVRAMLARI

Türk Hukukunda doğrudan kişisel veri kavramını konu alan ilk normatif düzenleme, 108 sayılı Sözleşme'nin imzalanması ile kabul edilmiştir. Türkiye Cumhuriyeti, Avrupa Konseyi tarafından hazırlanan 108 sayılı *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesi'ni"*, 28.01.1981 tarihinde imzalayarak; yürürlük sürecini 30.01.2016 tarihinde, 6669 sayılı Kanun'un kabul edilmesi ile sağlamıştır.[1]

Kişisel verilerin korunmasına ilişkin hak, 2010 yılında yapılan Anayasa değişikliğiyle *"Özel hayatın gizliliği"* kenar başlığı altında düzenlenen 20. maddeye eklenen üçüncü fıkra güvence altına alınmıştır. Kişisel verilerin korunmasına dair 2016 yılında gerçekleştirilen yasama faaliyetiyle, 6698 sayılı Kişisel Verilerin Korunması Kanunu[2] (KVKK) mevzuata dahil

---

1 Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesi (108 sayılı Sözleşme), 29656 sayılı ve 17 Mart 2016 tarihli Resmi Gazete.

2 Kişisel Verilerin Korunması Kanunu, 29677 sayılı ve 7 Nisan 2016 tarihli Resmi Gazete.

edilmiştir. Ancak KVKK'nın yürürlüğe girmesinden önce de hukuk sistemimizde kişisel verilerin korunmasına dair bazı düzenlemeler yapılmıştır. Türk Ceza Kanunu'nun (TCK) 135 ila 140. maddeleri arasında kişisel verilerin hukuka aykırı olarak ele geçirilmesi, kaydedilmesi, verilmesi ve mevzuatta düzenlenen süre içinde yok edilmemesine dair suçlar kaleme alınmıştır.

A. Kişisel Veri Kavramı

Kişisel Verilerin Korunması Kanunu'nun (KVKK) *"Tanımlar"* başlıklı 3/1/d maddesinde kişisel veri *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"* kapsayacak genişlikte tanımlanmıştır. Maddenin gerekçesinde[3] kişisel veri kavramı, *"Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir."* ifadesiyle açıklığa kavuşturulmuştur.

Kişisel verinin bir diğer tanımına da 108 sayılı Sözleşme'nin 2/a maddesinden ulaşılması mümkündür. Anılan maddede *"Kimliği belirli veya belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgi"* kişisel veri olarak tanımlanmıştır. Yapılan açıklamalardan da açıkça anlaşılacağı üzere kişisel veriler, mevzuatımızda sınırlı sayma ilkesi benimsenerek düzenlenmemiş ve örnek olarak sayılması yolu da tercih olunmamıştır.[4]

---

[3] https://kvkk.gov.tr/SharedFolderServer/CMSFiles/062384e3-d18c-4c38-b108-3a7a2a28e849.pdf (E. T. 28.04.2024)

[4] Bununla birlikte özel nitelikli kişisel veriler hakkında Kanunun 6/1. maddesinde yer verilen *"kişilerin 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"* ifadesiyle, bazı özel nitelikli kişisel veriler sınırlı sayıda düzenlenirken; kişisel veri örnekleri de yasa metnine dahil edilmiştir.

Bunun nedeni, kişisel verilerin niteliğinin, sayısının ve değişkenliğinin saymayla belirlenmeye uygun olmamasıdır. Benzer bir tercih, kişilik değerlerinin de özel olarak sayılmamasının nedenini oluşturur. Bu sayede gerek kişilik değerlerinin gerekse kişisel verilerin yaşamın dinamik yapısına uygun olarak belirlenebilmesi mümkün kılınır. Özellikle bilişim teknolojilerinde yaşanan gelişmelerin, her an korunması gereken yeni kişisel verilerin ortaya çıkmasına sebep olması, şaşırtıcı olmayacaktır.

Kişinin toplumdaki diğer fertlerden ayrılmasını sağlayan her türlü bilgi, yapılan kişisel veri tanımının kapsamı içerisine dahil edilmiştir. Kişinin mesleki yaşamında üstlendiği bir unvan, akademik veya sanat eserlerine yapılan yorum ve atıflar, geliri, ödediği vergi, borç ve/veya alacakları, sahip olduğu ödül ya da aldığı derece de kişiye ulaşmada kullanılabilecek ve gerçek kişiyi belirlenebilir kılmakta zorlanmayı gerektirmeyecek veriler arasındadır.[5]

Yasa koyucu kişisel veri teriminin tanımını yaparken yasama tercihini kapsayıcı olmaktan yana kullanmış ve bu amaçla yalnızca *"belirli"* değil; *"belirlenebilir kişilere"* dair kişisel verileri de tanımın kapsamına alma yolunu seçmiştir. Belirli veya belirlenebilir kişilere ait bilgilerin kişisel veri olarak kabulü, bu bilgilerin doğru veya yanlış; gizli ya da açık hatta güncel olmalarına bağlı değildir. Bu bilgiler kişinin parmak izi, DNA dizilimi, iris taraması veya kan grubu gibi nesnel, değişmez ve bilimsel olabileceği gibi; kişinin güvenilir veya borcuna sadık olup olmadığı, itaatkarlığı ya da isyankarlığı, işe yatkınlığı ve çalışma hevesi gibi öznel, değişken ve yoruma açık bilgiler de olabilir.[6]

---

5 **BADUR, Emel:** Çocuğun Kişisel Verilerinin Korunması -KVKK, GVKT ve AİHM Kararları Çerçevesinde Bir İnceleme-, Seçkin Yayınevi, Ankara 2023, s. 70; **HİZARCI, Emine:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun AB Veri Koruma Hukuku Işığında Değerlendirilmesi, Yetkin Yayınları, Ankara 2020, s. 26; **KELLEHER, Denis/ MURRAY, Karen:** EU Data Protection Law, Bloomsbury, London 2019, s. 82, 83.

6 **AKSOY, Hüseyin Can:** Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2016, s. 14; **AŞIKOĞLU, Şehriban İpek:** Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayınları, İstanbul 2018, s. 9; **DÜLGER, Murat Volkan:** Kişisel Verilerin Korunması Hukuku, 3. Baskı, Hukuk Akademisi, İstanbul 2020, s. 24; **TAŞTAN, Furkan Güven:** Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, On İki Levha Yayınları, İstanbul 2017, s. 38; **ÖZKAN, Oğulcan:** Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara 2020, s. 10; **BADUR**, s. 71.

Bir bilginin kişisel veri olarak nitelenmesi için, belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilebilmesi yeterlidir. Bu bilginin elde edilme, üretilme, kaydedilme, saklanma ve aktarılma biçimleri, kişisel veri olarak kabul edilmesi[7] açından önem taşımaz. Başka bir ifadeyle kişisel verinin yazılı olması, dijital ortamda saklanması, fotoğraf, resim, ses veya hareketli görüntüye ilişkin olması, o verinin kişisel veri niteliğini etkilemeyecektir.[8] Bir görüntünün kişisel veri olarak nitelendirilmesi için, ilgili gerçek kişinin görüntüsü olması da şart değildir. Örneğin bir kişinin çizdiği resim de onun kişisel verisi olarak nitelenebilir.

Kişisel veriler kişinin ekonomik, fiziksel, kültürel, psikolojik veya sosyal özelliklerini betimleyen bilgiler taşımasının yanı sıra vergi, sigorta ya da kimlik numaraları gibi diğer verilerle bağlantı kurulması suretiyle kişiye ulaşılması sonucunu doğuran durumları da içerir. En yaygın kişisel veri örnekleri kişinin adı, sesi, resmi, görüntüsü, kimlik/vergi/sosyal güvenlik/pasaport/iş yeri sicil ve telefon numaraları, adresi, motorlu taşıt plakası, parmak izi, genetik bilgileri, özgeçmişi, yayın ve eser listeleridir. Zira örneklendirilen tüm bu bilgiler, gerek doğrudan gerek dolaylı olarak veri sahibini belirlenebilir kılmaktadır.

Kişisel veri kavramı yakın tarihli bir Anayasa Mahkemesi kararında[9] da *"Kişinin sadece kimliğini ortaya koyan ad, soyad, doğum tarihi ve doğum yeri gibi bilgilerinden değil aynı zamanda telefon numarası, pasaport numarası, motorlu taşıt plakası, sosyal güvenlik numarası, öz geçmiş, görüntü ve ses kayıtları, resim, parmak izleri genetik bilgiler ile sağlık bilgileri, e-posta adresi, Internet Protokol (IP) adresi, alışkanlıklar, hobiler, grup üyelikleri, aile bilgileri gibi kişiyi belirlenebilir kılan bütün verilerden oluşmaktadır."* ifadesiyle açıklanmıştır.

B. Kişisel Verilerin Türleri

Kişisel Verilerin Korunması Kanunu'nun kaleme alınış şekli kişisel verilerin ilk bakışta türlere ayrılmadığı fikrini uyandırmaya elverişli olsa

---

7 Bu noktada açıklığa kavuşturulması gereken bir diğer husus, tüm kişisel verilerin KVKK kapsamında korunduğunu söylemenin mümkün olmadığına ilişkindir. Zira KVKK'nın 28. maddesinde Kanunun uygulanmayacağı bazı istisnalara yer verildiği gibi; ancak Kanunun işleme tanımı içinde kalan faaliyetlere tabi tutulan kişisel verilere koruma sağlanmıştır.

8 **AKSOY**, KVK, s. 15.

9 AYM, K. 2014/1970, T. 22.11.2017.

da; Kanunda hukuka uygun işlemeye dair benimsenen düzenlemeler kişisel verilerin genel ve özel nitelikli olacak şekilde ikili bir ayrıma tabi tutulduğunu göstermektedir. Zira yasa koyucu her iki veri grubu açısından sırasıyla Kanunun 5 ve 6. maddelerinde hukuka uygun işleme sebeplerini ayrı ayrı düzenlemiştir.

Yasa koyucu Kanunun 6. maddesinde *"özel nitelikli kişisel veriler"* ifadesini kullanmak ve maddenin ilk fıkrasında bu verileri sınırlı sayıda olmak üzere saymakla birlikte; bu tür verilerin haricinde kalan verileri bir tür olarak isimlendirmeyi tercih etmemiştir. Ancak kişisel veri türleri arasında bir karışıklığa yer vermemek amacıyla, özel nitelikli (hassas) kişisel veriler dışında kalanların, *"genel nitelikli kişisel veri"* olarak adlandırılmasının uygun olacağı kanaati hasıl olmuştur.

Özel nitelikli kişisel verilerin aksine, genel nitelikli kişisel veri belirlemesi yasa koyucu tarafından yapılmamıştır. Başka bir ifadeyle Kanun'da genel nitelikli (veya adi) kişisel veri ifadesine yer verilmemiştir. Bununla birlikte özel nitelikli kişisel verilerin dışında kalan yani özel nitelikli kişisel veri olmayan tüm kişisel verileri isimlendirmek için genel nitelikli kişisel veri teriminin kullanılması tercih olunmuştur.

Özel ve genel nitelikli veriler arasındaki en ciddi farklılıklardan ilki özel nitelikli verilerin sınırlı sayma (numerus clausus veya tahdidi) usulüne tabi düzenlenmesine karşın; genel nitelikli veriler hakkında bu ilkenin benimsenmiş olmamasıdır. Böylece bilişim teknolojilerinin gelişmesi ve yapay zekanın da kişisel veri işlemesinin yaygınlaşması sonucunda gerçek kişileri belirlenebilir kılan veya ilgili kişiye ilişkin olan tüm yeni verilerin; aksine bir düzenleme yapılıp özel nitelikli olarak kabul edilmediği sürece bu kapsamda olacağının söylenmesi mümkündür.

