BÜYÜK VERİ VE MOBİL UYGULAMALARDA İŞLENEN KİŞİSEL VERİLERİN (SAĞLIK VERİLERİ) HUKUKA UYGUNLUK SORUNU

Legal Challenges on Personal Data (Health Data) Processing through Big Data and Mobile Apps

Dr. Öğr. Üyesi Merve Ayşegül KULULAR İBRAHİM*
Av. Elife Filiz GÖKDAŞ**

Öz: Dijital varlıkların mirası konusu ve mobil uygulamalar aracılığıyla kişisel verilerin işlenmesi hususu özellikle pandemi dönemindeki uygulamalar nedeniyle endişeleri artırmıştır. Kamu sağlığının korunmasındaki üstün yarar gereği yaygınlaşan hassas kişisel veri kategorisi içinde yer alan sağlık verilerinin işlenmesi güncel tartışmalar arasında yer almaktadır. Ancak bu verilerin, büyük veri analizi ile pazarlanarak üçüncü taraflara aktarılması ve bu eylemlerden elde edilen kazanca yönelik hukuki tartışmalar yok denecek kadar azdır. Bu minvalde; bu çalışmada iPhone üreticisi Apple'ın iOS 15.2 güncellemesi ile gündeme gelen büyük veri analizi, büyük veri analisti şirketlerin kişisel sağlık verilerini analiz etmesi, büyük ver analizi kullanılarak geliştirilen uygulamaların kişilik haklarına yönelik riskleri ve bu uygulamaların KVKK ve TMK 23, 24, 25. maddeleri bağlamında hukuka aykırılık oluşturup oluşturmadığı tartışılacaktır. Çalışmanın amacı, vasi atama bildirimi örneği üzerinden büyük verinin hukuken değerlendirmesini yaparak toplumda büyük veri ve kişisel verilere dair duyarlılık uyandırmaktır. Bu bağlamda çalışmada öncelikle büyük veri tanımlanmış, ardından kişisel verilerin büyük veri kapsamında nasıl kullanıldığı tartışılmıştır. Özellikle hassas veri kategorisinde yer alan sağlık verilerinin işlenme şartları değerlendirilmiş ve büyük veri analizinde açık rıza olmaksızın nasıl sağlık verilerinin işlenebildiği detaylı şekilde analiz edilmiştir. Sonuç olarak sağlık verilerinin anonimleştirilerek büyük veri analizinde kullanımının şirketlere kazanç sağlarken diğer taraftan kişilerin özel hayatın gizliliği ve kişisel verilerin korunması hakkını ihlal etme riski taşıdığı ortaya konmuştur.
Anahtar Kelimeler: Özel Nitelikli Kişisel Veriler, Sağlık Verileri, Büyük Veri

Abstract: The issue of inheritance of digital assets and the processing of personal data through mobile applications have increased concerns, especially due to applications during the pandemic period. Processing of health data which is a type of sensitive personal data has become widespread for protection of public health. However, there are almost no legal discussions regarding the transfer of health data to third parties by marketing them with big data analysis and the profit obtained data marketing. In this study, big data analyst companies that came to the fore with iPhone manufacturer Apple's iOS 15.2 update, will be to clarify whether companies analyze personal health data constitute a violation of the personal data protection law and the civil law in the context articles 23, 24, 25 of the Turkish Civil Code. This study discusses the example of guardian appointment notification sent by Apple to patients to illustrate legal challenges triggered by big data. The aim of the study is to raise awareness in the society about legal evaluation of big data considering processing health data. In this context, the study first defines big data and then discusses how personal data is used within the scope of big data. It also evaluates the processing criteria of health data which is categorised as sensitive personal data. It questions how health data could be processed without explicit consent in big data analysis. As a result, this work illustrates the anonymisation of health data and the use of it in big data analysis brings profit to companies. On the other hand, this work lifts the lid on processing health data without explicit consent in the concept of big data analysis carries the crucial risk of violating people's right to privacy and the right to protection of personal data.
Keywords: Sensitive Personal Data, Health Data, Big Data

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi, aysegul.kulular@asbu.edu.tr, ORCID: 0000-0001-6556-0269.

** Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Öğrencisi, elifefiliz.gokdas@student.asbu.edu.tr, ORCID: 0009-0009-5194-6916.

Makale Geliş Tarihi: 04.12.2023, Makale Kabul Tarihi: 21.03.2024

DOI : 10.57083/adaletdergisi.1484072

GİRİŞ

Teknolojik gelişmeler, insan hayatının neredeyse mütemmim cüzü haline gelmiştir. İnternet kullanımının artması ile birlikte, internet üzerinde paylaşılan bilgi ve kişisel veri de artmış, bu verilerin teknoloji devi şirketler tarafından kullanılarak katma değer sağlandığı büyük veri analizine talepler yoğunlaşmıştır. Bireylerin özellikle sosyal medya üzerinden paylaştığı kişisel verilerle beğeni kazanma yahut gelir elde etme amacı güderken aslında paylaştığı verilerin istemediği şekillerde kullanılabileceği hususu gözden kaçırılan önemli bir konudur. Teknolojinin getirebileceği zararlar düşünülmemekte yahut gelir elde etme gayesi ile dikkate alınmamaktadır. Teknoloji kullanılarak yapılan her işlemde veri üretilmektedir. Bu veriler, veri sahibinin bilgisi ve izni olmaksızın başkaları tarafından ele geçirilip kaydedilebilmekte ve kullanılabilmektedir.

İlk kez 2005 yılında O'Reilly Media'da pazar araştırması direktörü olan Roger Magoulas tarafından "geleneksel ticari istihbarat (business intelligence) metodları ile artık yönetilmesi ve işlenmesi neredeyse imkansız olan çok büyük veri kümelerini tanımlamak üzere kullanılmış olan "büyük veri" terimi,[1] değere dönüştürülmesi için belirli teknoloji ve analitik yöntemler gerektiren yüksek hacim, (Volume) hız (Velocity) ve çeşitlilik (Variety) ile karakterize edilen bilgi varlığı şeklinde tanımlanabilir.[2] Kişilerin rızası ve haberi dâhi olmaksızın işlenen kişisel verileri kullanılarak büyük veri analizi ile yeni ve anlamlı veriler üretilebilmektedir. Bu durum, veri sahibi kişilerin, kendi kişisel verileri üzerindeki kontrolü kaybettiklerini göstermektedir.

Kontrolsüz şekilde kişisel verilerin işlenmesini ve muhtemel riskleri önlemek için akıllı telefonlar ve özellikle mobil uygulamalar aracılığıyla işlenen kişisel verilerin ve kişilik haklarının ayrıntılı bir şekilde düzenlenmesi ve korunması gerekmektedir. Zira büyük veriyi kullanan işletmeler, mobil uygulamalar kullanarak kişisel verileri, işlenebilir hale getirip satarak gelir elde etmekte ve kâr amacı ile kişilerin hakları çatıştığında kendi menfaatlerine ağırlık vermektedir. Pandemi dönemi, şirketlerin kâr artırma amacıyla mobil uygulama kullanıcılarının sağlık verilerini, bu uygulamalar aracılığıyla işleyip, depoladıkları ve bu verileri kullanarak, yurtiçine ve yurtdışına aktardıkları bu şekilde aslında kamu sağlığının korunması için getirilen istisnai düzenlemeyi hükmün amacına aykırı olarak maddi gelir sağlamak amacıyla kullandıkları önemli bir örnek durumdur. Konuyla ilgili Kişisel Verilerin Korunması Kurulu'nun 02.08.2018 tarihli kararı da önemlidir. Hakeri ve Söğüt'ün COVID-19 döneminde sağlık verilerinin işlenmesine yönelik çalışmasında vurguladığı üzere Kurul bu kararında, tedavi sürecinde hekim tarafından, veri sorumlusuna ait bir mobil

---

[1] C. Ganeshkumar / Jeganathan Gomathi Sankar / Arokiaraj David, "Adoption of Big Data Analytics: Determinants and Performances Among Food Industries", C.14, S. 1, 2023, International Journal of Business Intelligence Research, s. 1, 2.

[2] Monerah Al-Mekhlal / Amir Ali Khwaja, "A Synthesis of Big Data Definition and Characteristics", 2019, IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), s. 314.

uygulamadan sağlık raporunun ekran görüntüsünün başka bir cihaz ile çekilip internette ve sosyal medyada paylaşılması nedeniyle veri sorumlusuna idari para cezası uygulanmasına karar vermiştir.[3]

Pandemi gibi kamu sağlığını tehdit eden bir durumun söz konusu olmadığı normal şartlarda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 5. maddesi uyarınca kişisel veriler yalnızca ilgili kişinin ki bu çalışmada veri sahibi olarak anılmaktadır, açık rızası alınması suretiyle işlenebilmektedir. Kişilerin sağlık verileri ise özel nitelikli kişisel veri olarak nitelendiğinden hassas kişisel verilerin işlenme şartlarına yönelik KVKK 6. maddesi kapsamında düzenlendiği üzere veri sahibinin açık rızası ile işlenebilmektedir. Hassas kişisel verilerin ve hassas olmayan kişisel verilerin işlenmesinde temel şart aynı olup veri sahibinin açık rızasının bulunmasıdır.[4] KVKK 5. ve 6. maddesi arasındaki ayrım hassas kişisel verilerin açık rıza olmaksızın işlenebileceği istisnai durumların düzenlenmesindedir. Nitekim kişisel verilerin, sahibinin açık rızası olmaksızın işlenebildiği istisnai durumlar farklıdır. Yalnızca "kanunda açıkça öngörülen haller" hassas olan veya olmayan kişisel verilerin sahibinin açık rızası olmaksızın işlenebildiği ortak istisnadır. Ancak sağlık verisi bu kapsamda değildir. Dolayısıyla sağlık verisinin "kanunda açıkça öngörülen hallerde" dâhi veri sahibinin açık rızası olmaksızın işlenmesi hukuka aykırıdır. Zira sağlık verisinin işlenmesi, ancak veri sahibinin açık rızası alınmışsa hukuka uygundur. Bununla birlikte sağlık verilerinin, veri sahibinin rızası olmaksızın işlenebildiği ve bunun hukuka aykırı olmadığı yalnızca bir istisnai durum düzenlenmiştir. KVKK 6. maddesinde düzenlenmiş olan söz konusu istisnaya göre kamu sağlığının korunması amacıyla veya söz konusu sağlık sorununa ilişkin teşhis veya tedavinin sağlanması için veya maddede sınırlı olarak belirtilen diğer durumlar için sağlık verisi ait olduğu kişinin açık rızası alınmaksızın işlenebilecektir. Bu istisnadan yararlanabilecek olanlar ise maddede sınırlı sayıda belirtildiği üzere sır saklama yükümlülüğü altında olanlar yahut yetkili kılınmış kurum veya kuruluşlardır.

Pandemi döneminde kamu sağlığının korunması amacıyla konulmuş olan bu istisna, hükmün amacının ötesinde uygulanmıştır. Çalışmada detaylı şekilde incelenmiş olan bu durum ile özellikle mobil uygulamaların kullanıcılarının sağlık verilerini hukuka aykırı olarak büyük veri analiziyle işlemeleri halinde oluşabilecek muhtemel riskler tartışılmıştır. Nitekim mobil uygulamalar aracılığıyla, sağlık ve tıbbi araştırma bağlamında nitelikli ve kaliteli verilerin toplanması, veri sahibinin açık rızası alınmak şartıyla, sağlık hizmetinin, teşhis ve tedavinin yahut yönetiminin iyileştirilmesi noktasında, çok önemli bir yere sahipken[5] veri sahibinin rızası alınmaksızın hukuka aykırı olarak sağlık verilerinin işlenip oluşan anlamlı veriye göre veri

---

[3] Hakan Hakeri / İpek Sevda Söğüt, "Tıp Hukuku Açısından Bulaşıcı Hastalıklar", C.1, S. 64, 2020, Adalet Dergisi, s. 78.