Özel ve genel nitelikli veriler arasındaki bir diğer önemli farklılık ise genel nitelikli verilerin bir kısmının aleni veya dışardan kolayca gözlemlenebilir bilgiler olmasına karşılık özel nitelikli verilerin kişinin mahrem alanlarına girmesinin daha yaygın olmasıdır. Bu nedenle özel nitelikli kişisel veriler, hassas kişisel veriler olarak da adlandırılmaktadır. Bu verilerin hukuka aykırı şekilde elde edilmesi ve işlenmesi, ilgili kişinin ayrımcılığa maruz kalma riskini de arttırmaktadır.

Örneğin kişinin ismi, kimlik/pasaport numarası ve diğer nüfus kayıt bilgileri (medeni hali, doğum yeri, nüfusa kayıtlı olduğu yer vb.), sesi, görüntüsü, bedensel özellikleri (boy, kilo, benleri veya dövme vb.) telefon

numarası, mali/finansal bilgileri (IBAN/ banka hesap/kredi kartı numaraları), internet protokolü (IP) adresi, şifreleri, adresleri genel nitelikli kişisel veriler olarak örneklendirilebilir.

Kanunun 6/1. maddesinde özel nitelikli kişisel veriler *"Kişilerin 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 özel nitelikli kişisel veridir."* ifadesiyle sayılmışlardır.[10] 108 sayılı Sözleşme'nin 6. maddesinde de *"ırksal kökene, siyasi görüşlere, dini veya diğer inançlara, sağlığa, cinsel yaşama ve mahkumiyetlere ilişkin veriler"* özel nitelikli veri kapsamında düzenlenmişlerdir.

Yapay zeka kullanılarak gerçekleştirilen bir işleme faaliyetin yürütülmesi nedeniyle ilgili kişinin isim, ikametgah, banka hesap numarası ve ekonomik durumu gibi genel nitelikli kişisel verilerinin işlenmesinin yanı sıra özel nitelikli kişisel verilerinin de işlenmesi mümkündür. Özellikle yüz, iris, parmak izi veya el ayası tanıma ve eşleştirme sistemlerinin kullanılması, sağlık alanında yapay zekanın teşhiste bulunması gibi hallerde kişilerin hem biyometrik hem de sağlık verileri işlenmektedir.

C. İşleme Kavramı

Kişisel Verilerin Korunması Kanunu kapsamında, kişisel verilere uygulanabilecek her işlem değil; sadece yasa koyucu tarafından tanımlanan *"işleme"* faaliyeti kapsamındaki fiiller yasal korumanın çatısı altına alınmıştır. Bu durum KVKK'nın *"Kapsam"* başlıklı 2. maddesinde yer verilen *"...tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen ..."* ifadesiyle

---

[10] Özel nitelikli kişisel verilerin tanımları hakkında bkz. **BADUR**, s. 84; **BULUT, Metin:** "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", Ankara Barosu Dergisi, S. 3, Ankara 2020, s. 111; **ÖZER DENİZ, Miray:** Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, On İki Levha Yayınları, İstanbul 2022, s. 38 vd. Maddede benimsenen sınırlı saymaya kişilerin finansal (mali) verileriyle konum (yer) verilerinin dahil edilmemiş olması eleştirilmektedir. s. 134; **AKSOY**, KVK, s. 32; **BAŞAR, Cemal:** Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul 2020, s. 97. Konum verileri hakkında ayrıntılı bilgi için bkz. **TEKİNOĞLU, Dilara:** Kişisel Verilerin Korunması Hukuku Açısından Mobil Uygulamalarda Konum Gizliliği, On İki Levha Yayıncılık, İstanbul 2021, s. 12 vd.; Guide to the Case-Law of the of the European Court of Human Rights, s. 16 vd. https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, (E. T. 02.02.2024).

vurgulanmıştır. Başka bir ifadeyle kişisel veriye uygulanan fiilin (elde etme, kaydetme veya yayma vb.) tamamen veya kısmen otomatik olmadığı bir durumda, uygulanan fiil bir veri kayıt sisteminin de parçası değilse, Kanun kapsamında değerlendirilmesi mümkün değildir. Ancak bu noktada TCK'da düzenlenen suç tiplerinin hala uygulanabilir olduğu göz ardı edilmemelidir.

KVKK'nın 3/e maddesinde kişisel verilerin işlenmesi, *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifadesiyle ve kişisel verilere uygulanabilecek pek çok fiili kapsayacak genişlikte kullanılmıştır.

Özellikle işleme faaliyetinin kapsamına ilişkin bazı fiiller tanımda sayıldıktan sonra yer verilen *"gibi"* ifadesi yasa koyucunun amacının, işlemeye ilişkin fiilleri sınırlı sayıda saymayı amaçlamadığını göstermeye yeterlidir. Maddenin kaleme alınış şekli, kişisel verilerin işlenmesi sırasında uygulanabilecek fiillerin örneklendirilmesi amacının benimsendiği sonucuna ulaşmaya elverişlidir. Bir diğer ifadeyle kişisel verilerin işlenmesi, bu verilerin elde edilmesinden başlanılarak, veriler üzerinde uygulanan tüm işlemleri ifade eder.[11]

Bu noktada gözden kaçırılmaması gereken nokta, işleme kapsamındaki fiillerin *"tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt*

---

[11] Öğretide de kişisel verilerin işlenmesinin, bu verilerin ele geçirilmesi, kaydedilmesi, sınıflandırılması, aktarılması ve imha edilmesi gibi süreçler içerisinde veriler hakkında gerçekleştirilen her türlü işlemi kapsayacak şekilde tanımlandığı ifade edilebilir. **KELLEHER/ MURRAY**, s. 95; **BADUR**, s. 88; **MACMILLAN, Mac (Edt. USTARAN, Eduardo):** "Data Protection Concepts", European Data Protection Law and Practice, 3. Baskı, IAPP Publication, 2023, s. 103; **WELFARE, Damien/ CAREY, Peter (Edt. CAREY, Peter):** "Territorial Scope and Terminology", Data Protection A practical Guide to UK and EU Law, 5. Baskı, Oxford 2018, s. 15; **KUNER, Christopher:** European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, 2. Baskı, Oxford 2007, s. 75; **ÇEKİN, Mesut Serdar:** Kişisel Verilerin Korunması Hukuku, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2019, s. 46; **ÖZDEMİR, Hayrunnisa:** Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayınevi, Ankara 2009, s. 135.

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla" gerçekleştirilmesi şartıdır. Yasa koyucu, otomatik işleme kavramını tanımlama yolunu tercih etmemiştir. Buna karşılık otomatik işlemenin tanımına 108 sayılı Sözleşme'nin 2/c maddesinde yer verilmiştir. Anılan hükümde otomatik işleme *"tamamen veya kısmen otomatik yöntemlerce gerçekleştirilen; verilerin kaydı ve bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması"* ifadesiyle tanımlanır.

D. Veri Sorumlusu

Kişisel verilerin işlenmesinde kararları alan ve bunun karşılığında veri işleme faaliyetinin hukuki sorumluluğunu üzerinde taşıyan kişi yasa koyucu tarafından *"veri sorumlusu"* olarak isimlendirilmiştir. Veri sorumlusu kavramı KVKK'nın 3/ı maddesinde *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmıştır. Kimlerin kişisel verilerinin işleneceğine dair kararı verme yetkisi de veri sorumlusundadır.

Veri sorumlusu, hem hangi kişisel verilerin işleneceğine; hem de bu verilerin işlenme yöntem ve amaçlarına, saklanma sürelerine ve imha politikalarına dair kararları alan kişidir.[12] Kişisel verilerin hangi hukuka uygunluk sebeplerine dayalı olarak işleneceğine dair belirlemeleri yapma yetkisi veri sorumlusunundur. Zorunlu bir unsur olmamakla birlikte, veri işleme faaliyetinden bir menfaat elde ediliyorsa; elde eden kişi veri sorumlusudur.

Konuya yapay zeka sistemleri aracılığıyla kişisel verilerin işlenmesi açısından yaklaşıldığında, veri sorumlusunun başta KVKK olmak üzere mevzuatta yer alan tüm yükümlülüklerin muhatabı, kişisel verilerin işlenmesine ilişkin bütün ilke ve kuralların uygulayıcısı; ayrıca kişisel verilerin işlenmesi nedeniyle doğan zararların da sorumlusu olduğunun söylenmesi mümkündür. Başka bir ifadeyle yapay zeka sistemleri aracılığıyla işlenen kişisel verilerin işlenmesi halinde, yapay zekaya ilişkin sistemin geliştiricisi ve/veya sahibinin veri sorumlusu olduğu söylenebilir.

---

12 **PEKMEZ, Cüneyt:** "Overview of the Definitions of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, S. 67, İstanbul 2019, s. 61; **BADUR**, s. 104; **MACMILLAN**, s. 90; **WELFARE/ CAREY**, s. 18.

Bunlara ek olarak veri sorumlusu, kişisel verilerin korunmasına yönelik düzenlemelere uyum sağlanması için gerekli önlemlerin alınmasından, eğer bir veri işleyenle çalışılıyorsa bu kişinin denetimden ve ilgili kişilerin haklarının etkin bir şekilde kullandırılmasından sorumludur. Yasa koyucu tarafından yapılan tanımdan da anlaşılacağı üzere, veri sorumlusunun kamu hukuku veya özel hukuk tüzel kişisi[13] ya da gerçek kişi olması mümkündür. Veri sorumlusu, kişisel verilerin işlenmesi açısından özerk ve bağımsız bir kişidir. Kurulun ifadesiyle[14] veri sorumlusu, *"kimseden emir ve talimat almayan, bilakis bir başka kişiye veri işletmesi halinde bu hususta emir ve talimat veren, veri işleme süreçlerinin her anında serbestçe karar verme yetkisine sahip olan"* gerçek veya tüzel kişilerdir.

II. YAPAY ZEKA SİSTEMLERİ KULLANILARAK YAPILAN İŞLEME FAALİYETLERİ

Yapay zeka sistemleri barındıran uygulamaların, gerek gündelik hayatta gerçekleştirilen rutin faaliyetlerde (internetten market alışverişi yapmak, evde yokken robot süpürgeyi, fırını veya klimayı kontrol etmek vb.); gerekse iş yaşamında en basitinden daha karmaşığına (bir yerden başka bir yere gitmek için navigasyondan faydalanmak, müşteri veya öğrencileri çeşitli kriterlere göre notlandırmak vb.) kadar pek çok işin organize edilmesi ve gerçekleştirilmesi sırasında kullanıldığını görmek mümkündür.