[4] Sinan Sami Akkurt, "Açık Rıza", Kişisel Verilerin Korunmasına Akademik Bakış, Çağlayan Aksoy P / Aksoy H C (Ed.), Arkadaş Basım, Ankara, 2023, s. 157, 158.

[5] Arzu Kurşun, "Büyük Veri ve Sağlık Hizmetlerinde Büyük Veri İşleme Araçları", C. 24, S. 4, 2021, Hacettepe Sağlık İdaresi Dergisi, s. 923.

sahibine yapılan bilgilendirme ile kişinin ruh ve vücut bütünlüğünün zarar görebileceği, en temel hakkı olan yaşam hakkının ihlal edilebileceği, bu çalışma ile ortaya konulmaktadır. Çalışma e-Nabız gibi sağlık verilerinin güncelliğinin sağlanması açısından faydalı uygulamaları değerlendirerek sağlık, tıbbi ve klinik araştırmalarda kullanılan eski veri yönetiminin yerini, büyük verinin almasıyla birlikte, sağlık verilerinin güvenliğinin ne kadar sağlanabildiğini sorgulamaktadır. Çalışmada, sağlık verilerini analiz ederek pazarlayan büyük veri analiz firmalarının ve Apple gibi teknoloji devi şirketlerin yeni uygulamalarının hassas kişisel verilerin işlenmesi bağlamında değerlendirilerek kişilik hakkı kapsamında özel hayatın gizliliğinin korunması hakkı ile kişisel verilerin korunması hakkının ihlal riskleri tartışılmaktadır. Çalışma ile mobil uygulamalar temelinde açık rızaları alınmaksızın sağlık verileri işlenilen kişilerin büyük veri analizi sonucu yaşam süresinin, muhtemel kalan ömrünün dâhi hesaplanabilirliği, bu hesaplamalar üzerinden kişiselleştirilmiş bildirimler gönderilebilirliği vurgulanmıştır.

I. KİŞİSEL VERİLERİN İŞLENMESİNDE GENEL İLKELER

Kişisel verilere ilişkin OECD'nin (Ekonomik Kalkınma ve İşbirliği Örgütü) 1980'de yayınladığı "Mahremiyetin Korunması ve Sınıraşırı Veri Akışına Dair Rehber İlkeler" başlıklı metninde; GDPR ile KVKK ile uyumlu şekildeki genel veri işleme ilkelerine yer verilmektedir.[6] Söz konusu ilkelere benzer olarak 2016/679 sayılı Avrupa Birliği Tüzüğü olan Genel Veri Koruma Tüzüğü'nde (GDPR)[7] ve KVKK'de kişisel verilerin işlenmesinde uyulması gereken ilkeler düzenlenmiştir. Bunlara ilaveten 2709 sayılı Türkiye Cumhuriyeti Anayasası'nın (Anayasa) 20. maddesine eklenen

---

[6] Murat Volkan Dülger, "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", C. 1, S. 2, 2015, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, s. 47, 48; OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (s.e.t. 29.12.2022)

[7] Genel Veri Koruma Tüzüğü şeklinde Türkçe ifade edilen düzenlemenin ismi Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" şeklindedir. Söz konusu düzenlemenin tam metni için bakınız: Official Journal of the European Union, Eur-Lex, "General Data Protection Regulation" https://eur-lex.europa.eu/eli/reg/2016/679/oj (s.e.t. 03.11.2023) Söz konusu tüzükte ayrıca unutulma hakkı düzenlenmiş olup unutulma hakkının özel hayatın gizliliğinin korunması işlevi gördüğüne ilişkin detaylı bilgi için bakınız: Sinan Sami Akkurt, "17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"", C. 65, S. 4, 2016, Ankara Üniversitesi Hukuk Fakültesi Dergisi, s. 2622; Furkan Balaban / Merve Ayşegül Kulular İbrahim, "Sosyal Medya Ve Unutulma Hakkı: Meta Threads Örneği", C. 5, S. 2, 2023, Bilişim Hukuku Dergisi, s. 287 vd.

hüküm uyarınca kişisel verilerin korunması Anayasa ile güvence altına alınmıştır.

Kişisel verilerin korunmasına yönelik gerek Anayasa bağlamında gerek özel kanunlar bağlamında ve gerekse doğrudan KVKK bağlamında düzenlemeler yapılmış olması, bunların korunmaya değer ve önemli veriler olduğunu gösteren işaretlerdir. Teknolojinin kullanımı hemen hemen her defasında veri üretmektedir. Bu veriler kişilerin şahsına ilişkin çok fazla ayrıntılı bilgi içerebilmektedir. Özellikle sosyal medya üzerinden yapılan paylaşımlarda bir kişinin Instagram, Twitter ya da Facebook sayfasında bizzat kendisinin yer verdiği bilgilerini, ancak gelişmiş bir istihbarat ekibinin çok titiz incelemeleri neticesinde elde edebileceği bilinmektedir. Nitekim Instagram, Twitter (yeni ismiyle "X") ya da Facebook, Threads gibi sosyal medya platformları[8] veri paylaşanın konum bilgisi, ekonomik işlem bilgileri gibi oldukça fazla hacimdeki verisine erişerek anlık olarak veri sahibinin nerede, kim ile olduğuna ve hatta anlık olarak ne düşündüğüne dair verileri toplayabilmekte ve işleyebilmektedir. Sosyal medya platformları bu şekilde büyük veri analizlerini, kişilere "daha iyi hizmet sunmak için"[9] yaptıklarını iddia etmektedir. Ancak bu durum tartışmalıdır. Zira kişilere daha iyi hizmet sunulması için kişilerin kişilik hakkı bağlamında korunan temel değerlerinin ve temel haklarının[10] ihlaline neden olan bir metod kullanılması hukuka ve hakkaniyete aykırıdır. Kişisel veriler yalnızca sosyal medya platformlarınca değil ayrıca gerek kamu kurumlarında özellikle mesai takip sistemlerinde gerekse özel kuruluşların 'güvenlik amacıyla' olduğunu iddia ettikleri giriş ve çıkışlarında vatandaşların ve tüketicilerin görüntüleri işlenmekte ve hatta birçok kurumda biyometrik verilerin toplanıp işlendiği görülmektedir. İşyerlerine giriş-çıkış saatlerinin tespit edilebilmesi yahut işyeri içerisinde kişinin hareketlerinin takip edilmesi amacı kişisel verilerin işlenmesiyle gerçekleştirilebileceği halde kişisel veriler değil hassas kişisel veri olan biyometrik veriler kullanılarak gerçekleştiriliyorsa KVKK 4/2-(ç) ve (d) hükümlerine aykırılık söz konusudur. Nitekim bu hükümlerde, kişisel verinin işlendiği amaçla bağlantılılık, sınırlılık ve ölçülülük ilkelerine uygun işlenmesi gerektiği belirtilmiştir.[11] Bu durumda mesai takibi amacı biyometrik veriler kullanılmadan da gerçekleştirilebileceği halde biyometrik verilerin işlenmesiyle gerçekleştirildiğinde veri işleme ilkelerine aykırılık söz konusu olacaktır. Bu minvalde; gerek devletin ve kamu kurumlarının gerekse özel teşebbüslerin günden güne daha da gelişen, yaygınlaşan ve çeşitlenen araçlarla topladıkları kişisel verilerle hassas kişisel verilerin, daha

---

8 Sosyal medya platformları, internet aktörlerinin tanımlandığı 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 sayılı Kanun) kapsamında belirtilen şartları taşımaları durumunda "sosyal ağ sağlayıcı" olarak nitelendirilmektedir.

9 Facebook "Kullanım Koşulları" içerisinde yer alan söz konusu iddia için bakınız: Help Centre, "Terms of Use",
https://www.facebook.com/help/instagram/581066165581870 (s.e.t. 18.12.2022).

10 Sinan Sami Akkurt, Sosyal Medyada Gerçekleşen İhlâller Karşısında Kişilik Hakkının Korunması, Seçkin, Ankara, 2019, s. 29, 30.

11 Balaban ve Kulular İbrahim, 2023, s. 7.

sonra hangi ortamlarda, hangi kişiler tarafından ve ne amaçla, ne kadar süre ve ne tür işlemlerde kullanıldığı, kimlerle paylaşıldığı gibi sorular özellikle veri işleme ilkelerine aykırılık olup olmadığı dikkate alınarak sorgulanmalıdır.[12] Birçok kişi, gerçekten gerekli olup olmadığını sorgulamadan ve meydana getirebileceği tehlikeleri dikkate almadan, kişisel verilerini gönüllü olarak farkında olmadan paylaşmaktadır. Örneğin; günlük alışverişinde herhangi bir market yahut mağaza indiriminden yararlanmak için niçin mağaza kartı yahut mağazaya üyelik şartı konulduğu hakkında düşünen ve endişelenenlerin sayısı oldukça azdır.[13] Bununla birlikte tüketici verileri gerek çevrimdışı işlemlerde gerekse çevrim içi işlemlerde ve özellikle sosyal medyada işletmeler tarafından toplanmakta bu bağlamda sosyal medya bir pazarlama aracı şeklinde kullanılmaktadır.[14] Kişisel veriler her türlü kanuni düzenlemeye rağmen söz konusu örneklerde açıklandığı üzere hâlâ korumasız bir durumdadır ve bu korumasızlığın meydana getirebileceği sorunlara karşı, hâlâ yeterli ölçüde farkındalık bulunmamaktadır.

II. ÖZEL NİTELİKLİ KİŞİSEL VERİ OLARAK SAĞLIK VERİLERİ

Kişisel veriler içerisinde kendine özgü özellikleri ve barındırdıkları etki ve riskler dolayısıyla ayrı bir sınıfta kategorilendirilen ve çok daha ileri düzeyde denetlenen özel nitelikli kişisel veriler (hassas veri) bulunmaktadır.[15] KVKK. m.6/ I hükmünde özel nitelikli kişisel veriler sınırlı sayıda olacak şekilde belirtilmiştir. KVKK'da belirtilen hassas kişisel veriler örnek niteliğinde olmayıp sınırlı sayıdadır. KVKK 6. maddede belirtilenlerle sınırlandırılmış olan hassas kişisel veriler, hem özel hayatın gizliliği hem de diğer kişiler tarafından öğrenildiklerinde ayrımcılığa ve mağduriyete sebebiyet verebilecekleri endişesiyle hassas olmayan kişisel verilere kıyasla daha sıkı bir denetimle daha sıkı şekilde korunmaktadır.[16]

Sağlık verileri, hassas veriler olarak KVKK bağlamında özel nitelikli kişisel veriler arasında sınıflandırılmıştır ve yüksek düzeyde koruma gerektirmektedir. Kişilerin sağlık verileri, yalnızca hastalığın gelişimi, tedavisi, ruhsal bozukluklar, röntgen sonuçları ve muayene sonuçları ile sınırlı değildir. Tüm bunlarla birlikte; kişinin sağlık verileri kullanılarak tercih ettiği hastane veya tedavi yöntemine ödediği ücret dikkate alındığında sosyo-ekonomik düzeyine ilişkin verisine, genetiğin etkili olduğu hastalıklarla ilgili aile üyelerinin hassas kişisel verilerine de erişilebileceği ve

---

[12] Elif Küzeci, "Anayasal Bir Hak: Kişisel Verilerin Korunması", S. 128, 2011, Bilişim Dergisi, s. 143.