Özellikle telefonlarda, bilgisayar ve tabletlerde, son dönem arabalarda, akıllı ev/ofis/yapı sistemlerinde ve nesnelerin interneti barındıran eşyalarda yapay zeka sistemleri kullanılmaktadır. Yapay zeka sistemlerinin kullanılması, sadece ürünleri (malları) değil; müşterilere sunulan hizmetleri de dönüştürmektedir. Örneğin kredi veya yatırım portföylerinin uygunluğunun belirlenmesinden, sosyal medyada karşımıza çıkacak içeriklerin sıralanmasına, kişiye özel okuma/izleme tavsiyelerinde bulunulmasına kadar pek çok alanda yapay zeka sistemleri kullanılmaya başlanmıştır.[15] Yukarıda verilen örnekler, yapay zeka sistemleri kullanılarak

---

[13] Tüzel kişi veri sorumluları açısından dikkat edilmesi gereken husus, veri sorumlusunun tüzel kişiliğin içinde kişisel verilerin işlenmesinden sorumlu olan gerçek kişi (çalışan, yönetici vb.) veya organın değil; bizzat tüzel kişiliğin kendisinin olmasıdır.

[14] KVKK, K. 2020/71, T. 30.01.2020. https://www.kvkk.gov.tr/Icerik/6874/2020-71. (E. T. 10.04.2024)

[15] **DÜLGER, Murat Volkan:** "Algoritmik Karar Verme ve Veri Koruması", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792207, s. 4. (E. T. 08.11.2024)

sürdürülen faaliyetlerin sadece çok sınırlı bir kısmını kapsayacak niteliktedir.[16] Bununla birlikte, makalenin konu sınırlaması açısından verilen örneklerin yapay zekanın kullanılma alanlarına değil; kişisel veriler üzerindeki işleme faaliyetlerine ve bunların sonuçlarına özgülenmesi gerekli görülmektedir.

KVKK'da da GVKT'de de yapay zekaya ve yapay zeka sistemleri kullanılarak gerçekleştirilen işleme faaliyetlerine ilişkin özel bir hükme yer verilmemiştir. Buna karşılık KVKK'nın 11/1/g maddesinde *"İlgili kişinin hakları"* kenar başlığı altında, herkesin *"İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme"* hakkına sahip olduğu düzenlenmiştir. Başka bir ifadeyle yasa koyucu, profilleme ve otomatik karar alma terimlerini tanımlamadan ve hatta bu terimleri kullanmadan, ilgili kişinin bu konuda bir itiraz hakkı olduğunu düzenlemekle yetinmiştir.[17] Yasa koyucu tarafından KVKK'nın 11/1/g maddesinde kullanılan ifadeyle ilgili kişiye itiraz hakkı tanınan işleme faaliyetinin iki önemli unsurunun *"profilleme"* ve *"otomatik karar almaya tabi tutulma"* olmak üzere ele alınması mümkündür.

Öğretide[18] haklı olarak, temel hakları ihlal etme potansiyeli barındıran ve ilgili kişi açısından ciddi sonuçlara yol açabilecek nitelikteki bir işleme faaliyeti olan otomatik kararlara ve profillemeye, işlem sonrasında itiraz etme hakkı tanınmasının, KVKK'nın 1. maddesinde belirtilen amaca

---

16 Konu hakkında ayrıntılı bilgi için bkz. **AKSOY, Ecem:** Yapay Zeka'nın Sorumluluk Hukukundaki Konumu ve Büyük Veri ile İlişkisi, Seçkin Yayınevi, Ankara 2022, s. 62 vd.

17 Kurul tarafından hazırlanan sözlükte profilleme tanımlanırken, "Kişisel verilerin münhasıran otomatik sistemler vasıtasıyla işlemek suretiyle, ilgili kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi şeklindeki kişisel veri işleme biçimi." şeklinde açıklama yapılmıştır. Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, s. 117. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu, (E. T. 04.05.2024)

18 **BÜYÜKSAĞİŞ, Erdem:** "Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı", YÜHFD, C. XVIII, S. 2, İstanbul 2021, s. 535.

uygun olmadığı ileri sürülmüştür. Zira hakkında salt algoritmalar[19] vasıtasıyla bir karara varılan ilgili kişi, çoğu zaman kararın neden ve hangi ölçütler göz önüne alınarak verildiğini dahi bilmeyeceğinden, itiraz hakkını kullanamayacaktır.[20]

A. Profilleme

Profilleme (veya profil çıkarma) terimi, GVKT'nin aksine KVKK'da tanımlanması tercih olunmamış bir terimdir. Profilleme ilgili kişinin bir takım davranış ve hareket özelliklerine dair verilerin (işteki başarı, sınav notları, ekonomik durum, sağlık, alış veriş tercihleri, ilgi alanları, kredibilitesi, sıklıkla bulunduğu konumlar vb.) analiz veya tahmin edilmesiyle ulaşılan çıkarımlara dair her türlü otomatik karar alma suretiyle gerçekleştirilen kişisel veri işleme faaliyetidir.[21] Günümüzde yapay zeka sistemleri kullanılarak gerçekleştirilen profilleme faaliyetlerinin özellikle sağlık, bankacılık, sigortacılık ve reklamcılık sektörlerince kullanıldığı söylenebilir.[22]

Her profilleme faaliyeti, otomatik bir veri işleme sürecini gerektirir ve ilgili kişinin kişisel özelliklerinin değerlendirilmesi amacını taşır.[23] İlgili kişinin profili belirlendikten sonra, bu belirleme kişi hakkında ileride

---

19 Algoritmanın tanımı ve yapay zekanın bileşenlerinden biri olması hakkında ayrıntılı bilgi için bkz. **AKSOY**, Yapay Zeka, s. 64.

20 Yapay zeka sistemlerinin, mahremiyet ve özel hayat üzerindeki etkileri konusunda ayrıntılı bilgi için bkz. **DÜLGER, Murat Volkan:** "Yapay Zekalı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli?", Terazi Hukuk Dergisi, C. 13, S. 142, Ankara 2018, s. 84.

21 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, s. 6, https://ec.europa.eu/newsroom/article29/items/612053/en, (E. T. 10.04.2024)

22 **DÜLGER,** Algoritmik, s. 6.

23 Konu hakkında bkz. **AKSOY, Hüseyin Can:** "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", Kişisel Verileri Koruma Dergisi, C. 4, S. 2, Ankara 2022, s. 69-87; **ERDOĞAN, Irmak:** Yapay Zeka ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri, Seçkin Yayıncılık, Ankara 2022, s. 77 vd.; **KELLEHER/ MURRAY**, s. 103; **KAYA, İslam Safa/ TOLUN, Yüksel:** Türkiye'de ve Avrupa'da Kişisel Verilerin İşlenmesi, Adalet Yayınevi, Ankara 2020, s. 53, 125; **ÖZGÜL, Nurullah:** "İnsan Haklarının Korunması ve Geliştirilmesinde Yeni Bir Sorun Alanı: Algoritmik Profilleme", Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi, C. 5, S. 9, s. 83-115; **CAYGIN, Fatmanur/ YAVUZ, Can:** "Yapay Zeka ve Çocuk Haklarına Kısa Bir Bakış", İBD, C. 94, S. 3, İstanbul 2020, s. 218-229; **BADUR**, s. 98; **KELLEHER/ MURRAY**, s. 224.

verilecek otomatik kararların temelini oluşturabilir. Profillemenin arama motorlarının ve sosyal medya sitelerinin çalışma modellerinin ayrılmaz bir parçası olduğu da belirtilmektedir.[24]

Üstelik ilgili kişi hakkında yapılan profilleme sonucunda, yapay zeka sistemi tarafından kişi hakkında yeni bir kişisel veri üretilmektedir. İlgili kişi hakkındaki verilerin gerçeği yansıtıp yansıtmaması veya objektif olması ya da sübjektif bir değerlendirmenin sonucunu taşıması, kişisel veri nitelemesi açısından önem taşımadığından; profilleme sonucunda ulaşılan *"kredi puanı veya sigorta riski yüksek/düşük; çalışkan/tembel ya da başarılı/başarısız"* gibi sonuçlar da o kişi hakkındaki kişisel veriler olarak nitelenmeye uygundur.

Profilleme GVKT'nin 4/4. maddesinde, *"bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını içeren her türlü otomatik kişisel veri işleme"* biçimine karşılık gelecek şekilde tanımlanmıştır.

Üye devletler açısından doğrudan bir bağlayıcılığı bulunmamakla birlikte Avrupa Konseyi Bakanlar Komitesi, 23.11.2010 tarihinde, CM/Rec (2010)13 sayılı ve *"Profilleme Uygulamaları Kapsamında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Üye Devletlere Yönelik Tavsiye Kararı"*[25] başlıklı bir metin hazırlamıştır.[26] Türkiye Cumhuriyeti de üye devletlerden ve 108 sayılı Sözleşmenin taraflarından biri olması nedeniyle söz konusu Tavsiye Kararının muhatabıdır.

---

[24] **BADUR**, s. 99; **KELLEHER/ MURRAY**, s. 226; **KUNER, Christopher/ BYGRAVE, Lee A./ DOCKSEY, Christopher:** The EU General Data Protection Regulation: A Commentary, Oxford University Press, Oxford 2021, s. 97; **PETKOVA, Bilyana/ BOEHM, Franziska (Edt. SELINGER, Evan/ POLONETSKY, Jules/ TENE, Omer):** "Profiling and the Essence of the Right to Data Protection", The Cambridge Handbook of Consumer Privacy, Cambridge University Press, Cambridge 2018, s. 291; **WELFARE/ CAREY**, s. 23.

[25] https://rm.coe.int/16807096c3 (E. T. 14.04.2024)

[26] Resmi olmayan Türkçe çeviri metni için bkz. https://rm.coe.int/profilleme-uygulamalar-kapsam-nda-kisisel-verilerin-otomatik-isleme/1680a4396d (E. T. 14.04.2024)

Anılan kararda *"Profil"* bir kişinin sınıflandırılmasını (kategorisini karakterize eden) sağlayan ve bu kişiye uygulanması amaçlanan veri dizisi; *"Profilleme"* ise özellikle kişiyle ilgili kararlar alınması ya da söz konusu kişinin kişisel tercihlerini, davranışlarını ve tutumlarını analiz veya tahmin etmek amacıyla bir profilin bir kişiye uygulanmasını içeren otomatik veri işleme (karar alma) tekniği olarak tanımlanmıştır.

Tavsiye kararının giriş kısmında, profilleme uygulamalarının, şeffaflıktan yoksun, hatta *"görünmez"* olmasının ve önceden belirlenmiş varsayımsal kuralların otomatik bir şekilde uygulanmasının sebebiyet verebileceği yanlışlıkların hak ve özgürlüklere yönelik önemli riskler yaratabileceğinin göz önünde bulundurulduğuna dikkat çekmiştir. Profillemenin -meşru şekillerde yapılsa bile- uyarı ve özel koruma tedbirleri olmadan kullanılmasının, insan onuruna, ekonomik ve sosyal haklar da dahil olmak üzere diğer temel hak ve özgürlüklere ciddi biçimde zarar verebileceği hususu, üye devletlere hatırlatılmıştır.

Tavsiye Metninin 3/A/3.5. maddesinde kendi adlarına özgür, spesifik ve bilgilendirilmiş şekilde rıza veremeyen herkesi kapsayacak bir ifadeyle, bu durumdaki kişilere yönelik profilleme uygulamaları kapsamında kişisel verilerin toplanması veya işlenmesinin, söz konusu işlemin ilgili kişinin meşru menfaatine olduğu veya üstün bir kamu yararının bulunduğu haller dışında yasaklanması gerektiği açıkça belirtilmiştir. İlgili kişinin meşru menfaatinin olduğu veya üstün bir kamu yararının bulunduğu hallerde gerçekleştirilecek profillemeler için de kanunla uygun güvenceler getirilmelidir.