[13] Küzeci, 2011, s. 145.

[14] Sinan Sami Akkurt, "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Hâlinde Ortaya Çıkacak Cezaî Sorumluluğa Medenî Hukuk Bağlamında Bir Bakış", C. 25, S. 2, 2017, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, s. 332, 333.

[15] Elif Polat, "Sağlıkta Kişisel Veriler; Etik, Hukuk ve Günümüz Uygulamalar", https://pharmaino.com/saglikta-kisisel-veriler-etik-hukuk-ve-gunumuz-uygulamalar/ (s.e.t. 28.12.2022).

[16] Polat, 2022. Dülger, 2015, s. 51.

bu hassas verilerin hukuka aykırı işlenebileceği durumlar dikkate alınmalıdır. Hastalar hem hekime hem de sağlık kurumuna, tedavi süreci gereği, kendileriyle ilgili çok fazla bilgi vermektedir. Sağlık sektöründe teknolojinin gelişmesi, hastaların sağlık verilerinin elektronik ortamlarda saklanmaya başlanmasını beraberinde getirmiştir. Dijital ortamda büyük veri kullanılarak sağlık hizmetinin iyileştirilmesi için oldukça büyük hacimdeki sağlık verilerinden başlıcaları; hastaların kimlik bilgileri, biyometrik verileri, randevu vakitleri ile hasta geçmişi olarak adlandırılan geçmişteki sağlık sorunlarına, bunların tespitinde kullanılan tahlil ve görüntülemelere, bu görüntülerin radyoloji yorumlamalarına, tanı ve tedavi yöntemlerine dair sağlık bilgileridir.[17]

Elektronik sağlık kayıtlarının sağladığı pek çok yarar bulunmaktadır. Örneğin; zamandan tasarruf etme, verimliliği artırma, kayıtların okunaklılığını sağlama, tıbbi hata yahut malpraktis nedeniyle oluşan zararları en aza indirgeme, verilere daha hızlı erişim sağlayabilme, daha fazla veriye daha hızlı erişim sağlayarak daha doğru tespit ve değerlendirmede bulunabilme, bu değerlendirmeye dayanarak muhtemel riskleri öngörebilme, tedavi ve bakım sürecinin sonuçlarını ölçebilme, bunların birlikte sonucu olarak sağlıkta tanı, teşhis, tedavi ve bakım kalitesini artırma, hasta kayıtlarının kaybolma riskinin ortadan kaldırma, pahalı testlerin tekrar alınmasının önüne geçme, mevcut kayıtlara ulaşılarak hayati durumlarda ilgili hasta bilgilerine ulaşabilme ve hastayı etkin şekilde izleyebilme, sağlık verilerinin işlenmesindeki başlıca faydalardır. Somutlaştırmak gerekirse; örneğin hastanın alerjisi olan maddelerin ve buna dair hasta öyküsünün bilinmesi, özellikle hastanın bilincinin kapalı olarak hastaneye ulaştırıldığı acil durumlarda oldukça büyük önem arz etmekte olduğundan doğru teşhis için kişilerin en mahrem sağlık bilgileri dâhil her türlü sağlık verisi kaydedilmektedir.[18]

Elektronik sağlık kayıtlarının, yukarıda bahsi geçen bütün yararlarının yanında, hastaların bu kayıtların gizli kalmasını isteme hakkı bulunmaktadır; çünkü bireylerin sağlık durumlarına dair söz konusu veriler, hassas verilerdir ve bu hassas veriler, hastaların mağduriyetine ya da ayrımcılığa maruz kalmalarına neden olma riski taşımaktadır.[19]

Sağlık verilerinin özel hayatın gizliliği hakkıyla ilgisine dair Hasta Hakları Yönetmeliği'nin 21. maddesi önem arz etmektedir. Buna göre hastanın sağlığına ilişkin her türlü verinin, muayenenin, değerlendirmenin, teşhisin, sağlık harcamalarının ve tedavinin hasta mahremiyetine saygı

---

[17] Kurşun, 2021, s. 923; Ertuğrul Aktan, "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu" C. 1, S.1, 2018, Bilgi Yönetimi Dergisi, s. 6; Berna Terzioğlu Bebitoğlu / Hilal İlbars, "Kişisel Verilerin Klinik Araştırmalarda Kullanımına İlişkin Yasal Düzenlemeler", C. 25, S.1, 2020, Anatolian Clinic the Journal of Medical Sciences s. 67.

[18] Polat, 2022; Küzeci, 2011, s. 143; Dülger, 2015, s. 72; Pervin Somer, "Tıbbi Kayıtlar", 2010, Barosu III. Sağlık Hukuku Kurultayı, Ankara, 2010, s. 549. http://copy.ankarabarosu.org.tr/Siteler/2012yayin/2011sonrasikitap/3.saglik-hukuku-kurultayi-son.pdf (s.e.t. 30.12.2022); Nesrin Çobanoğlu, Kurumsal ve Uygulamalı Tıp Etiği, Efil Yayınevi Yayınları, Ankara, 2009, s. 153.

[19] Polat, 2022.

kapsamında gizli olarak yürütülmesi gerekmektedir. Bu düzenleme ile sağlık verilerini paylaşan hastanın hem sağlık verilerinin korunması hem de bu verilerin parçası olduğu özel hayatın gizliliğinin korunması hakkının ihlaline karşı her türlü önlemin alınması gerekmektedir. Söz konusu verilerin korunmasında süre hastanın ömrüyle sınırlı olmayıp "*Ölüm olayı, mahremiyetin bozulması hakkını vermez."* şeklinde açıkça hükme bağlandığı üzere hasta verilerinin açıklanmaması hasta öldükten sonra da mahremiyetine saygı gösterilerek verilerin saklanması yahut işlenmesine gerek kalmadığı durumlarda imhası gerekmektedir. Hastane gibi kamusal alanlarda gerçekleşen işlem veya davranışlar dolayısıyla elde edilen veriler kullanılarak kişilik hakkının zarara uğratılması mümkündür.[20] Bu nedenle hem hastanın mahremiyet hakkının hem de hasta yakınlarının mahremiyet hakkının hastanın ölümünden etkilenerek ölüm olayı ile sona ermesi söz konusu değildir.

Tedavi yönteminin belirlenmesi ve tedavinin başarılı şekilde sonuçlanabilmesi için hasta en mahrem verileri dâhil sağlık verilerini paylaşmak durumundadır. Hastanın mahrem verilerini paylaşması sağlık çalışanları tarafından talep edilebileceği gibi bu şekilde bir talep olmaksızın hastanın rahat davranışları ile verilerini paylaşması da mümkündür. Bu şekilde hastanın sakınmayarak tedavi sürecinin etkin gerçekleşeceğine inandığı mahrem verilerini sağlık çalışanı talep etmeksizin paylaşmış olması hastanın özel hayatın gizliliği hakkından feragat ettiği anlamına gelmemelidir. Akkurt bu konuda, veri sahibinin mahrem verilerini paylaşımı hususunda sakınmaması yahut rahat davranışlarda bulunmasının 'mahremiyetten vazgeçme' şeklinde değerlendirilemeyeceğini belirtmiştir.[21]

Bununla birlikte hastanın paylaşmasında yarar olmayan verilerinin hastadan talep edilmemesi gerekmektedir. Hassas kişisel verilerden olan sağlık verilerinin hastanın hastalığıyla ve tedavisiyle ilgili olmayan sağlık verilerini de kapsayacak şekilde hastadan alınması ve kullanılması durumunda bu verilerin hukuka aykırı işlendiği kabul edilmelidir. Zira hassas verilerin işlenmesinde göz önünde bulundurulması önem arz eden bir sınırlama nedeni "minimumluk ilkesi" *(principle of minimality)*dir. Bu ilkenin önemi ise toplanan kişisel verileri, amaçlarını gerçekleştirmek için zorunlu olduğu kadarıyla sınırlı olarak işlenmeyi gerektirmesinden kaynaklanmaktadır.[22] Minimumluk ilkesi gözetilerek yalnızca hastalığın teşhis ve tedavisinde gerekli olan veriler alınmalı ve işlenmeli, bunun dışında hastalıkla bağlantılı olmayan diğer sağlık verilerinin kullanılması durumunda KVKK'de belirtilen amaçla bağlantılı, sınırlı ve ölçülü olma ilkeleri gibi veri işleme ilkelerinin ihlal edildiği ve veri işleme faaliyetinin hukuka aykırı olduğu kabul edilmelidir.

---

[20] Sinan Sami Akkurt, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", C. 2, S. 1, 2020, Kişisel Verileri Koruma Dergisi, s. 26.

[21] Akkurt, 2019, s. 63.

[22] Cemil Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", C. LXIX, S.1-2, 2011, İÜHFM, s. 324; Dülger, 2015, s. 54.

III. BÜYÜK VERİ (BİG DATA) KAVRAMI

"Büyük veri" (big data) terimi, NASA'da araştırmacı olarak yer alan Michael ve David isimlerindeki kişilerin yazdığı; ana belleğin, yerel diskin ve hatta uzak diskin kapasitesini zorlayacak derecede büyük veri kümelerinin bulunduğu, bunların görselleştirilmesinin oldukça güç olduğu ve bu durumun "büyük veri problemi" olarak adlandırılabileceğini belirttikleri çalışmada yer almıştır.[23] İnternette kullanılan hesaplar arası etkileşimler, arama motorlarına yazılan kelime veya kelime grupları yahut arama motorlarında kullanılan görseller, arama sonucunda ziyaret edilen siteler ve sitelerde gerçekleştirilen işlemler, yapılan alışverişler gibi çerezler[24] vasıtasıyla toplanan veriler yahut veri parçacıkları, ödemelere dair kart bilgileri ve ilişkili diğer bilgiler ve kullanıcılar ile internet arasında gerçekleşen tüm etkileşimlerin oluşturduğu veri yığınlarından büyük veri beslenmektedir. Büyük veri, bu verileri işleyip bu verilerden çeşitli analizler yaparak veri sahiplerinin kendilerinin dâhi haberdar olmadıkları yeni bilgilere ulaşabilmekte ve bunları ticari olarak pazarlanmak üzere gruplayabilmektedir. Birçok veri noktası karşılaştırılarak ve birbirleriyle veri ilişkileri belirginleştirilerek, veri ilişkilerinin öğrenilmesi ve daha iyi kararlar alınması olanaklı hale gelmektedir. Toplanan verilere dayalı modeller oluşturulmakta ve bilişim teknolojileri kullanılarak oluşturulan simülasyonlar verinin elde edildiği kişinin kendisinin dâhi bilmediği farklı kişisel verilerini gösterebilmektedir. Veri noktalarının konumu her değiştirildiğinde, sonuçların nasıl etkilendiği simülasyonlar üzerinden açık olarak izlenebilmektedir. Eskiden, veriler veritabanı (database) ile sınırlı ve çok düzenli olduğundan bunların analiz ve takibi büyük veride kullanılan yöntemlerden daha basit metotlar kullanılarak yapılabilmiştir. Ancak özellikle sosyal medya kullanımının artması, internetin yaygınlaşmasıyla veriler hacimsel olarak önceki veri tabanlarına oranla ciddi ölçüde artmıştır. Bunların klasik veri analizi yöntemleriyle analiz edilmesi mümkün olmamış ve veri kavramı çok karmaşık bir yapıya dönüştüğünden bu karmaşık yapıdaki ciddi hacimsel verileri analiz ederek anlamlı sonuçlar oluşturabilecek farklı yöntemler gerekmiştir. Bu bağlamda *"genellikle, geleneksel istatistiksel yöntemlerin yanı sıra daha yenilikçi analitik araçlar kullanarak verilerin toplanmasına ve matematiksel olarak analiz edilmesine yardımcı olan yeni bir teknoloji"*[25] olarak büyük veri kullanılmaktadır. Özellikle sağlık alanında büyük veri yatırımları neticesinde yalnızca sağlık çalışanları değil aynı zamanda hastalar da kendi sağlık süreçlerini takip edebilmekte ve yapay zeka, nesnelerin interneti veya karmaşık algoritmalar kullanılarak büyük veri analizleriyle yenilikçi yöntemler, hem önleyici tıbbın gelişimine

---

[23] Michael Cox / David Ellsworth, "Application-Controlled Demand Paging for Out-of-Core Visualization", 1997, IEEE Visualization, s. 235.

[24] İnternet sunucusu tarafından kullanıcıya ilişkin verilerin ele geçirilerek bir internet tarayıcısında saklanmak üzere gönderilen küçük bilgi parçası şeklinde tanımlanabilen çerezler kullanıcıların kişisel verilerini kullanarak kullanıcı mahremiyetini ihlal etme riski taşımaktadır. Furkan Balaban, Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2023, s. 112.

[25] Balaban, 2023, s. 247.

katkı sunmakta hem de hastaneler gibi sağlık kuruluşlarının iş yükünün azalmasını sağlamaktadır.[26] Veriler büyük veri kullanılarak belirli kategorilerde sınıflandırılabilmekte ve bu şekilde hasta profilinin büyük veri analiziyle anlamlı sonuçlarının olduğu yeni veriler doğrultusunda tedavi yöntemi belirlenebilmektedir. Bu durum, işletmelerin müşteri profili analizi doğrultusunda stratejilerini belirlemelerini sağladığından[27] sağlık hizmeti veren işletmeler için de önemli faydalar sunmaktadır.

IV. KİŞİSEL VERİLERİN KORUNMASI VE ÖZEL HAYATIN GİZİLİLİĞİNİN KORUNMASI HAKLARI: LEANDER – İSVEÇ KARARI

Anayasal bir hak olan özel hayatın gizliliğinin korunması hakkı temel haklardan olup bilişim teknolojilerinin gelişmesiyle birlikte oluşan risk, tehdit ve tehlikeler nedeniyle zarara uğrama ihtimali artmış olan kişilerin korunması için getirilen "dördüncü kuşak haklar" içerisinde yer almaktadır.[28] Kişilerin devletler tarafından gözlenmesi sorununun insanın eşsiz ve biricik olmasına ilişkin "kişiliğinin" geliştirilmesine engel olması nedeniyle demokratik devletlerin bireylerin kişiliğini geliştirmeleri için özel düzenlemeler kabul etmesi gerekmiştir. Türkiye Cumhuriyeti Anayasası'nda da 2010 yılında yapılan değişiklik ile özel hayatın gizliliğinin korunması hakkının düzenlendiği 20. maddede kişisel veriler Anayasa ile güvence altına alınmıştır. Bu şekilde kişisel verilerin, sadece yetkili kişilerce ve sadece meşru amaçlarla işlenmesi amaçlanmaktadır.[29]

Konuyla ilgili Avrupa İnsan Hakları Mahkemesi'nin (AİHM) Leander / İsveç Davası önem arz etmektedir. 1985 tarihli bu davada İsveç vatandaşı Torsten Leander AİHM'e başvurarak İsveç'in Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesini ihlal ettiğini iddia etmiş, ayrıca AİHS'nin 10. ve 13. maddelerinin ihlal edildiğine yönelik şikayetinin de incelenmesi gerekmiştir. Söz konusu dava sonucu verilen karar; temelde, kişisel verilerin toplanması ve saklanmasına ilişkindir. Başvurucu, 20.08.1979 tarihinde müze teknisyeni pozisyonunda 10 aylık bir süre için işe başlamış olduğu İsveç'in Karlskrona bölgesindeki Deniz Müzesi'nin Karlskrona Deniz Üssü'nün bitişiğinde bulunuyor olması ve Karlskrona Deniz Üssü'nün askeri güvenlik bölgesi olarak nitelendirilmesi, başvurucunun çalışmakta olduğu müzenin de bazı binalarının bu bölge içinde yer alması nedeniyle Deniz Kuvvetleri Komutanlığı'nın haiz olduğu gizli veriler için öngörülmüş olan güvenlik

---

[26] Balaban, 2023, s. 247.

[27] Beste Ekin, "Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri", Yayınlanmamış Yüksek Lisans Tezi, İhsan Doğramacı Bilkent Üniversitesi, 2020, s.92. http://repository.bilkent.edu.tr/bitstream/handle/11693/54879/10372944_.pdf?sequence=1&isAllowed=y (s.e.t. 25.12.2022); Büşra Sarıkaya, "Big Data ve Kişisel Verilerin Korunması", Hukuk ve Bilişim Dergisi https://hukukvebilisim.org/big-data/ (s.e.t. 13.12.2022).

[28] Bayram Doğan, Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, Adalet Yayınevi, Ankara, 2023, s. 26.

[29] Küzeci, 2011, s. 145.

kontrolü için gerekli güvenlik önlemini geçemediği gerekçesiyle işten çıkarılmıştır. Bu minvalde; 3 Eylül 1979 tarihinde, işten çıkarıldığına yönelik kendisine bildirimde bulunulmuştur. Bildirimde, 1969 yılı Personel Kontrol Yönetmeliği gereği, kendisinin bahsi geçen pozisyona uygun olmadığı belirtilmiştir. Başvurucu, hükümete şikâyette bulunmuştur. Şikayetinde, Deniz Kuvvetleri Komutanlığı'nın değerlendirmesinin iptal edilmesini ve Deniz Müzesi'nde işe alınmama nedenlerinin kendisine bildirilmesini talep etmiştir. Ayrıca Başvurucu, Avrupa İnsan Hakları Sözleşmesi (AİHS) 8. maddesinin[30] ihlal edildiği iddiasında bulunmuştur. İddiasında bu tür bilgilerin saklanmasının ve açıklanmasının, AİHS 8(1) maddesinde düzenlenen özel hayata saygı hakkına müdahale oluşturduğunu ileri sürmüştür. Ancak başvuru reddedilmiştir. Ret kararında gerekçe olarak Personel Kontrol Yönetmeliği madde 13 bağlamında, Başvurucu'nun siciline ilişkin bilgilendirilmesine yönelik özel bir hususun olmadığı belirtilmiştir. Karara konu olayda, başvurucunun Deniz Kuvvetleri Komutanlığı'ndaki gizli bilgileri kullanılmış; ancak kendisine söz konusu bilgilerin içeriği hakkında bilgilendirme yapılmamıştır. Söz konusu bilgiler yüzünden işine son verilmiş olmasına rağmen, işlem iptal edilmediği ve özel hayatın gizliliği ihlal edildiği için başvuruda bulunulmuştur. AİHM tarafından yapılan tespit; başvurucuya uygulanan kişisel kontrolün, ulusal mevzuata uygun olarak yapıldığı yönündedir. Şöyle ki; İsveç personel kontrol sisteminin amacı, ulusal güvenliğin korunmasıdır. Bu sebeple; Sözleşme'nin "özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinin amaçları açısından meşru olduğu kabul edilmiştir. Nitekim AİHS 8. maddesinde düzenlenmiş olan özel hayatın gizliliğinin korunması hakkına kamu makamının müdahale edebileceği istisnai durumlar aynı maddenin 2. fıkrasında belirtilmiştir. Bu durumlar arasında ulusal güvenliğin ve kamu güvenliğinin korunması da bulunmaktadır. Dolayısıyla somut olayda olduğu gibi AİHS 8. maddesine göre ulusal güvenliğin korunması amacıyla kamu makamlarının özel hayatın gizliliği hakkına müdahalede bulunması, aynı maddede belirtilen diğer unsurların da bulunması şartıyla, hukuka uygun kabul edilmektedir.[31]

Leander'in İsveç'e karşı açmış olduğu davadaki tartışmanın iki ana konusu bulunmaktadır. Bunlar; AİHS 8. maddenin istisnasını oluşturan durumlar için gerekli şartlardır. Bu şartlar; özel hayata müdahalenin "hukuka uygun" ve demokratik bir toplumda gerekli olup olmadığıdır. Bu minvalde; gizli Deniz Kuvvetleri Komutanlığı sicilinin, başvurucunun özel hayatıyla ilgili bilgileri içerdiği açıktır. Sözleşme'nin 8. maddesinin 2. fıkrasındaki

---

[30] European Court of Human Rights, "Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı", https://www.echr.coe.int/Documents/Guide_Art_8_TUR.pdf (s.e.t. 22.12.2022).

[31] European Court of Human Rights, "Case of Leander v. Sweden", https://hudoc.echr.coe.int/rus?i=001-57519 (s.e.t. 24.12.2022); KOIOS Kişisel Verilerin Korunması Hukuku Çalışma Grubu, "Avrupa İnsan Hakları Mahkemesi (26 Mart 1987, Başvuru No: 9248/81) Leander/İsveç Karar Özeti (Madde 8, 10 ve 13)" https://kisiselveriihlali.com/Anasayfa/wp-content/uploads/2021/11/Bay-Leander-Isvec-AIHM-Karar-Ozeti.pdf (s.e.t. 24.12.2022); Soner Sönmez, "Leander / İsveç Davası", https://sonersonmez.av.tr/kisisel-verilerin-korunmasi-kanunu/ (s.e.t. 24.12.2022).