Profillemeye ilişkin işleme faaliyetlerinden önemli bir kısmı, kişilerin girdiği internet sitelerine yerleştirilen çerezler (cookies) aracılığıyla yapılmaktadır. İnternet sitelerine yapılan her ziyarette kişiler, ziyaret ettiği sitelerde izler bırakmaktadır. Rakam ve harflerden oluşan bu izler (çerezler) takip edilerek kişinin profili çıkarılmakta ve profillenen özellikleri doğrultusunda ilgili kişiye mal ve hizmet sağlayıcıları tarafından öneriler ve reklamlar yapılmaktadır.[27] Çerez kullanan siteler, hem ilgili kişiye bu

---

[27] Çerezler ve KVKK'ya uygun kullanılmaları hakkında ayrıntılı bilgi için bkz. **AYÖZGER ÖNGÜN, A. Çiğdem:** Kişisel Verilerin Korunması, 2. Baskı, Beta Yayınları, İstanbul 2016, s. 244; **KESER, Yıldırım:** "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza", SÜHFD, C. 28, S. 3, Konya 2020, s. 1196; **AKSOY, Hüseyin Can/ HALICIOĞLU, Mesut:** "AB ve Türk Hukuklarında Çerezler, Kişisel", Kişisel Verileri Koruma Dergisi, C. 3, S. 1, Ankara 2021, s. 61-88; **IŞIK, Alper:** "Fransız Veri Koruma

davranışlarına dair aydınlatma yapmakta hem de her siteye girişte çerez kullanımı için rıza istenmektedir. Üstelik çoğu zaman ilgili kişiye çerezleri kabul etmeden internet sayfasının tamamını görüntüleyebilme veya sitede ziyaretini sürdürebilme imkanı da tanınmamaktadır.

Çerez kullanımına ilişkin yukarıda açıklanan şekilde alınan rızaların (yapılan aydınlatmanın, metinlerini okudum/anladım şeklinde kutucukların tıklanmasıyla sayfada ilerlenebilmesinin) KVKK kapsamında geçerli olduğu söylenemez. Buna rağmen sadece çerezlerden yola çıkarak kişinin doğrudan belirlenebilmesinin mümkün olmaması nedeniyle, kişisel verilerin kullanılması anlamında rızanın alınmasının gerekli olmadığı; aksi halde gereksiz rıza yorgunluğuna sebebiyet verilebileceği de ileri sürülen görüşlerdendir.[28]

Buna karşılık Keser'in[29] de haklı olarak belirttiği üzere, çerezleri yerleştiren veri sorumlusunun ek bazı verileri kullanarak, kişilerin kimliğini belirleyebilmesi durumunda, çerezlerin ve bunlardan yola çıkılarak gerçekleştirilen profillemenin kişisel verilerin korunması hukukunun alanına gireceği tartışmasızdır. Özellikle şirketlerin, çerez teknolojilerini kullanarak kullanıcıların kişisel bilgilerini elde edebildikleri ve bu bilgilerle kullanıcıları tanımlayan dijital profiller oluşturabildikleri göz önüne alındığında konunun çocuklar açısından önemi daha anlaşılır olmaktadır.

Meseleye çocukların profillenmesi açısından yaklaşıldığında, profilleme ve otomatik karar almanın, ilgili kişi olan çocuk açısından içerdiği risklerin, bir yetişkinin ilgili kişi olmasına kıyasla daha fazla olduğunun kabulü gerekir. Bunun ilk sebebi veri sorumlusu tarafından ilgili kişi çocukken yapılan profillemenin, bu kişiyi hayatı boyunca takip etmesinin ve ömrünün yetişkinlik dönemine dair de etkiler doğurmasının mümkün olmasıdır.

Bir diğer önemli neden de çocukların rıza gösterecekleri profilleme veya otomatik karar alma faaliyetlerinin kapsam ve sonuçlarını tam olarak algılayarak konuya ilişkin özgür iradeye dayalı rıza açıklamalarının

---

Otoritesinin (CNIL) Google Kararı ve Türk Hukuku Bağlamında Çerezler", AS-BÜHFD, C. 4, S. 2, Ankara 2022, s. 762-797; Çerez Uygulamaları Hakkında Rehber, https://www.kvkk.gov.tr/Icerik/7353/Cerez-Uygulamalari-Hakkinda-Rehber. (E. T. 05.05.2024).

28 Konuya ilişkin ayrıntılı bilgi için bkz. **KESER**, s. 1197.

29 **KESER**, s. 1197.

zorluğudur.[30] Örneğin çocuklar üzerinde çevrimiçi oyunlarda gerçekleştirilen profilleme aracılığıyla, harcama yapma olasılığı en yüksek olan oyuncuları belirlemek ve onlara kişiselleştirilmiş önerilerde bulunmak veya bir pazarlama uygulaması için çocuğun olgunluğuna karşılık gelmeyen kişiselleştirilmiş duyurular sağlamak mümkündür.[31]

B. Otomatik Karar Alma

Otomatik karar alma, ilgili kişinin elde edilen kişisel verilerinin, önceden belirlenmiş kriterlere dayalı olarak ve otomatik bir veri işleme sürecine tabi kılınarak, kişi hakkında bazı sonuçlara varılması şeklinde tanımlanabilir.[32] Otomatik karar almanın en yaygın örneklerinden biri, otomatik hız ölçümü yapılan yollarda sürücünün belli noktalardan geçiş zamanlarının hesaplanması suretiyle hızının tespit edilmesi ve sınırların üzerinde olduğuna otomatik olarak karar verilmesi halinde cezalandırılmasıdır.

Otomatik karar alma sistemlerinde yapay zekanın insan kaynakları alanında kullanıldığına da şahit olmak mümkündür. Özellikle verilen iş ilanına çok sayıda başvurunun olduğu durumlarda, adayların özgeçmişlerinin ilk elemesinin (mezun olunan Üniversite, fakülte, bölüm veya not ortalaması, iş deneyimi vb. kriterlere dayalı olarak) yapay zeka sistemli bir algoritma üzerinden yapıldığı durumlar otomatik karar alma örneği olarak düşünülebilir.

Özellikle anlaşılabilir (hatta şeffaf) olmayan algoritmalar nedeniyle ortaya çıkan veri asimetrisi, ilgili kişilerin kendi kişisel verileri üzerindeki kontrol haklarını ihlal edebilir niteliktedir. Bu durumda ilgili kişinin kişi-

---

30 Özellikle profilleme sonrasında, çocukların profillerine uygun reklamların -bu verilerin reklam verenlerle de paylaşılması suretiyle- profillenen çocuğun karşısına çıkarılması, akla ilk gelen sakıncalardan biridir. Diğer olumsuz etkiler için bkz. **ESEN BAYGÜNEŞ, Merve:** "Dijital Ortamda Çocukların Kişisel Verilerinin Korunması", BÜHFD, C. 7, S. 1, Ankara 2021, s. 169.

31 **PERSANO, Federica:** "GDPR and Children Rights in EU Data Protection Law", European Journal of Privacy Law & Technologies, C. 11, Özel Sayı, Torino 2020, s. 34.

32 **BADUR**, s. 98; **WELFARE/ CAREY**, s. 23; **LLOYD-JONES, Heledd/ CAREY, Peter (Edt. CAREY, Peter):** "The Rights of Individuals", Data Protection A Practical Guide to UK and EU Law, 5. Baskı, Oxford University, Oxford 2018, s. 149; **PETKOVA/ BOEHM**, s. 286; Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, s. 6. https://ec.europa.eu/newsroom/article29/ items/612053/en, (E. T. 10.04.2024)

sel verilerinin işlenmesine yönelik olarak açıkladığı rıza iradesinin geçerliliği de sorgulanabilir hale gelmektedir. Özellikle algoritmik kararların kapalı (kara) kutu etkisi[33], öncelikle veri sorumlusunun aydınlatmasını; sonrasında da aydınlatmaya dayalı olarak oluşturulan ve özgür iradeye dayanan rızanın geçerliliğini sakatlayan bir durum olarak ortaya çıkabilmektedir. Ayrıca profilleme veya algoritmik kararla yaratılan durumun geri döndürülmesinin mümkün olmayabileceği de göz önünde bulundurulmalıdır.[34]

GVKT'nin 15/1/h ve 22. maddelerinde ilgili kişilerin haklarının profilleme ve otomatik karar alma süreçlerinden korunmasına karşı etkin bir koruma sağlanmaya çalışılmıştır. İlgili kişi profilleme de dahil olmak üzere otomatik karar alma süreçlerinin varlığı; bu işlemeler sırasında benimsenen (izlenen) yönteme ilişkin anlamlı bilgiler ve söz konusu işlemenin öngörülebilir sonuçlarına ilişkin bilgilendirilme hakkına sahip kılınmıştır. Ayrıca ilgili kişiye kendisiyle ilgili hukuki sonuçlar doğuran[35] veya benzer şekilde kendisini ciddi şekilde etkileyen[36] otomatik karar alma süreçlerine rızası haricinde tabi olmama hakkı tanınmıştır. Konuya ilişkin

---

33 "Yapay zeka tarafından çıktı üretmek için girdiler üzerinde yapılacak işlemler 'öğrenme' adı verilen aşamada gerçekleştirilen çok sayıda istatistiksel değerlendirme sonucunda yazılım tarafından belirlendiğinden ve kullanılan tekniğe göre değişmekle birlikte özellikle gelişmiş örneklerde bu işlemler insanlar tarafından anlaşılabilir veya okunabilir olmadığından, bu modellerin üreteceği çıktılar insanlar tarafından tam anlamıyla öngörülebilir değildir. Bu durum çoğunlukla kara kutu problemi (black box problem) olarak adlandırılmaktadır." **AKSOY RETORNAZ, Eylem/ GÜÇLÜTÜRK, Osman Gazi:** "Yapay Zekada Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler", Kişisel Verilerin Korunmasına Akademik Bakış, Ankara 2023, s. 414.

34 **BÜYÜKSAĞİŞ**, s. 535.

35 İlgili kişi hakkında hukuki sonuç doğuran kararlar, kişinin hukuki hak ve yükümlülüklerini veya hukuken tabi olduğu statüyü belirleyecek etkiler içerirler. Örneğin kişinin hakkında alınan böyle bir karar sonrasında bir ülkeye giriş yapması veya bir sözleşmeye taraf olması engellenebilir. Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, s. 21, https://ec.europa.eu/newsroom/article29/items/612053/en, (E. T. 10.04.2024); **KUNER/ BYGRAVE/ DOCKSEY**, s. 99.

36 Bu durumda alınan karar ilgili kişi hakkında hukuki sonuç doğurmasa da bu kişiyi önemli ölçüde etkilemekte yani ilgili kişinin içinde bulunduğu koşullar, sergilediği davranışlar veya yaptığı seçimler üzerinde sonuç doğuracak etkiler göstermektedir. Bu etkiden söz edilebilmesi için, kararın ilgili kişi üzerinde *"uzun süreli veya kalıcı bir etkiye sahip olması ya da kişinin dışlanmasına ve/veya ayrımcılığa uğramasına yol açması"* gerekir. Örneğin ilgili kişinin yapmış olduğu iş başvurusunun otomatik reddi bu

olarak dikkatli yaklaşılması gereken nokta, ilgili kişi hakkında verilecek kararın, hukuki sonuç doğurmaya benzer etkiler göstermesinin gerekli olmasıdır.