"hukuka uygunluk" ibaresi gereği; müdahalenin, iç hukukta bir temele sahip olması gerekmektedir. Gizli Deniz Kuvvetleri Komutanlığı siciline bilgi girişi yapılabilmesinin şartları bulunmaktadır. Bu şartlar; bilgilerin, Deniz Kuvvetleri Komutanlığı teşkilatı için gerekli olması ve "ulusal güvenliğe karşı suçlar gibi suçları" önleme veya tespit etme amacına hizmet etmesidir. Mahkeme, bahsi geçen tüm bu hususları göz önünde bulundurarak bir değerlendirme yapmıştır. Değerlendirmesinde, İsveç Hukuku'nun vatandaşlara, personel kontrol sistemi altında bilgi toplama, kaydetme ve yayınlama hususunda, sorumlu makamlara tanınan takdir yetkisinin kapsamı ve kullanım şekli hakkında gerekli bilgiyi verdiğini ve açıklamayı yaptığını belirtmiştir. Bu sebeple; mahkeme, başvurucunun özel hayatına yapılan müdahalenin 8. madde dâhilinde hukuka uygun olduğuna hükmetmiştir. Burada anlatılmak istenen gereklilik kavramı, müdahalenin aciliyetini ve izlenen meşru amaçla orantılı olduğunu ifade etmektedir. devletin ulusal güvenliğini korumaya yönelik menfaati ile başvuranın özel hayatına saygı hakkındaki menfaatinin dengelenmesi gerekmiştir. Mahkeme kararında çatışan hakların dengelenmesinde ulusal güvenliğin korunmasına ağırlık vermiştir. Bu bağlamda İsveç ulusal mevzuatının, özel hayatın gizliliğini ihlal niteliği taşıyacak şekilde kişinin bilgilerin ulusal güvenlik söz konusu olduğunda kullanılabileceğine izin verdiği vurgulanmıştır. Devletin, ulusal güvenliğin korunması amacıyla kişinin yalnızca ilgili bilgilerinin toplanıp yayımlandığı belirtilmiştir. Mahkeme AİHS 8. maddesinin 2. fıkrası uyarınca kişinin "özel ve aile hayatına saygı hakkı"nın ihlal edilmediğine hükmetmiştir.[32]

Leander'in İsveç'e yöneltmiş olduğu dava, ayrı haklar olan ve bazı somut durumlarda üst üste gelebilen özel hayatın gizliliğinin korunması hakkı ile kişisel verilerin korunması haklarının birlikte değerlendirildiği durumların bir örneğini oluşturmaktadır. Özel hayatın gizliliğinin korunması hakkı ile kişisel verilerin korunması hakları birbirinden farklı haklardır; ancak bu hakların örtüştüğü durumlar olabilir. Özel hayatın gizliliğinin korunması hakkı ile kişisel verilerin korunması haklarının örtüştüğü durumlar olması bu hakların aynı haklar olduğunu göstermez. AİHS 8. maddesindeki düzenleme ile örtüşecek şekilde ülkemizde de Anayasa'nın 20. maddesinde ilk fıkrada özel hayatın gizliliğinin korunması hakkı düzenlenmiştir. Aynı maddede özel hayatın gizliliğinin korunması hakkı ile kişisel verilerin korunması hakkı ayrı haklar olarak ele alınmıştır. Anayasa 20. maddede kişisel verilerin korunması hakkı özel hayatın gizliliğinin korunması hakkının düzenlendiği 1. fıkradan bağımsız olarak 3. fıkrada düzenlenmiştir. Buna göre kişilerin kendileri ile ilgili verilerin korunmasını isteme hakkı bulunmaktadır. Kişisel verilerin işlenmesi veri ilgilisi yahut sahibi olarak ifade edilen kişisel verinin tanımladığı bireyin açık rızasının alınması ile mümkündür. Açık rıza alınarak kişisel verilerin işlenmesinin istisnalarının yasa ile öngörülmesi mümkündür. Anayasal güvence sağlanmış olan kişisel verilerin korunması hakkı bir temel haktır. Bu hakkın korunması kural, kanunlarda öngörülen hallerde sınırlanması ise

[32] European Court of Human Rights, "Case of Leander v. Sweden"; KOIOS Kişisel Verilerin Korunması Hukuku Çalışma Grubu; Sonmez.

istisnadır.[33] Kişisel verilerin işlenme şartları ve istisnaları KVKK'de açıkça belirtilmiştir. Bununla birlikte KVKK 28. maddesinde kişisel verilerin işlenmesine yönelik KVKK hükümlerinin uygulanmayacağı haller belirtilmiştir. KVKK 28/1-b hükmüne göre kişisel verilerin araştırma, planlama ve istatistik veya benzer bir amaç için anonimleştirilerek kullanılması halinde kişisel verilerin işlenmesine yönelik genel ilkelere ve kişisel verilerin korunmasına dair diğer yükümlülüklere tabi olunmayacağı belirtilmektedir.[34] Burada kişisel verilerin anonimleştirilerek hangi amaç ile kullanılmasının istisna kapsamında olduğu değerlendirilmelidir. Zira kanunda "araştırma, planlama ve istatistik gibi" amaçlarlar denilerek "gibi" ifadesinden anlaşıldığı üzere sınırlı sayıda amaç değil örnekseme yoluyla aktarılmış amaçlar bulunmaktadır. Bu madde, KVKK ile düzenlenmiş kişisel verilerin korunmasına ilişkin hiçbir hükümle bağlı olmaksızın anonimleştirilmiş kişisel verilerin birçok amaçla kullanılmasına imkan tanımaktadır. Bu nedenle özellikle veri analizi şirketleri büyük veri analizi ile birçok kişinin kişisel verisini bilgilendirme yapmaksızın ve rıza almaksızın işlemektedir. Büyük veri kapsamında kişisel verileri işleyen şirketler, bu işlemlerinin hukuka aykırı olmasını önlemek amacıyla rıza almadan ele geçirdikleri kişisel verileri anonimleştirme yoluna gitmektedir. Bir başka ifadeyle büyük veri analizinde şirketler KVKK'deki yükümlülüklerden kaçınmak için kişisel verileri anonimleştirerek işlemektedir. Söz konusu kişisel veriler birçok farklı kaynaklardan elde edilmektedir. Veri analizinde kullanılmak üzere kişisel verilerin ele geçirilmesinde birçok şirket yapay zeka kullanmaktadır. Bu veriler içerisinde özel nitelikli kişisel veriler niteliğini haiz sağlık verileri de bulunmaktadır. Sağlık kayıtları, tıbbi literatür, klinik araştırmalar, sigorta verileri, eczane kayıtları ve hastaların sosyal medya içerikleri gibi birbirinden farklı birçok kaynaktan yapay zeka kullanılarak özel nitelikli kişisel veriler toplanarak işlenmektedir.[35] Yapay zeka kişilerin sağlık verilerini çok çeşitli ortamlardan ele geçirmekte ve mobil uygulamalar da kişisel verilerin ele geçirildiği ortamlar arasında yer almaktadır.

---

[33] Küzeci, 2011, s. 146.

[34] Özellikle araştırmalarda kullanılan kişisel verilerin anonimleştirilmesine ilişkin bakınız: Araştırma Verileri Yönetimi Eğitim Portalı, "Verinin Anonimleştirilmesi", https://acikveri.ulakbim.gov.tr/acik-veri-acik-bilim/bolum-3-veri-isleme/3-4-verinin-anonimlestirilmesi/ (s.e.t. 17.02.2023).

[35] Merve Ayşegül Kulular İbrahim, "Legal Challenges of Artificial Intelligence in Healthcare", Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence, (Ed.) Muharrem Kılıç, Sezer Bozkuş, Kahyaoğlu, Springer Publishing, Singapore, 2023, s. 148.

Araştırma amacıyla işlense dâhi hastanın kimlik bilgilerinin hasta rızası alınmaksızın açıklanamayacağı yönünde görüşler için bakınız: Dülger, 2015, s. 71.

V. KİŞİSEL VERİLERİN İŞLENMESİNDE MOBİL UYGULAMALARIN YERİ

Mobil uygulamalar, kişisel verilerin ele geçirilmesinde kullanılan önemli ortamlar arasındadır. Mobil uygulamaların kullanımı artmıştır.[36] Büyük veriye yatırım yaparak, hedef kitle olarak belirledikleri tüketicilerin istek ve arzularına önem veren işletmeler, mobil uygulamaları kendi yarar ve kazanımları yönünde kullanmaya başlamışlardır. Bu sebeple; rekabette önde olmak isteyen işletmelerin, artık mobil dünyada bulunmaları vazgeçilmez bir unsurdur. Büyük veriye yatırım yapan işletmeler, mobil kullanıcılara erişebilmek amacıyla çeşitli yollara başvurmaktadırlar. Şöyle ki mobil uygulamaların, bildirim gönderme özelliği avantajı bulunmaktadır. Kullanıcılara erişmenin en ivedi ve kullanışlı yolu bildirimlerdir. Büyük veri analistleri, bildirimler sayesinde kullanıcılar ile ciddi oranlara varan etkileşime ulaşabilmektedirler. Büyük veri analistleri, gönderdikleri bildirimlerin, içerik ve zamanlamasını kişiye göre değiştirmektedirler. Uygulama içi bildirimler, kullanıcılara göre kurgulanmaktadır. Bildirimler, kullanıcıların işlem ve eylemlerine göre bilgilendirme, yardım ve öneri şeklinde gelmektedir. Mobil uygulamalar, çevrimdışı da çalışabilmesi yani kişilere çevrimdışı erişim fırsatı sunması sebebiyle de mobil kullanıcılar tarafından tercih edilmektedir. Ayrıca, mobil uygulamalar ile kişiselleştirilebilen ayarlar sayesinde, sunulan hizmet de kişiselleştirilebilmektedir. Mobil kullanıcıların kişisel zevk, istek ve ihtiyaçlarına göre, tercihleri değişiklik göstermektedir. Mobil uygulamalar, bu anlamda kullanıcıların istedikleri gibi kişiselleştirilebileceği sayısız nitelik ve özellikle donatılabileceği için özellikle büyük veriyi kullanan işletmelerin, hedef topluluklarına imtiyazlı ve öncelikli bir hizmet anlayışı sunmalarını sağlamaktadır. Mobil uygulama sahipleri, mobil uygulamalarını kullananların davranış niteliklerine bakarak ve takip ederek, onların merak, beğeni ve ilgi alanlarına yönelik içerikler sunmaktadır. Mobil uygulama sahipleri, kullanıcıların kişisel davranışlarının yanı sıra, coğrafi verilerini de dikkate alarak, konum ve zaman esaslı içerikler sunarak kullanıcıların kişisel bir deneyim yaşamalarına olanak sunmaktadır. Mobil uygulamalar, kullanıcıların verilerini indirdikleri cihazların hafızasında yerel olarak saklamaktadır. Bu uygulamaların, kullanıcıyı hatırlayan özelliği bulunmakta ve bu özellik sebebiyle, kullanıcılara daha ivedi ve rahat erişim sağlanmaktadır. Özellikle, mobil uygulamalar, kullanıcı alışkanlıklarını takip ederek, ilgili kişinin karşısına ilgili ürünü çıkarması sebebiyle, hem hizmet sağlayıcılar hem de büyük veriyi kullanan işletmeler açısından önemli bir noktada bulunmaktadır. Kullanıcılar, akıllı telefonlarına bir uygulama indirdiğinde, kurulum aşamasında uygulama, yüklenmekte olduğu cihazın birçok unsuruna erişim izni istemektedir. Bu izinler istenildiğinde, çoğu

[36] 2015 yılında yayımlanan mobil uygulamalarla ilgili çalışmada mobil uygulamalarla yapılan ödemelerin önceki yıla göre %2 arttığını ifade etmektedir. Tüketicilerin sürekli yanlarında bulundurdukları mobil cihazları üzerinden mobil uygulamalara anında erişebilmeleri mobil uygulama kullanım oranını artırmaktadır. Reyyan Daçe / Sinan Nardalı, "Markaların Mobil Uygulamalarının Satın Alma Eğilimi Üzerine Etkisi ve Starbucks Örneği", C. 4, S. 1, 2021, Journal of Business, Innovation and Governance, s. 13, 14.