29. Madde Çalışma Grubu[37] olarak adlandırılan AB yetkili organının hazırladığı raporda[38] GVKT'nin Başlangıç kısmının 71. paragrafından yola çıkarak çocukların profillenmeleri söz konusu olduğunda Tüzüğün 22/2. maddesinde yer verilen istisnalara[39] dayanılmaması yönünde görüş açıklamıştır. Başka bir ifadeyle Tüzüğün *"İlgili kişinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profillenmeler de dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama"* hakkına ilişkin 22/1. maddesinin çocuklar söz konusu olduğunda istisnasız şekilde uygulanması gerektiğini belirtmiştir.

Özellikle ilgili kişilerin sigorta risk ve primlerinin belirlenmesinde, iş başvurusu yapan adayların özgeçmişlerinin incelenme ve elenmesinde, tüketici kredisi almak için başvuran kişilerle sözleşme yapılıp yapılmamasının seçilmesinde algoritmik yazılımlarla verilen otomatik kararlar

---

kapsamda değerlendirilebilir. Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, s. 22, https://ec.europa.eu/newsroom/article29/items/612053/en, (E. T. 10.04.2024); **KUNER/ BYGRAVE/ DOCKSEY**, s. 99.

37 Metinde söz edilen 29. Madde Çalışma Grubu GVKT ile yürürlükten kaldırılan kişisel verilerin korunması hakkında AB Direktifinin 29. maddesiyle kurulduğundan bu adı almıştır. Açıklanan nedenle resmi isimlendirmesi *"Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkında Çalışma Grubu"* olsa da; öğreti ve uygulamada *"29. Madde Çalışma Grubu (Article 29 Working Party)"* ifadesiyle kısaltılarak kullanılmaktadır. Söz konusu çalışma grubu, sadece Direktifin değil; Direktif sonrasında yürürlüğe giren GVKT'nin de üye devletlerarasında yeknesak biçimde uygulamasına hizmet eden raporlar kaleme almıştır. 29. Madde Çalışma Grubu, GVKT'nin yürürlüğe girmesiyle birlikte, yerini GVKT'nin 94/2. maddesi uyarınca kurulan *"Avrupa Veri Koruma Otoritesine"* bırakmıştır.

38 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, s. 28, https://ec.europa.eu/newsroom/article29/items/612053/en, (E. T. 10.04.2024)

39 GVKT'nin 22/2. maddesinde, *"ilgili kişiyle veri sorumlusu arasında bir sözleşme kurulması veya uygulanması için gerekli olması; veri sorumlusunun tabi olduğu ve ilgili kişinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya üye devlet hukuku çerçevesinde izin verilmesi veya ilgili kişinin açık rızasına dayanması durumlarında profilleme de dahil olmak üzere otomatik karar alma süreçlerinin işletilebileceği"* düzenlenmiştir.

söz konusu olmaktadır. İlgili kişiler hakkında yeni bir hukuki durum yaratan veya benzer şekilde önemli bir durum meydana getiren algoritmik kararlar, insan denetiminden geçirildikten sonra uygulamaya konmalıdır.[40]

III. YAPAY ZEKA SİSTEMLERİ KULLANILARAK YAPILAN İŞLEME FAALİYETLERİNDE ÖZEN GÖSTERİLMESİ GEREKEN HUSUSLAR

Bir veri işleme faaliyetinin yapay zeka sistemleri kullanılarak gerçekleştirilmesi halinde, ilgili kişilerin kişisel verilerinin ve özel yaşamlarının korunması, mahremiyetlerine saygı gösterilmesi açısından özen gösterilmesi gereken bazı durumlar bulunmaktadır. Bu kapsamda yapay zeka sistemleri tarafından yapılan işlemelerde, kişisel verilerin işlenmesinde uyulması zorunlu olan temel ilkelere uygun davranılmasının garanti altına alınması ilk gereklilik olarak ortaya çıkmaktadır. Özellikle yapay zeka sistemleri tarafından gerçekleştirilen profilleme ve otomatik karar alma uygulamalarında, yapay zekanın genellemelere dayalı olan önyargılı tutumlarının sonuca ulaşmak üzerindeki etkisinin önlenmesi bir zorunluluktur.

Ayrıca yapay zeka sistemleri tarafından yapılan işlemelerde kullanılan yazılımların ve algoritmaların anlaşılması ve kavranması güç olan formüller barındırması (kara kutu etkisi), ilgili kişilere bu tür işleme faaliyetlerine ilişkin olarak yapılan aydınlatmaları da zorlaştırmakta; hatta etkisiz hale getirmektedir. Aydınlatmaya ilişkin yaşanan hukuki sorunların, bu aydınlatmalara dayalı olarak alınan rızaların da hukuka uygunluğunu tartışmaya açık hale getirmesi mümkündür.

A. Genel İlkelere Uygun İşleme

Yapay zeka kullanılarak yapılan işleme faaliyetlerinde özen gösterilmesi gereken öncelikli husus, KVKK'nın 4. maddesinde düzenlenen kişisel verilerin işlenmesinde uyulması zorunlu olan temel ilkelere uygun hareket edilmesinin sağlanmasıdır. Bu temel ilkelere göre *"kişisel verilerin işlenmesi hukuka ve dürüstlük kurallarına uygun; doğru ve gerektiğinde güncel olmalı; kişisel veriler belirli, açık ve meşru amaçlar için işlenmeli; işlendikleri*

---

40 **BÜYÜKSAĞIŞ**, s. 530.

amaçla bağlantılı, sınırlı ve ölçülü olmalı; ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza" edilmelidir.[41]

Bu ilkelere kişisel verilerin türleri arasında bir ayrım yapılmadan ve bu verilerin herhangi bir hukuka uygunluk sebebi uyarınca işlenmesi sırasında riayet edilmesi gerekir. Genel ilkeler verilerin işlenmesindeki her aşamayı ve her türlü veri işleme faaliyetini kapsamaktadır.[42] Kişisel verilerin yapay zeka tarafından işlenmesi sırasında, bu temel işleme ilkelerine uygun davranılması, veri sorumlusu tarafından gerçek kişilerin denetimine tabi kılınarak nihai bir kontrol sağlanmalıdır.

Ayrıca KVKK'da yer verilmeyen bazı başka ilkelerin GVKT'de düzenlendiği görülmektedir. Bunlardan biri GVKT'nin 5/1/a maddesinde, kişisel verilerin işlenmesi ilkesi olarak açıkça kaleme alınan şeffaflık (transparency) ilkesidir. Bu ilkeyle sağlanması amaçlanan en önemli hedefin, ilgili kişinin kişisel verilerinin hangi veri sorumlusu tarafından ve hangi amaçla işlendiğinin istisnasız şekilde öğrenilebilmesini sağlamak olduğu belirtilmiştir.[43] Özellikle yapay zeka tarafından profilleme ve oto-

---

41 KVKK'nın 4/2. maddesinde belirlenen ilkeler, 108 sayılı Sözleşmenin 5. maddesinde *"Verilerin Niteliği"* başlığı altında düzenlenen kurallarla uyumludur. 108 sayılı Sözleşmede, işlenecek kişisel verilerin *"adil bir şekilde ve yasal yoldan elde edilmesi; belirli ve meşru amaçlar için kaydedilmesi ve bu amaca aykırı kullanılmaması; kaydedilme amaçlarına uygun ve sadece gerektiği kadar verinin saklanması; verilerin doğru ve gerektiğinde güncel olması; ilgili kişinin kimliğini belirtecek şekilde, ancak kaydedilme amacını sağlamak için gerekli olan süre kadar saklanması"* gerektiği düzenlenmiştir.

42 Konuya ilişkin ayrıntılı bilgi için bkz. **BADUR**, s. 114 vd; **CAREY, Peter (Edt. CAREY, Peter):** "Data Protection Principles", Data Protection A practical Guide to UK and EU Law, 5. Baskı, Oxford 2018, s. 32-41; **DÜLGER,** KVKH, s. 261; **OĞUZ, Sefer:** "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Ekonomisi ve Yönetimi Dergisi, C. 12, S. 3, Ankara 2018, s. 121-138; **KIRATLI, Metin:** "Kişisel Verilerin Korunması Hukukunun Temel İlkeleri", Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, Yetkin Yayıncılık, Ankara 2022, s. 219-237; **TURGUT BİLGİÇ, Ezgi:** "Genel Veri Koruma İlkelerinin Yapay Zekâ Karşısında Uygulanabilirliği Sorunu", Türkiye Adalet Akademisi Dergisi, S. 57, Ankara 2024, s. 247-282; **YÜCEDAĞ, Nafiye:** "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi, C. 1, S. 1, Ankara 2019, s. 47-63; **BAŞKAYA, Fatma/ KARACAN, Hacer:** "Yapay Zekâ Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme", Bilişim Teknolojileri Dergisi, C. 15, S. 4, Ankara 2022 s. 481-491.

43 **CAREY**, s. 33; **DÜLGER,** KVKH, s. 271; **KELLEHER/ MURRAY**, s. 139; **KUNER/ BYGRAVE/ DOCKSEY**, s. 68.

matik karar alma türünde işlemelerin yapıldığı her durumda, verisi işlenen ilgili kişilere söz konusu şeffaflık sağlanabilir olmalıdır. Bu da algoritmik kararlara dayanak teşkil eden, algoritmaların ilgili kişilerce öğrenilebilir olmasına imkan tanınmasını gerekli kılar.[44]

Anayasa Mahkemesi de yakın tarihli bir kararında[45] *"Kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme ve bu verilere erişme hakkı Anayasa'nın 20. maddesinin üçüncü fıkrasında açıkça öngörülmüş olan güvencelerdir. Kişisel verilerin şeffaflığı ilkesi de bu güvencelerin sağlanmasını gerektirmektedir."* ifadesini kullanmak suretiyle, KVKK'da açıkça yer verilmeyen bu ilkeye atıf yapmıştır.

B. Aydınlatma ve Rızaya İlişkin Hususlar

Kişisel verilerin yapay zeka karşısında korunması için, özellikle dikkatli olunmasını gerektiren bir diğer husus da yapay zeka sistemleri tarafından veri işlemenin ilgili kişinin rızasına dayalı olarak gerçekleştirildiği durumlarda, aydınlatmaya ve rızanın serbest irade sonucunda oluşmasına özen gösterilmesi gerekliliğidir. Kişisel verilerin hukuka uygun olarak işlenmesindeki temel kural, bu işlemenin ilgili kişinin rızasına dayanmasıdır. Kişisel verilerin işlenmesinde rızanın önemi, Anayasa'nın kişisel verilerin korunmasına ilişkin 20/3. maddesinde *"Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir."* ifadesiyle yer verilen kuralda da rızaya yapılan vurgudan anlaşılabilir.

Kişisel verilerin hukuka uygun olarak işlenmesiyle ilgili temel kural KVKK'nın *"Kişisel verilerin işlenme şartları"* kenar başlıklı 5/1. maddesinde *"Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez."* ifadesiyle ortaya konulmuştur. Yasa koyucu, KVKK'nın 6/3/a maddesinde de özel nitelikli kişisel verilerin işlenmesi açısından, ilk hukuka uygunluk sebebi olarak ilgili kişinin rızasını esas almıştır. Bir işleme türü olan kişisel verilerin ak-

---

44 Yapay zekanın nasıl veri elde ettiğinin ve işleme sonucunda nasıl karar verdiğinin veya iç işleyişinin anlaşılamaması ve gözlemlenememesi "kara kutu (black box)" olarak adlandırılmaktadır. Bu terim, kişisel verilerin algoritmik hesaplama içine girmesi ve üretilen çıktının neye göre verildiğinin bilinmemesi durumunu da kapsar. Özellikle yorumlanması zor karmaşık hesaplamaları içeren yapay zeka işlemeleri için geçerli olan kara kutu sorunu, yapay zekanın istenmeyen sonuçlar üretmesi halinde, bunların düzeltmesini zorlaştırır. Konu hakkında ayrıntılı bilgi için bkz. **TURGUT BİLGİÇ**, s. 262.