zaman, hangi verinin nasıl kullanılacağına dair detaylı bir açıklama yapılmamaktadır. Uygulama izinlerinin sonradan kapatılabileceği bilgisi verilse de uygulamaların, bu hususa kısmen izin verdiği durumların bulunduğu, kullanıcıların bu külfete katlanmak durumunda kaldığı, kullanıcıların uygulamayı yüklerken kolaylıkla onaylayabildiği erişim izinlerini kaldırmak için oldukça karmaşık bir süreç izlemesi gerektiği görülmektedir. Esasen şüpheli görünen hiçbir uygulamayı, kullanıcıların telefonlarına kurmamaları gerekmektedir. Bu husus, günümüzde başlı başına bir tartışma konusu teşkil etmektedir. Bir uygulamanın, yalnızca tasarlandığı maksada yönelik izinleri istemesi gerekmektedir. Maksadı haricinde, daha çok izin talebinde bulunan uygulamaların, değişik hedefler için tasarlanmış olabileceğinin mutlaka göz önünde bulundurulması gerekmektedir. Mesela, kullanıcılar bir sosyal medya uygulamasını kullanmak istediklerinde; sosyal medya uygulamaları genellikle rehber, telefona gelen çağrılar, depolama ayarları, mesajlar, vücut sensörleri, mikrofon, kamera, konum ve galeri gibi öğelere erişim izni istemektedir. Kullanıcılar tarafından bu izinler verilmediğinde ise uygulama çalışmamaktadır. Bu uygulamaların, çalışabilmesi için ilgili ve gerekli olmayan öğelere, erişim izni istemesinin sebebinin, kişisel verilerin toplanarak büyük veri analizinde kullanılması ve bu şekilde tüketicilerin profillenerek hür iradelerinin yönlendirilebileceği düşünülmektedir. Tüketicilerin bu şekilde profillenerek bireysel tercihlerine göre kişiselleştirilmiş reklamlara maruz bırakılmaları, tüketimi ve şirketlerin kârını artırmaktadır. Öyle ki kişiselleştirilmiş reklamlar; kullanıcıları; kendi ilgi alanlarına ve zevklerine göre sunulan ve bazı durumlarda saldırgan satış yöntemi niteliğini haiz olan reklamlar vasıtasıyla kişisel ilgi alanı kapsamındaki ürünlere iyice bağımlı hale getirebilmektedir. Bu bağlamda mobil uygulamalardan elde edilen büyük veri, satıcıları kitlesel reklam yerine kişiselleştirilmiş reklam yatırımlarına yönelten önemli bir etken olarak ortaya çıkmaktadır.[37]

Kayaköy Taş'ın ifadesiyle *"sosyal medya araçları bağımlılık yapan maddeler gibi bireyleri etkilemektedir".*[38] Sosyal medya uygulamaları, arka planda kullanıcı verilerini toplayarak, ziyaret edilen siteleri öğrenebilmekte ve davranışsal profilleme yapabilmektedir. Kişisel verilerin ele geçirilmesinde ve toplanmasında kullanılan yaygın metodlardan biri ücretsiz mobil uygulamalardır. Bu uygulamalar, ücretsiz olmaları sebebiyle, çok sayıda kullanıcı tarafından indirilebilmektedir. Mobil uygulamalar kişisel verilere zarar vermeyecek şekilde ve özel hayatın gizliliğinin korunması hakkını ihlal etmeyecek şekilde tasarlanmış olsalar dâhi çok fazla kullanıcı tarafından indirilip tercih edildiğinde veri potansiyeli nedeniyle kar amacı güden şirketler tarafından sonraki güncellemede verilerin ticari amaçla kullanılabileceği hale getirilebilmektedir. Kullanıcılar ise güncellemenin

---

[37] Merve Ayşegül Kulular İbrahim, "Psikolojik Planlı Eskitme ve COVID-19 Pandemisinde Durum", C. 12, S. 47, 2021, Türkiye Adalet Akademisi Dergisi (TAAD), s. 398.

[38] Merve Kayaköy Taş, "Pazarlama İletişiminde Sosyal Medya Kullanımı: Sigorta Pazarına Bir Uygulama" Yayınlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s. 12.

detayları hakkında bilgilendirilmedikleri için mevcut mobil uygulamaya duydukları güven zedelenmeden kullanıma devam etmektedir. Bu bağlamda mevcut kullanıcısı belli bir kapasiteye ulaşmış uygulamaların veri analistlerince satın alınarak güncelleme yöntemiyle kişisel verilere ulaşılması, kullanıcıların profillenmesi, verilerinin büyük veri analizi ile elde edilen anlamlı sonuçlarının pazarlanması sıkça kullanılan bir yöntemdir. Aynı amaç için en baştan bir uygulama geliştirip, bu uygulamanın yaygın ve tercih edilebilir bir hale getirilmesi daha fazla zaman, emek ve maliyete mal olacağından bunun yerine yaygın bir şekilde kullanılmakta olan ücretsiz uygulamaların satın alınarak bu uygulamalar aracılığıyla, kişisel verilerin ele geçirilmesi tercih edilmektedir.[39]

Kişisel verilerin, mobil uyumlu web siteleri ve mobil uygulamalar aracılığıyla toplanmasındaki en önemli faktörlerden birisi de üçüncü kişi faktörüdür. Bahsi geçen üçüncü kişi faktörler; internet servis sağlayıcıları, istatistik büyük veri analistleri ve reklam verenler gibi oldukça farklı hizmet sunucu faktörlerdir. Özellikle, ücretsiz uygulamalardan da çeşitli yöntemler kullanılarak gelir elde edilebilmektedir. Bu bağlamda kullanıcının indirmek için herhangi bir ödeme yapması gerekmeyen ücretsiz mobil uygulamaların kullanıcılara amme hizmeti sundukları algısı bir yanılsamadan ibarettir. Zira uygulama içerisine entegre edilebilen reklamlar yahut uygulama kapsamında gösterilen sponsor verileri veya ortaklıktan para kazanma yahut da abonelik modeli gibi yöntemlerden birisini veya bazılarını seçerek, şirketler, ücretli uygulamadan elde edilebilecek karı veya daha fazlasını ücretsiz uygulamadan elde edebilmektedir.

Yüz okuma, parmak izi, kamera, mikrofon, GPS (Küresel Konumlandırma Sistemi), barometre, konum değişimi, sabit durma, yürüme, koşma, bilgisayarda çalışma, ovma, oturma, hareket yönü veya hareket hızı gibi algılayıcılardan sağlanan verileri baz alarak, kullanıcının bağımlılık, alışkanlık, etkinlik, eylem ve sağlık bilgilerine dair oldukça büyük hacimde ve farklı türden veriler elde edilmektedir. Bu veriler; alınarak, toplanarak, yönetilerek ve analiz edilerek, genellikle çerezler veya başkaca benzeri yazılımlar vasıtasıyla, kullanıcı davranışları esas alınarak bireyselleştirilmekte, pazarlama ve reklam hedefiyle, tekrar gerçek kullanıcıya takdim edilmekte ve önerilmektedir.[40] Bu şekilde ulaşılan kişisel veriler, kart bilgilerini, fotoğraf ve konum bilgilerini, harcama verilerinden

---

[39] İhsan Karlı / Sema Doğru / Yusuf Bahadır Doğru, "Akıllı Telefonların Uygulama İzinleri Üzerine Bir Farkındalık Çalışması", C. 9, S. 30, 2018, AJIT-e: Online Academic Journal of Information Technology,

https://dergipark.org.tr/tr/download/article-file/1113741 (s.e.t. 11.01.2023), s. 153; Baran Erdoğan, "Ücretsiz Uygulamalara Dikkat: Kişisel Verileriniz Hedef Olabilir", 2021 https://www.hurriyet.com.tr/teknoloji/ucretsiz-uygulamalara-dikkat-kisisel-verileriniz-hedef-olabilir-41782207 (s.e.t. 12.01.2023); Bekir Çelik, "Uygulamaların Mobil Uyumlu Sitelere Tercih Edilmesinin 4 Önemli Nedeni", 2018, https://blog.mobiroller.com/tr/uygulamalarin-mobil-uyumlu-sitelere-tercih-edilmesinin-4-onemli-nedeni/ (s.e.t. 10.01.2023); Polat, 2022.

[40] Faruk Çayır, "Pandemi Takip Uygulamaları Ve Kişisel Verilerin İzlenmesi Raporu" Alternatif Bilişim Derneği, 2020, https://ekitap.alternatifbilisim.org/pdf/covid19-pandemi-takip-uygulamalari-raporu.pdf (s.e.t. 13.01.2023).

sosyo-ekonomik duruma, eğitim kayıtlarına ve sağlık verilerine kadar her türlü veriyi kapsayabilmektedir.[41] Öyle ki akıllı telefonlardan elde edilen veriler kullanılarak bu cihaz kullanıcıların sigara içme, yemek yemeyi unutma yahut aşırı kahve tüketimi gibi sağlığa zararlı davranışları belirlenebilmektedir.[42]

Mobil uygulamalardan sağlık verileri elde edilebildiği gibi, doğrudan sağlık hizmeti sunmak amacıyla oluşturulan mobil uygulamalar da bulunmaktadır. Mobil sağlık uygulamaları ile kullanıcılar da kendi sağlık durumlarını kontrol ve takip edebilmektedir. Aynı zamanda mobil sağlık uygulaması sahipleri yahut uygulamanın izin verdiği çalışanları da kullanıcıların sağlık durumunu takip edebilmektedir. Bu şekilde takibi yapılan, izlenen ve analiz edilerek işlenen sağlık verileri, sağlık alanındaki çalışmaların ilerleyebilmesi için önemli bir yere sahiptir. Bu bağlamda istatistiksel veriler ve ilgili sağlık verilerinin birleşimi ile yeni tedavilerin belirlenmesine ve keşfedilmesine katkı sunulabileceği gibi erken teşhis yöntemlerinin geliştirilmesine de imkan sağlanmaktadır. Tüm bu çalışmalar yapılırken işlenmesi gereken sağlık verileri, hassas kişisel veriler kapsamında yer almaktadır. Bu nedenle özel nitelikli kişisel veriler olan sağlık verilerinin işlenmesinin daha katı denetime tabi tutulması gerekmektedir. KVKK 6. maddede açıkça belirtildiği üzere sağlık verilerinin, söz konusu veri sahibinin -ki bu veri sahibi genellikle hastadır- açık rızası olmaksızın işlenmesi yasaktır. Ayrıca sağlık verilerinin işlenebilmesi ancak Kurul tarafından belirlenen önlemlerin yeterli düzeyde alınması ile mümkündür.

Diğer taraftan sağlık verilerinin hastanın rızası olmaksızın istisnai hallerde işlenebileceği de KVKK 6. maddesinde düzenlenmiştir. Bu istisnai işleme için Kanuna göre ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacı bulunmalıdır. Mobil uygulama şirketleri ise kar amacı güden şirketler olup hastalar için sundukları hizmette Kanunda belirtilmiş olan kamu sağlığının korunması veya teşhis, tedavi gibi sağlık hizmetlerine ilişkin bir amacı değil gelir elde etme amacını haizdirler. Ayrıca bu istisnai olarak sayılan hallerde hastanın açık rızası olmaksızın sağlık verilerinin işlenebilmesi için sadece sır saklama yükümlülüğü altında bulunan kişiler veya bazı kurum ve kuruluşlar yetkili kılınmıştır. Buradan hareketle sağlık hizmeti sunan mobil uygulamalar geliştirip pazara sunan kâr amacı güden şirketlerin maddede geçen "yetkili kurum ve kuruluşlar"dan olması gerekmektedir. Dolayısıyla yetki için başvurmaksızın ve tarafına yetki verilmeksizin geliştirdiği sağlık uygulamasını doğrudan piyasaya süren, mobil uygulama şirketlerinin kullanıcılarının geçerli açık rızası olmaması durumunda sağlık verilerini işlemesi kişisel verilerin hukuka aykırı işlenmesi nedeniyle yasaya aykırıdır. Aksinin kabul edilmesi veri koruma hukuku içerisinde yapılan hassas veri ayrımına aykırıdır. Zira sağlık verilerinin, kapsam ve sınırları belirsiz

[41] Doğan, 2023, s.239.

[42] Ensar Arif Sağbaş / Serkan Ballı "Akıllı saat algılayıcıları ile insan hareketlerinin sınıflandırılması" C. 21, S. 3, 2017, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, s. 981.

amaçlar için ve kapsam ve sınırları belirsiz kişilerin yetkili olduğu kabul edilerek işlenmesine izin verilmesi veri koruma hukukunun temeli ile doğrudan çelişmektedir.[43]

Sağlık verilerinin anonim olarak işlenmesi durumunda ise söz konusu işleme faaliyetinin kişisel verilerin işlenmesi faaliyetinin kapsamından çıktığı iddia edilmektedir. Bu bağlamda hastaları profilleyerek ve bir hastaya ilişkin sağlık verilerini o hastanın adı yahut T.C. kimlik numarası gibi doğrudan hastayı niteleyecek şekilde tutmak yerine X hastası ya da 1. hasta gibi hasta kimliğini gizleyerek tutup işleme durumunda anonimleştirilen verinin işlenmekte olduğu ileri sürülmektedir. Hasta verilerinin anonimleştirilerek işlenmesinde kullanılan yöntemlerden bir başkası ise hastaları numaralandırmak yahut harflendirmek yerine belli profillere göre sınıflandırmaktır. Burada belli özelliklerdeki hastaların her biri o özellikler için açılmış bir klasör içerisinde değerlendirilebilmektedir. Bu bağlamda hasta verisinin doğrudan hastayı tanımlayacak şekilde tutulmayıp X klasöründeki veriler şeklinde tutularak işlendiği düşünülebilir. Bu şekilde büyük veri olarak kişisel veriler ve hassas kişisel veri olan sağlık verileri kullanılmakta, büyük miktarda sağlık verisi depolanabilmekte ve analiz edilebilmektedir. Söz konusu örneklerde belirtildiği şekilde yahut çok daha farklı anonimleştirme yöntemleri ile sağlık verileri anonimleştirildiği iddia edilerek artık kişisel veri olma niteliğini kaybettiği öne sürülerek veri sahibinin rızası alınmaksızın ve KVKK'nın ilgili hükümleri yerine getirilmeksizin büyük veri kapsamında analiz edilebilmekte ve bazı mobil uygulama sahiplerince istenildiği gibi işlenebilmektedir. Anonimleştirmeyi öne sürerek büyük veri analistleri, verilerin sahibine ulaşma imkânlarının olmadığı yönünde argüman sunabilmektedirler. Kişisel verilerin anonim hâle getirilmesi, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 10. maddesinde "*kişisel verilerin başka verilerle eşleştirilse dâhi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir*" şeklinde tanımlanmıştır. Tanımdan da açıkça anlaşıldığı üzere sağlık verilerinin anonim hale getirilmesi durumunda verilerin silinmesi yahut işlenemez hâle getirilmesi değil bilakis sağlık verisinin ait olduğu gerçek kişi ile bağının kesilerek işlenmeye devam edilmesi söz konusudur. Yönetmeliğin 10. maddesinin 2. fıkrasında her ne kadar anonimleştirilen verinin geri döndürme gibi teknikler kullanılarak gerçek kişiyle ilişkisinin yeniden kurulmaması gerektiği belirtilmiş olsa da İngilizcede "deanonymisation" şeklinde ifade edildiği üzere anonimleştirilen veri aslında anonimleştirme işleminin geri döndürülmesi gibi farklı teknikler kullanılarak veri sahibi ile yeniden ilişkilendirilebilmektedir. Bu bağlamda aslında veri ile verinin ait olduğu gerçek kişi arasındaki ilişkinin anonimleştirme yoluyla kesildiği iddia edilse dâhi genellikle mobil uygulama sahipleri istedikleri zaman söz konusu verinin ait olduğu kişi ile ilişkisini kurabilecek teknik donanımı da haizdir. Bu bağlamda gerekli teknik yapıyı haiz büyük veri şirketleri anonimleştirerek işleyip analiz edip kullandıkları sağlık verilerinin kime ait

[43] Ayşe Aslı Alçın, "Türk Hukukunda Kişisel Sağlık Verileri Ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü", C. 13, S. 51, 2022, Türkiye Adalet Akademisi Dergisi (TAAD), s. 381.

olduğunu tespit edebilmekte, söz konusu tespiti yapıp kullandıktan sonra veriyi yeniden anonim hâle getirebilmektedir. Bu prosedür büyük veri kullanılarak elde edilen gelir karşısında çok düşük maliyetli ve yapılması her an ihtimâl dâhilinde bir uygulamadır. Veriler, anonim hâle getirilse dâhi ilgili veri yığınlarına bağlantılar sağlanarak, kişileri tanımlamak mümkün olabilmektedir. Bu nedenle de verilerin anonimleştirilmesi hususu, tüm dünyada kişisel verilerin korunması hususunda tartışılmakta olan bir konudur.

Genellikle araştırma ve istatistik gibi hedeflerle tutulan ve bir gerçek kişiyle ilişkilendirilmekten ziyade, kitlesel bilgi kümesi olarak çıkan anonim sağlık verileri, kişilerle bağdaştırılamadığı için kişisel veri kapsamında kabul edilmediğinden KVKK bağlamında getirilen hiçbir yükümlülüğe tabi olunmaksızın rahatça işlenerek bilimsel çalışmalarda kullanılabildiği gibi ticari amaçla da pazarlanmaktadır. Mobil uygulamalar aracılığıyla, sağlık ve tıbbi araştırma bağlamında toplanan veriler, mevzuat uyarınca veri sahibinin açık rızası alınmak şartıyla, sağlık yönetimini iyileştirme ve sağlık araştırması amacı ile işlenebilmektedir. KVKK 28. maddesinde anonimleştirilen kişisel verilerin istatistik veya araştırma amacıyla işlenebileceği belirtilmiştir. KVKK 28 (1/b) maddesi gereği, veri sorumlusunun anonimleştirdiği sağlık verileri ile yalnızca bilimsel çalışma yapılabilmelidir. Verilerin, kanunda bahsi geçen amaçlar dışında ve bilimsel çalışma haricinde, özellikle pazarlama veya reklam gibi ticari amaçlar için işlenmesi, kullanılması veya ücret karşılığında paylaşılması hukuken yasaklanmıştır.

VI. MOBİL UYGULAMALAR ARACILIĞIYLA SAĞLIK VERİLERİNİN TOPLANMASI VE BÜYÜK VERİ ANALİZİ: APPLE ÖRNEĞİ

Apple yeni güncellemesi ile bir düzenleme getirerek "Apple Kimliğiniz için Vâris ekleme" başlıklı bir uygulama kullanmıştır. iPhone üreticisi Apple, iOS 15.2 işletim sisteminde Miras İrtibatı (Legacy Contact) adında bir düzenleme getirmiştir. Bu uygulama ile kullanıcıların, vefât etmesi halinde Apple kimliklerine erişmesini istedikleri kişiyi vâris olarak atayabilmeleri sağlanmıştır. Apple, daha önce yalnızca mahkeme kararı ile kişilerin vefâtından sonra, Apple kimliklerine erişime izin verdiğinden bu uygulama ile mahkeme kararı olmaksızın kullanıcının ölmeden önce Apple kimliğine vâris tayin etmesi amaçlanmıştır. Bu düzenleme ile kişiler vefât ettiğinde, vâris olarak atadıkları kişi, vefât eden kişilerin iPhone verilerine ve Apple kimliklerine erişebilmektedir. Sosyal medya şirketlerinin, kişilerin vefâtı durumunda hesaplarının sahipliğinin kime devrolacağı hususu üzerinde uzun bir süredir çalıştıkları bilinmektedir.

Kişilerin sağlık verilerinin işlenerek pazarlanması; kanser gibi ölümü yakın olan kullanıcıların tespit edilmesi, bu kullanıcıların ölümünden sonra, hesaplarına ulaşabilecek kişiyi tayin etmeleri için bildirim gönderilmesi gibi uygulamalara olanak tanımaktadır. Sağlık verilerinin büyük veri analitiği aracılığıyla, dış dünyanın erişimine açılabilirliğinin bu tür uygulamaları gündeme getirmesi, büyük veri güvenlik önlemlerinin yeterince alınamadığını somut olarak ortaya koymaktadır. Büyük veri kapsamında anonimleştirilerek işlenen özel nitelikli sağlık verileri ile tespit edilen ölmesi muhtemel görünen hesap sahibinin bizzat kendisine bildirim

gönderilebilmesi olası bir uygulamadır. Bu tür bir uygulama, söz konusu sağlık verisinin ilişkili olduğu hesap sahibinin tespit edilebildiğini göstermesi açısından önemlidir. Bir başka ifadeyle anonimleştirilerek işlenen sağlık verisine geri döndürme yahut başka teknikler uygulanarak sağlık verisinin ait olduğu gerçek kişi tespit edilebilmektedir. Bu şekilde sağlık verileri işlenerek belli bir zaman içerisinde ölmesi muhtemel görünen gerçek kişiye bildirim gönderilebilmesi mümkün olmaktadır. Apple'ın, yeni getirdiği bu vasi atama uygulamasının ilgili herkese bildirim gönderilmesi yerine sadece, bu büyük veri analizleri sonucunda, ölümü yakın olduğu düşünülen kişilere vasi atama bildiriminin gönderilmesi şeklinde uygulanma ihtimâli ve bunun hastalar üzerindeki muhtemel etkileri dikkate alınmalıdır. Burada sorgulanan husus şirketlerin bir kişinin ölümünün yakın olduğunu nasıl bilebildiğidir. Zira kişinin belki kendisinin dâhi durumdan haberdar olmadığı ancak en temel haklardan olan yaşam hakkını etkileyecek bu derece hassas kişisel sağlık verilerinden uygulama sahibi teknoloji şirketlerinin haberdar olabilmesi ve kişilerin ömrüne göre kişiselleştirilmiş bildirimler gönderebilmesi veri anonimizasyonunun kişisel verilerin korunmasındaki işlevini yerine getiremediğini göstermektedir.