45 AYM, K. 2018/6161, T. 28.06.2022.

tarılması için de yasa koyucu tarafından aynı kuralın benimsenmesi suretiyle, kişisel verilerin yurt içine aktarılması için KVKK'nın 8/1. maddesinde ilgili kişinin rızası aranmıştır.

Aydınlatma sadece KVKK'nın 10. maddesi kapsamında veri sorumlusu tarafından yerine getirilmesi gereken bir yükümlülük değil; aynı zamanda ilgili kişinin rızasının serbest iradeye dayalı olarak oluşmasının da önkoşuludur. Zira hangi kişisel verilerinin, hangi amaç ve yöntemlerle işleneceğini; bu işlemenin sonuçlarını ve olası etkilerini aydınlatma sayesinde öğrenen bir kişi bu faaliyeti açıklayacağı rıza iradesi ile hukuka uygun kılabilir.

Kurul[46] aydınlatmayı, *"veri sorumlusu ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile ilgili kişinin diğer haklarının neler olduğu konusunda kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi tarafından ilgili kişiye yapılan bilgilendirme"* olarak tanımlamıştır. Aydınlatma yükümlülüğünün temelinde şeffaflık ilkesinin yer aldığının söylenmesi de mümkündür.[47] Veri işleme süreci ne kadar teknik, kapsamlı ve karmaşıksa, veri sorumlusunun bilgilendirme yükümlülüğü aynı oranda ciddileşir.[48]

Kişisel verilerin yapay zeka sistemleri aracılığıyla işlenmesi halinde, ortaya çıkan başlıca güçlük aydınlatmaya ilişkin olmaktadır. Yapay zeka sistemlerinin kara kutu etkisi, aydınlatmanın içeriğinin anlaşılırlığını düşürmekte; bu da işlemeye ilişkin rıza açıklamalarının serbest irade

---

46 Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü, s. 104. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu (E. T. 04.06.2024)

47 Konu hakkında ayrıntılı bilgi için bkz. **AŞIKOĞLU, Şehriban İpek:** "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", KVKD, C. 1, S. 2, Ankara 2019, s. 43. "Kullandığı veya maruz kaldığı teknolojinin nasıl çalıştığı konusunda bilgi sahibi olmayan bir kişinin verilerinin işlenmesiyle ilgili nasıl bir risk değerlendirmesi yapıp rızasını ona göre verebileceği önemli bir sorudur." **GÜLTEKİN VARKONYİ, Gizem:** "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumluluklar", KVKD, C. 2, S. 2, Ankara 2020, s. 19-29.

48 **BADUR**, s. 153.

sonucu oluşamaması (sakatlanması) ihtimalini yükseltmektedir. Özellikle yapay zeka sistemleri tarafından yapılan işlemelerde, ilgili kişilerin hangi verilerinin hangi amaçlarla işlendiğine yönelik şeffaflığın sağlanması hukuka ve dürüstlük kurallarına uygunluğa, ölçülülüğe ve hesap verebilirliğe bağlı kılınması için zorunlu görülmektedir.

Yapay zeka sistemleri aracılığıyla işlenen kişisel verilere yönelik yapılan aydınlatmada amaç doğru şekilde belirlenmiş olsa bile amacın ilgili kişiye sunulmasında kullanılacak olan dilin anlaşılabilir olmasına ayrıca özen gösterilmelidir.[49] Kurul tarafından hazırlanan yapay zeka sistemleri aracılığıyla gerçekleştirilen veri işleme faaliyetine yönelik Tavsiyelerde[50] de *"Uygulama ile etkileşime giren kişiler, kişisel veri işleme faaliyetinin gerekçeleri, kişisel verilerin işlenmesinde kullanılan yöntemlerin detayları ile muhtemel sonuçları hakkında aydınlatılmalı ve gerekli haller için etkili bir veri işleme onay mekanizması tasarlanmalıdır."* ifadesiyle hukuka uygun işleme açısından aydınlatma ve rızanın önemine dikkat çekilmiştir.

GVKT'nin 35/1. maddesinde *"Veri koruma etki değerlendirmesi"* kenar başlığı altında düzenlenen hükümde *"**Özellikle yeni teknolojiler** kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek **kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde** veri sorumlusu, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar."* ifadesi kullanılmıştır.

KVKK'da karşılığı bulunmayan bu hüküm gereğince yapay zeka sistemlerini kullanarak işleme faaliyetinde bulunan veri sorumluları, işleme sürecin gerekliliğini, kapsamını, süresini, hukuka uygunluk sebep-

---

[49] Örneğin çevrim içi video platformunun yapay zeka sistemi kullanarak yürüttüğü işleme faaliyetine yönelik olarak "yapay sinir ağları ve derin öğrenme yöntemleri kullanılarak oluşturulacak istatistiksel çıktılar ile kişilerin ilgi alanları ve izleme geçmişi arasındaki bağlantının hesaplanması sonrasında en ilgili olan içeriklerin belirlenmesi ve uygulama ara yüzünde ilgi derecesine göre kullanıcıya sunulması" ifadesiyle yaptığı aydınlatma, ilk bakışta belirlilik açısından uygun görülebilse de; ifadenin içerdiği teknik terimler ve uzunluğu sebebiyle ilgili kişinin kafasının karışması sonucunu doğurabilecek ve aydınlatma amacına ulaşamayacaktır. **AKSOY RETORNAZ/ GÜÇLÜTÜRK**, s. 430.

[50] https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler (E. T. 06.05.2024)

lerini, orantılılığını, şeffaflığını ve işlemenin sonuçlarını kullanılan teknolojinin etkisini de göz önünde bulundurarak, ilgili kişilerin hak ve özgürlüklerine ilişkin oluşabilecek riskler açısından değerlendirmekte ve bu riskleri minimize etmeye yoğunlaşmaktadırlar. Türk Hukuku açısından da yapay zeka sistemleri kullanarak veri işleyen veri sorumluları, veri koruma etki değerlendirmesi yaparak; kişisel verilerin işlenmesinden önce işlemeye risklerin ve bunları minimize edecek tedbirlerin belirlenmesini sağlayabilirler.[51]

Öğretide[52] yapay zeka sistemlerinin geldiği seviye itibariyle, yapay zekanın kişisel veri olarak nitelenemeyen verilerden veya anonimleştirilmiş verilerden yola çıkarak yürüttüğü faaliyet sonucunda kişisel veri üretmesinin de mümkün olduğu hususuna dikkat çekilmektedir. Üstelik böyle bir durumda işlenen ve ilgili kişileri doğrudan belirlenebilir kılan olası tahminler karşısında bu kişilerin korunma yöntemlerine ilişkin belirsizlikler bulunmaktadırBu durum, yapay zeka sistemleri karşısında, kişisel verilerin anonimleştirilmesini etkisizleşmesi sonucunu doğurmaya elverişlidir.

C. Kişisel Verileri Koruma Kurulunun Tavsiye Metni

Konuya ilişkin olarak üzerinde durulması gereken son nokta, Kişisel Verileri Koruma Kurulu tarafından hazırlanan *"Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"*[53] adlı rehberdir. Anılan metinde Kurul tarafından yapılan tavsiyeler, *"Genel Tavsiyeler"*; *"Geliştiriciler, Üreticiler ve Servis Sağlayıcılar İçin Tavsiyeler"* ve *"Karar Alıcılar İçin Tavsiyeler"* olarak ayrımlamaya tabi kılınmıştır.

---

51 **BURHAN, Begüm Tuğçe:** "Yapay Zekâ Sistemlerinde Veri Koruma Yaklaşımları", Kişisel Verilerin Korunmasına Uzman Bakış, Ankara 2023, s. 434.

52 **ABUDUREYIMU, Yiliyaer/ OĞURLU, Yücel:** "Yapay Zeka Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, C. 20, S. 41, İstanbul 2021, s. 774; **ÇAVUŞOĞLU, Gökçe Filiz:** Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları, Yetkin Yayınları, Ankara 2021, s. 78; **KOTİL ÖĞRETMEN, Zeynep:** Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka, On İki Levha Yayıncılık, İstanbul 2022, s. 87; **NARBAY, Şafak/ KİRAZLI, Şerife Nur:** "Otonom Araçlarda Yapay Zeka, Kişisel Verilerin İşlenmesi ve Sonuçları", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C. 11, S. 1, Sakarya 2023, s. 51.

53 https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler (E. T. 06.05.2024)

Genel Tavsiyeler kısmında yapay zeka uygulamalarının geliştirilmesi ve uygulanması sürecinde ilgili kişilerin temel hak ve özgürlüklerine saygı gösterilmesi, insan hakları ve temel özgürlüklerin özellikle de insan onurunun korunmasının gözetilmesi gerekliliği vurgulanmıştır. Yapay zeka sistemleriyle kişisel verilerin işlendiği hallerde veri toplama çalışmalarının kişilerin temel hak ve özgürlüklerini koruyan bir yaklaşım içerisinde genel veri işleme ilkelerine uyularak, veri güvenliği yaklaşımına riayet edilerek gerçekleştirilmesi gerektiği belirtilmiştir. Kurula göre yapay zeka sistemleri aracılığıyla kişisel verilerin işlenmesinde, potansiyel risklerin önlenmesi ve azaltılması üzerine odaklanan, insan haklarını, demokrasinin işleyişini, sosyal ve etik değerleri de göz önünde bulunduran bir bakış açısı benimsenmelidir.

Yapay zekanın kullanıldığı işleme faaliyetlerinde de *"kontrol prensibinden"*[54] ödün verilmemelidir. Kişisel veri işleme temelli yapay zeka çalışmalarında, kişisel verilerin korunması açısından yüksek risk öngörülüyorsa, mahremiyet etki değerlendirmesi uygulanmalı ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmelidir. Yapay zeka sistemleri geliştirilirken ve uygulanırken özel nitelikli kişisel veriler de işleniyorsa hem bu tür veriler için geçerli olan hukuka uygunluk sebeplerine hem de teknik ve idari tedbirlere daha sıkı şekilde uyulmalıdır. Yapay zeka sistemlerinin geliştirilmesi ve uygulanmasında aynı sonuca kişisel veri işlenmeksizin ulaşılabiliyorsa; verilerin anonim hale getirilmesi sağlanmalıdır.

Rehberin, *"Geliştiriciler, Üreticiler ve Servis Sağlayıcılar İçin Tavsiyeler"* kısmında yapay zeka sistemlerinin tasarımında, ulusal ve uluslararası normlara uygun ve kişisel veri mahremiyetini esas alan bir yaklaşımın benimsenmesi; uygun risk önleme ve azaltma tedbirlerine uyulması; kişisel verilerin elde edilmesinden başlayarak işlemenin her aşamasında, temel hak ve özgürlüklerin gözetilmesi ve ilgili kişiler hakkında oluşabilecek ayrımcılık riski veya önyargıların önlenmesi gerekliliklerine vurgu

---

[54] İlgili kişinin, kendisine ait kişisel veriler üzerinde sahip olduğu hak, kişisel verilerinin işlenmesi sürecinde belirleyici olma yetkisinin de bu kişide olmasını gerekli kılmaktadır. Kişinin rıza vermek (veya esirgemek ya da geri almak) suretiyle verileri üzerinde sahip olduğu yetkiye "kontrol prensibi" adı da verilmektedir. Konuya ilişkin ayrıntılı bilgi için bkz. **LAZARO, Christophe/ LE METAYER, Daniel:** "Control Over Personal Data: True Remedy of Fairy Tale", SCRIPTed: A Journal of Law, Technology and Society, C. 12, S. 1, 2015, https://script-ed.org/wp-content/uploads/2015/06/lazaro_metayer.pdf?d= 11192022. (E. T. 10.06.2024); Badur, s. 133.

yapılmıştır. Yapay zeka sistemlerini geliştiren, üreten veya servis sağlayanlar veri minimizasyonunu gerçekleştirmeli ve geliştirilen modelin doğruluğunu sürekli şekilde izlenmelidirler. Özellikle bağlamından koparılmış algoritma[55] modelleri, bireyler ve toplum üzerinde olumsuz etkilere sebep olma riski açısından dikkatle değerlendirilmelidir.

Yapay zeka sistemlerini geliştiren, üreten veya servis sağlayanlar bu sistemlerin kişisel verileri analiz etme ve kullanma gücünü göz önünde bulundurarak, ilgili kişilerin ulusal ve uluslararası mevzuattan doğan haklarını korumalıdır. İlgili kişilerin otomatik işlemeye dayalı olarak kendilerini etkileyecek bir karara maruz kalmamalarını sağlayacak ürün ve hizmetlerin tasarlanmasına özen gösterilmelidir. Ayrıca Kurul tarafından kişilerin yapay zeka sistemleriyle sunulan önerilerin sonucuna güvenmeme özgürlüğünün korunması hususuna vurgu yapılmış ve algoritmaların veri koruma hukuku yönünden hesap verebilir nitelikte olmasının sağlanması gerektiği ifade edilmiştir. İlgili kişilere veri işlemeyi durdurabilme hakkı tanınmalı ve yapay zeka sistemleri açısından da kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinin yolları tasarlanmalıdır.

Son olarak Kurul, *"Karar Alıcılar İçin Tavsiyeler"* başlığı altında *"hesap verebilirlik ilkesine"*[56] vurgu yapmış ve işlemenin tüm aşamalarında bu ilkenin gözetilmesi gerektiğini belirtmiştir. Karar alıcılar, yapay zeka sistemlerinin farklı bir bağlam veya amaç için kullanılıp kullanılmadığını izlemek üzere yeterli kaynak ayırmalı ve özellikle karar alma süreçlerinde insan müdahalesinin rolünü tesis etmelidir. Bireylerin, yapay zeka uygulamaları ile sunulan önerilerin sonucuna güvenmeme özgürlüğü korunmalıdır. Ayrıca ilgili kişilerin yapay zeka sistemlerini ve etkilerini anlama konusunda farkındalığının artırılması amacıyla dijital okuryazarlık ve eğitim kaynaklarına yatırım yapılmalıdır.

---

55 "Bağlamından koparılmış algoritma, başlangıçta belirli bir yapay zeka modeli için tasarlanmış algoritmaların amacı dışında farklı bir amaç ya da yapay zeka modelinde kullanılmasını ifade eder."

56 GVKT'nin 5/2/g maddesinde veri sorumlusunun tüm ilkelere uygun davranmakla yükümlü olduğu ve ilkelere uygun davranmadığı durumlarda sorumluluğunun gündeme geleceği belirtilmiştir. Bu ilke, hesap verilebilirlik ilkesi olarak anılmaktadır.

D. AB Yapay Zeka Tüzüğü

Bu başlık altında incelenmesi gerekli görülen temel hukuki düzenleme Avrupa Birliği (AB) Hukukuna ilişkindir. AB Komisyonu yapay zeka sistemlerinin geliştirilmesi ve kullanılmasına ilişkin bir hukuki çerçeve düzenlemek amacıyla AB Yapay Zeka Tüzüğü Teklifi metinini 21.04.2021 tarihinde açıklamış ve AB Yapay Zeka Tüzüğü (AI Act) 13.06.2024 tarihinde AB Parlamentosu ve AB Konseyi'nce resmi olarak kabul edilerek; 01.08.2024 tarihinde yürürlüğe girmiştir.[57] Anılan Tüzük, Türk Hukuku yönünden bağlayıcılık taşımamakla birlikte; yapay zeka sistemlerine ilişkin hukuki düzenleme yapılması ve bu kapsamda kişisel verilerinde yapay zeka karşısında korunmasına ilişkin hükümler barındırması açısından önemli bir adımdır.[58]

Tüzüğün temel konusunu yapay zeka sistemleri oluşturmaktadır. Tüzüğün tanımlara ilişkin 3/1. maddesinde yapay zeka sistemi, *"değişen seviyelerde özerklikle çalışmak üzere tasarlanmış, kurulumdan sonra uyarlanabilirlik gösterebilen ve açık veya örtülü hedefler için, aldığı girdiden, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerik, öneriler veya kararlar gibi çıktıları nasıl üreteceğini çıkaran makine tabanlı bir sistem"* olarak tanımlanmıştır. Tüzükte yapay zeka sistemleri risk tabanlı bir yaklaşımla *"kabul edilemez riskli, yüksek riskli, sınırlı riskli ve düşük riskli"* olmak üzere dört kategoriye ayrılmıştır.

AB bu düzenleme ile yapay zeka teknolojilerinin Avrupa değerlerini, demokratik toplum yapısını ve temel hakları ihlal etmeden ekonomiye ve topluma saplayacağı katkıları en üst seviyeye taşımayı hedeflemektedir. Bu çerçevede risk temelli bir yaklaşımla hazırlanan metin, topluma zarar verme potansiyeli yüksek olan insan davranışlarını yönlendirme, insanların zafiyetlerini kullanma veya biyometrik sınıflandırma

---

[57] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 (E. T. 06.11.2024). Konu hakkında ayrıntılı bilgi için bkz. **BOZKURT YÜKSEL, Armağan Ebru:** "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakış", TAAD, C. 13, S. 51, Ankara 2022, s. 19-46.

[58] Tüzük tarafından getirilen yapay zeka sistemleri ile ilgili düzenlemeler, AB pazarına sunulan veya kullanması AB'de bulunan kişileri etkileyen mal ve hizmetler açısından, AB içinde yerleşik olan ve olmayan tüm kamu ve özel sektör kişileri açısından bağlayıcı niteliktedir (Tüzük md. 2). Konu hakkında ayrıntılı bilgi için bkz. **AKSOY**, Yapay Zeka, s. 218.

gibi işlevlere sahip yapay zeka sistemlerinin kullanımını yasaklamaktadır.

Tüzüğün Giriş kısmının 69. paragrafında özel hayatın ve kişisel verilerin korunması hakkının, yapay zeka sistemlerinin tüm yaşam döngüsü boyunca garanti altına alınması gerektiği kaleme alınmıştır. Bu bağlamda, GVKT'de belirtildiği gibi, veri minimizasyonu ve tasarımla ve varsayılan olarak veri koruma ilkeleri, kişisel veriler yapay zekayla işlendiğinde de geçerlidir. Bu ilkelere uyumu sağlamak için yapay zeka sağlayıcıları tarafından alınan önlemler, yalnızca anonimleştirme ve şifrelemeyi değil; aynı zamanda algoritmaların kişisel verilere uygulanmasına izin veren ve bu Tüzükte öngörülen veri yönetimi gerekliliklerini ihlal etmeksizin, ham veya yapılandırılmış kişisel verilerin aktarımı veya kopyalanması olmaksızın yapay zeka sistemlerinin eğitilmesine izin veren teknolojinin kullanımını da içerebilir.

Tüzüğün 10/5. maddesinde yüksek riskli yapay zeka sistemleri açısından, özel nitelikli kişisel verilerin yapay zeka sistemlerinde kullanılmasına, önyargının tespiti ve düzeltilmesi için izlenmesi gerekli olduğu ölçüde ve gerçek kişilerin temel hak ve özgürlükleri için uygun güvencelere tabi kılınması şartıyla izin verilmiştir. Bu durumda bile özel nitelikli kişisel veriler işlenirken, veri güvenliğine özel önem verilecek; bu veriler başka aktarılmayacak veya başka bir şekilde yetkisiz kişilerce erişilemeyecek halde saklanacaktır. Madde kapsamında işlenen özel nitelikli kişisel veriler, yanlılık düzeltildiğinde veya kişisel veriler saklama süresinin sonuna geldiğinde (hangisi önce gerçekleşirse) silinecektir.

Tüzüğün Giriş kısmının 54. paragrafında biyometrik verilerin özel nitelikli kişisel veriler arasında da hassas bir niteliğe sahip olduklarının altı çizilerek, ilgili Birlik hukuku ve ulusal hukuk kapsamında kullanımlarına izin verildiği ölçüde, biyometrik sistemlerin yüksek riskli olarak sınıflandırılması uygun bulunmuştur. Gerçek kişilerin uzaktan biyometrik tanımlanmasına yönelik yapay zeka sistemlerinin teknik yanlışlıklarının, yanlı sonuçlara yol açabileceği ve ayrımcı etkiler doğurabileceği belirtilmiştir. Bu tür yanlı sonuçlar ve ayrımcı etkilere dair riskler özellikle yaş, etnik köken, ırk, cinsiyet veya engellilikle ilgilidir. Bu nedenle uzaktan

biyometrik tanımlama sistemleri, oluşturdukları riskler göz önünde bulundurularak yüksek riskli olarak sınıflandırılmalıdır.[59]

Tüzüğün 50/2. maddesi gereğince yapay zeka sistemleri aracılığıyla duygu tanıma yapılması veya biyometrik kişisel verilerin kullanılması suretiyle sınıflandırma gerçekleştirilmesi halinde, buna maruz kalan gerçek kişiler sistemin işleyişi hakkında bilgilendirecektir.[60]

SONUÇ

Yapay zeka sistemleri vasıtasıyla kişisel verilerin işlenmesinin olası riskler barındırdığı yönünde genel bir kabul bulunmaktadır. Yapay zeka sistemlerinin kişisel verilerini işlediği ilgili kişilere yönelik olarak ayrımcılık yapılması endişesi başta olmak üzere, kişisel veri gizliliğinin ihlali, veri minimizasyonu ilkesinin göz ardı edilmesi, şeffaflık ve hesap verilebilirlik gibi temel veri işleme ilkelerine riayet edilememesi gibi kişisel verilerin hukuka uygun şekilde işlenmesi için gerekli olan hususların ayrıca dikkate alınması gerekliliği ortaya çıkmıştır.

Yapay zeka karşısında kişisel verilere etkin koruma sağlanabilmesinin önündeki bir diğer engel, yapay zeka sistemlerinin işleyişine dair bilgilerin kapalı kutu yapısında olmasındadır. Başka bir ifadeyle yapay zekanın hangi kişisel verileri hangi algoritmalara tabi tutarak işlediği ve ne gibi bileşenlerin etkisiyle kişisel veri niteliği taşıyan hangi sonuçlara ulaştığı anlaşılması zor süreçler içermektedir. Bu durum yapay zeka sistemleri vasıtasıyla yapılan işleme faaliyetlerinin hukuka aykırılık barındırıp barındırmadığı konusunda belirleme zorlukları yaratmaktadır.

Kişisel verilerin yapay zeka sistemleri vasıtasıyla işlenmesindeki temel hukuki meselelerden bir diğeri de yine kapalı kutu etkisiyle bağlantılı olana aydınlatma ve rıza sorunlarıdır. Veri sorumluları tarafından karmaşık algoritmalara dayalı yapay zeka sistemleri aracılığıyla işlenen kişisel

---

59 Bu sınıflandırma, kimlik doğrulama da dahil olmak üzere biyometrik doğrulama için kullanılması amaçlanan ve tek amacı belirli bir gerçek kişinin iddia ettiği kişi olduğunu teyit etmek ve bir hizmete erişim sağlamak, bir cihazın kilidini açmak veya tesislere güvenli erişim sağlamak amacıyla gerçek bir kişinin kimliğini doğrulamak olan yapay zeka sistemlerini hariç tutmaktadır.

60 Ancak bu yükümlülük, üçüncü tarafların hakları ve özgürlükleri için uygun güvencelere tabi olarak ve AB yasalarına uygun olarak, cezai suçları tespit etmek, önlemek veya araştırmak için yasalarca izin verilen biyometrik sınıflandırma ve duygu tanıma için kullanılan yapay zeka sistemleri açısından geçerli olmayacaktır.

verilere yönelik aydınlatma yükümlülüğünün ifası sırasında, bu algoritmaların işleyiş mantığının (veya programının ya da yöntemin) ilgili kişilere -kural olarak onların da anlayabileceği ifadelerle- açıklanması gerekmektedir.

Yapay zeka sistemleri kullanılarak gerçekleştirilmesi muhtemel kişisel veriler henüz elde edilirken, bu duruma ilişkin yukarıda belirtilen şekilde aydınlatma yapıldıktan sonra; ilgili kişilerin kişisel verilerinin bu şekilde işlenmesine rıza göstermelerine imkan tanınmalıdır. Hatta bu noktada ilgili kişilerin, veri sorumlusu tarafından kişisel verilerinin, yapay zeka sistemleri marifetiyle işlenip işlenmemesine yönelik ayrı ayrı rıza verebilmelerine olanak tanınmalıdır.

KAYNAKÇA

ABUDUREYIMU, Yiliyaer/ OĞURLU, Yücel: "Yapay Zeka Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, C. 20, S. 41, İstanbul 2021, s. 765-782.

AKSOY, Ecem: Yapay Zeka'nın Sorumluluk Hukukundaki Konumu ve Büyük Veri ile İlişkisi, Seçkin Yayınevi, Ankara 2022. (Yapay Zeka)

AKSOY, Hüseyin Can: Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2016. (KVK)

AKSOY, Hüseyin Can: "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", Kişisel Verileri Koruma Dergisi, C. 4, S. 2, Ankara 2022, s. 69-87. (Algoritmik)

AKSOY, Hüseyin Can/ HALICIOĞLU, Mesut: "AB ve Türk Hukuklarında Çerezler, Kişisel", Kişisel Verileri Koruma Dergisi, C. 3, S. 1, Ankara 2021, s. 61-88.

AKSOY RETORNAZ, Eylem/ GÜÇLÜTÜRK, Osman Gazi: "Yapay Zekada Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler", Kişisel Verilerin Korunmasına Akademik Bakış, Ankara 2023, s. 413-438.

AŞIKOĞLU, Şehriban İpek: "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", KVKD, C. 1, S. 2, Ankara 2019, s. 41-65. (Aydınlatma)

AŞIKOĞLU, Şehriban İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayınları, İstanbul 2018. (Büyük Veri)

AYÖZGER ÖNGÜN, A. Çiğdem: Kişisel Verilerin Korunması, 2. Baskı, Beta Yayınları, İstanbul 2016.

BADUR, Emel: Çocuğun Kişisel Verilerinin Korunması -KVKK, GVKT ve AİHM Kararları Çerçevesinde Bir İnceleme-, Seçkin Yayınevi, Ankara 2023.

BAŞAR, Cemal: Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul 2020.

BAŞKAYA, Fatma/KARACAN, Hacer: "Yapay Zekâ Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme", Bilişim Teknolojileri Dergisi, C. 15, S. 4, Ankara 2022 s. 481-491.

BULUT, Metin: "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", Ankara Barosu Dergisi, S. 3, Ankara 2020.

BURHAN, Begüm Tuğçe: "Yapay Zeka Sistemlerinde Veri Koruma Yaklaşımları", Kişisel Verilerin Korunmasına Uzman Bakış, Ankara 2023, s. 429-444.

BÜYÜKSAĞİŞ, Erdem: "Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı", YÜHFD, C. XVIII, S. 2, İstanbul 2021, s. 529-541.

CAREY, Peter (Edt. CAREY, Peter): "Data Protection Principles", Data Protection a Practical Guide to UK and EU Law, 5. Baskı, Oxford University Press, Oxford 2018, s. 32-41.

CAYGIN, Fatmanur/ YAVUZ, Can: "Yapay Zeka ve Çocuk Haklarına Kısa Bir Bakış", İBD, C. 94, S. 3, İstanbul 2020, s. 218-229.

ÇAVUŞOĞLU, Gökçe Filiz: Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları, Yetkin Yayınları, Ankara 2021.

ÇEKİN, Mesut Serdar: Kişisel Verilerin Korunması Hukuku, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2019.

DÜLGER, Murat Volkan: "Yapay Zekalı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli?", Terazi Hukuk Dergisi, C. 13, S. 142, Ankara 2018, s. 82-87. (Yapay Zeka)

DÜLGER, Murat Volkan: Kişisel Verilerin Korunması Hukuku, 3. Baskı, Hukuk Akademisi, İstanbul 2020. (KVKH)

DÜLGER, Murat Volkan: "Algoritmik Karar Verme ve Veri Koruması", https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3792207. (E. T. 08.11.2024) (Algoritmik)

ERDOĞAN, Irmak: Yapay Zeka ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkileri, Seçkin Yayıncılık, Ankara 2022.

ESEN BAYGÜNEŞ, Merve: "Dijital Ortamda Çocukların Kişisel Verilerinin Korunması", BÜHFD, C. 7, S. 1, Ankara 2021, s. 165-182.

GÜLTEKİN VARKONYİ, Gizem: "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumluluklar", KVKD, C. 2, S. 2, Ankara 2020, s. 19-29.

HİZARCI, Emine: 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun AB Veri Koruma Hukuku Işığında Değerlendirilmesi, Yetkin Yayınları, Ankara 2020.

IŞIK, Alper: "Fransız Veri Koruma Otoritesinin (CNIL) Google Kararı ve Türk Hukuku Bağlamında Çerezler", ASBÜHFD, C. 4, S. 2, Ankara 2022, s. 762-797.

KAYA, İslam Safa/ TOLUN, Yüksel: Türkiye'de ve Avrupa'da Kişisel Verilerin İşlenmesi, Adalet Yayınevi, Ankara 2020.

KELLEHER, Denis/ MURRAY, Karen: EU Data Protection Law, Bloomsbury, London 2019.

KESER, Yıldırım: "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza", SÜHFD, C. 28, S. 3, Konya 2020, s. 1181-1215.

KIRATLI, Metin: "Kişisel Verilerin Korunması Hukukunun Temel İlkeleri", Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, Yetkin Yayıncılık, Ankara 2022, s. 219-237.

KOTİL ÖĞRETMEN, Zeynep: Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka, On İki Levha Yayıncılık, İstanbul 2022.

KUNER, Christopher: European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, 2. Baskı, Oxford 2007.

KUNER, Christopher/ BYGRAVE, Lee A./ DOCKSEY, Christopher: The EU General Data Protection Regulation: A Commentary, Oxford University Press, Oxford 2021.

LAZARO, Christophe/ LE METAYER, Daniel: "Control Over Personal Data: True Remedy of Fairy Tale", SCRIPTed: A Journal of Law, Technology and Society, C. 12, S. 1, 2015, https://scripted.org/wp-content/uploads/2015/06/lazaro_metayer.pdf?d=11192022. (E. T. 10.06.2024)

LLOYD-JONES, Heledd/ CAREY, Peter (Edt. CAREY, Peter): "The Rights of Individuals", Data Protection A practical Guide to UK and EU Law, 5. Baskı, Oxford University Press, Oxford 2018, s. 122-154.

MACMILLAN, Mac (Edt. USTARAN, Eduardo): "Data Protection Concepts", European Data Protection Law and Practice, 3. Baskı, IAPP Publication, 2023, s. 81-105.

NARBAY, Şafak/ KİRAZLI, Şerife Nur: "Otonom Araçlarda Yapay Zeka, Kişisel Verilerin İşlenmesi ve Sonuçları", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, C. 11, S. 1, Sakarya 2023, s. 49-66.

OĞUZ, Sefer: "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi Ekonomisi ve Yönetimi Dergisi, C. 12, S. 3, Ankara 2018, s. 121-138.

ÖZDEMİR, Hayrunnisa: Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayınevi, Ankara 2009.

ÖZER DENİZ, Miray: Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, On İki Levha Yayınları, İstanbul 2022.

ÖZGÜL, Nurullah: "İnsan Haklarının Korunması ve Geliştirilmesinde Yeni Bir Sorun Alanı: Algoritmik Profilleme", Türkiye İnsan Hakları ve Eşitlik Kurumu Akademik Dergisi, C. 5, S. 9, s. 83-115.

ÖZKAN, Oğulcan: Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara 2020.

PEKMEZ, Cüneyt: "Overview of the Definitions of Data Controller and Data Processor within the Scope of The Turkish Code of Personal

Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, S. 67, İstanbul 2019, s. 59-71.

PERSANO, Federica: "GDPR and Children Rights in EU Data Protection Law", European Journal of Privacy Law & Technologies, C. 11, Özel Sayı, Torino 2020, s. 32-42.

PETKOVA, Bilyana/ BOEHM, Franziska (Edt. SELINGER, Evan/ POLONETSKY, Jules/ TENE, Omer): "Profiling and the Essence of the Right to Data Protection", The Cambridge Handbook of Consumer Privacy, Cambridge University Press, Cambridge 2018 s. 285-300.

TAŞTAN, Furkan Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, On İki Levha Yayınları, İstanbul 2017.

TEKİNOĞLU, Dilara: Kişisel Verilerin Korunması Hukuku Açısından Mobil Uygulamalarda Konum Gizliliği, On İki Levha Yayıncılık, İstanbul 2021.

TURGUT BİLGİÇ, Ezgi: "Genel Veri Koruma İlkelerinin Yapay Zekâ Karşısında Uygulanabilirliği Sorunu", Türkiye Adalet Akademisi Dergisi, S. 57, Ankara 2024, s. 247-282.

WELFARE, Damien/ CAREY, Peter (Edt. CAREY, Peter): "Territorial Scope and Terminology", Data Protection A practical Guide to UK and EU Law, 5. Baskı, Oxford University Press, Oxford 2018, s. 1-31.

YÜCEDAĞ, Nafiye: "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi, C. 1, S. 1, Ankara 2019, s. 47-63.

YÜKSEL, Armağan Ebru: "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakış", TAAD, C. 13, S. 51, Ankara 2022, s. 19-46.