Apple'ın Miras İrtibatı şeklindeki uygulaması ile amaçlanan özellikle anıların yahut önemli verilerin ölen kişinin mirasçılarına aktarılmasında kolaylık sağlanmasıdır. Ayrıca ölen kişinin söz konusu verileri içerisinde ekonomik değer taşıyan dijital varlıklarının da miras yoluyla mirasçılara geçmesi gerekir.[44] Nitekim ölen kişinin ilgili hesaba kayıtlı verileri dijital miras kapsamındadır.[45] Bu bağlamda oldukça faydalı olabilecek nitelikteki bu tür uygulamaların kullanımında kişisel verilerin işlenmesindeki ilkelere uyumun sağlanması hususunda bir kanuni çerçevenin çizilmesi ve anonimleştirmenin kişisel verilerin korunmasında işlevsiz olabileceğinin göz ardı edilmemesi gerekmektedir. Aksi halde her bir bireyin ne kadar ömrü kaldığının takriben belirlenebilmesi ve bunun teknoloji şirketleri tarafından kullanılabilmesi olağan bir durum hâline gelebilecektir.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in 4. maddesinde kişisel verilerin işlenmesi tanımlanmış olup bu tanıma göre kişisel veriler kullanılarak yapılan her türlü işlem kişisel verilerin işlenmesini oluşturmaktadır. Bu bağlamda mobil uygulamalarda veya internet sitelerinde kişisel verilerin toplanması, saklanması, birleştirilmesi, açıklanması, erişilebilir kılınması, uyarlanması, yayılması, üçüncü kişilerle paylaşılması, kombinasyonu veya ilişkilendirilmesi şeklinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesi olarak kabul edilmektedir. Görüldüğü üzere; burada kişisel verinin, veri sahibinin açık rızası olmaksızın işlenmesi söz konusu olabilmektedir. Örneğin güncellemelere yönelik bir bildirim alan kişinin güncellemeyi yüklerken sağlık verilerinin işlenerek ölme riskinin tayin edilebileceği hakkında kapsamlı ve anlayabileceği şekilde detaylı

---

[44] Sinan Sami Akkurt, Dijital Varlıkların Miras Yoluyla Bırakılması, Seçkin, Ankara, 2022, s. 327.

[45] Dijital mirasın kapsamına giren unsurlar hakkında detaylı bilgi için bakınız: Akkurt, 2022, s. 22 vd.

bilgilendirilmesi sağlanmış olmalıdır. Güncellemeyi yükleyen kişinin vereceği rızanın sınırlarını ve sonuçlarını öngörerek ve kabul ederek, güncellemeyi reddetme seçeneği de bulunmasına rağmen hür iradesiyle kabul ederek açıkça rıza vermesi halinde veri işleme faaliyetinin hukuka uygun olduğu kabul edilmelidir. Aksi halde kişinin güncellemeyi indirmeyi kabul etmiş olması, sağlık verilerinin işlenmesine rıza göstermiş olması şeklinde değerlendirilemez. Nitekim ancak verisinin nasıl işleneceği hakkında yeterli düzeyde ve açıkça bilgilendirilerek serbest bir irade ile verilmiş rıza hukuken değeri olan bir rıza olarak kabul görebilir.[46] Zira rıza, tereddüte yer vermeyecek seviyedeki bir açıklık ile tereddüte yer vermeyen net bir irade beyanı ve aktif bir davranış ile ortaya konması halinde açık rıza niteliği kazanacaktır.[47] Bu bağlamda Oral'ın vurguladığı üzere Yargıtay da E. 1976/6297 K. 1977/2541 sayılı kararında rızanın geçerli kabul edilebilmesini bireyin gerektiği ölçüde aydınlatılmasına ve iradesini açıklarken baskı altında kalmamasına bağlamıştır.[48] Bu bağlamda güncelleştirmeyi reddetme seçeneği sunulmaksızın yalnızca kabul etme seçeneği sunulması durumunda kişinin iradesini serbestçe kullandığından bahsedilemeyecek, bilakis yalnızca kabul et seçeneği sunularak ve sürekli olarak güncelleme isteminin gönderilmesi kişinin iradesinin etki altında kalmasını sağladığından bu şekilde verilen güncelleme onayı geçerli bir rıza niteliğini haiz olamayacaktır. Dolayısıyla büyük veri analizi yapan şirketlerin kişilerin özel nitelikteki kişisel verilerinin işlenebilmesi için kanunda açık rıza şartı olmasına rağmen, rızaları alınmaksızın ve hiçbir istisnaya da girmemesine rağmen yasa dışı veri işleme faaliyetinde bulundukları durumlar olabilmektedir.[49]

Kişisel verilerin kimliğini belirli yahut belirlenebilir kıldıkları gerçek kişinin açık rızası alınmaksızın işlenmesi , KVKK bağlamında hukuka aykırılık teşkil etmekte olduğu gibi TMK 23 ve devamı maddeleri ile korunan kişilik haklarına da aykırılık teşkil etmektedir. Nitekim kişisel verilerin korunması hakkı bir kişilik hakkıdır.[50] Sağlık verileri bu bağlamda

---

[46] Merve Ayşegül Kulular İbrahim, "Rıza, Üstün Nitelikte Özel Ve Kamusal Yarar Bağlamında Hukuka Uygunluk Nedenleri", C. 9, S. 2, 2019, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, s. 317.

[47] Akkurt, 2023, s. 171, 172.

[48] Tuğçe Oral, "Hekimin Aydınlatma ve Hastanın Rızasını Alma Yükümü", S. 2, 2011, Ankara Barosu Dergisi, s.188.

[49] Polat, 2022. Hassas kişilerin işlenmesine yönelik olarak doktorun hastası hakkında işlediği sağlık verileri yahut çalışana ait sendikalılık bilgisinin özlük dosyasında mevzuat gereği tutulması gibi örneklerle ilgili olarak bakınız: KVKK, Özel Nitelikli Kişisel Verilerin İşlenme Şartları https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari (s.e.t. 15.02.2023).

[50] Merve Ayşegül Kulular İbrahim, "Protection of Privacy Against IT", The Palgrave Handbook of Global Social Problems, (Ed.) Rajendra Baikady ve diğerleri, Palgrave Macmillan, Cham, 2022, s. 8, 9; Esin Gürsel Düğmeci / Fatih Düğmeci, "Özel Hayatın Gizliliği Kapsamında Kişisel Verilerin Korunması Yöntemlerinden Biri Olarak Erişimin Engellenmesi" Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış, Cemil Kaya (Ed.), Oniki Levha Yayıncılık, İstanbul, 2023, s.305.

mahremiyet, şeref ve haysiyet gibi kişilik hakkı kapsamında korunan değerlerle sıkı bir ilişki içerisindedir.[51] Bu değerlerin korunması için mobil uygulamalarda işlenen kişisel verilerin de her türlü işleme faaliyetinde gerek hukuka gerek dürüstlük kuralına riayet edilerek işlenmesi gerekmektedir.[52] Kişisel verilerin bu şekilde hukuka uygun işlenebilmesi için kullanıcı anlayacağı şekilde sadelikte ve verilerinin işlenmesi sürecine dair her türlü gerekli bilgiyi içerecek şekilde aydınlatılmalıdır. Bu aydınlatma sonrasında kişisel veriler, kullanıcının rızasının kapsam ve sınırları çerçevesinde ve hukuka, ahlaka ve dürüstlük kurallarına aykırı olmayan meşru amaçlar doğrultusunda işlenmelidir. Bir başka ifadeyle, kişisel veriler işlendikleri amaç ile bağlantılı, sınırlı ve ölçülü olmalıdır. Amacın gerçekleştirilebilmesi için gerekli olmayan sağlık verilerinin işlenmesi, kanuna aykırılık teşkil etmektedir. Zira TMK'nın 24. maddesinin 2. fıkrasında açıkça görüleceği üzere, kişilik haklarına yapılan saldırıda hukuka aykırılığın giderilmesindeki hukuka uygunluk nedenleri; kişilik hakkı zedelenen kişinin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması şeklinde belirtilmiştir. Ancak çalışma konusu güncelleme örneğinde görüldüğü üzere, Apple'ın kişilerin sağlık verilerine erişerek, kanser gibi ölümü yakın olan kullanıcılara vasi atama uygulaması ile ilgili bildirim göndermesi, TMK'nın 24. maddesinde düzenlenen, hukuka uygunluk nedenleri kapsamında değerlendirilememektedir.

Sağlık verileri ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Verinin saklanmasına yönelik meşru amacın bulunmaması halinde ise ilgili veri kanuna göre silinmeli veya yok edilmelidir. Bunlardan biri yapılmak istenmiyorsa veri anonim hale getirilerek saklanmalıdır. Ancak burada anonim hale getirilmesi durumunun barındırdığı muhtemel riskler göze alındığında kişisel verilerin korunması için silinmesi yahut yok edilmesi gerektiği düşünülmektedir. Aksi halde kişilik haklarının TMK 24. maddede öngörülenin aksine dışarıdan gelen saldırılara karşı yeterli şekilde korunması mümkün olmayacaktır. Bu bağlamda, özellikle de sağlık verilerinin işlendiği somut örnek düşünüldüğünde kişisel verilerin anonimleştirilerek işlenmeye devam edilmesi kişilik hakkının, üçüncü kişilerden gelecek zararlara karşı korunamayacağını göstermektedir. Bu nedenle kişilik hakkının korunması için verilerin anonimleştirilmesi yeterli olmayıp silinmesi yahut yok edilmesi gereklidir. Bu nedenle mevcut mevzuatta yer alan KVKK 7.

---

[51] Sinan Sami Akkurt, "Kişisel Sağlık Verilerinin İşlenmesine ve Covid19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış", C. 19, S. 38 Covid-19 Hukuk Özel Sayısı, 2020, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, s. 146.

[52] Veri sorumlusunun kişisel verileri hukuka ve dürüstlük kuralına uygun işlemesi, Türk Medeni Kanunu'nda düzenlenmiş dürüstlük kuralından farklı olarak Kişisel Verilerin Korunası Kanunu'nca veri sorumlusuna getirilmiş bir yükümlülük olup veri sorumlusunun bu Kanun'dan doğan haklarını adil olarak kullanmasını ifade etmektedir. Mesut Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayili Kanun Çerçevesinde Kişisel Verilerin Korunmasi Hukuku, On İki Levha, İstanbul, 2020, s. 70. Bu şekilde veri sorumlusunun Kanun'dan doğan haklarını kullanarak veri ilgilisine zarar vermesinin önüne geçilmesi amaçlanmıştır.

maddesindeki "işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler ... silinir, yok edilir veya anonim hâle getirilir" ifadesi ve Yönetmelikte yer alan "kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin ... silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir" ifadesi yeniden ele alınarak anonimleştirmenin mevzuattan çıkarılması yahut veri güvenliği ve gizliliğini gerekli seviyede sağlayacak anonimleştirme metodlarının sınırlı sayıda belirlenerek mevzuatta belirtilmesi hem kişisel verilerin hem mahremiyetin hem de bu vesileyle kişilik haklarının korunması için önemli bir adım olacaktır.

SONUÇ

Yüksek hacimdeki (Volume) ve oldukça farklı çeşitteki (Variety) verini son derece hızlı (Velocity) şekilde gelişmiş teknolojiler vasıtasıyla işlenerek anlamlı yeni verilerin elde edilmesi ve bunların pazarlanması büyük veri çalışmaları kapsamında yapılmaktadır. Hemen her alanda olduğu gibi sağlık alanında da büyük veri, oldukça önem arz etmektedir. Büyük veri kullanımının tedavi sürecine ve sağlık hizmetlerine, hastaya ve sağlık çalışanlarına, sağlık kuruluşlarının iş yükünün hafifletilmesine sunduğu önemli katkılar bulunduğu gibi özellikle mobil uygulamalar aracılığıyla büyük veri analiz şirketleri tarafından, sağlık verileri işlenerek elde edilen yeni anlamlı bulgulara dair veriler pazarlanmakta ve kişilik haklarını ihlal eder nitelikte zararlı kullanımlar söz konusu olabilmektedir.

Mobil uygulamalar aracılığıyla, bireylerin kişisel verilerini, özellikle de kişisel sağlık verilerini analiz eden, büyük veri analiz firmaları, sağlık alanındaki çalışmaların geliştirilmesi amacı dışında gerek KVKK gerekse TMK bağlamında korunan ve Anayasa'da güvence altına alınan kişisel verilerin veya özel hayatın gizliliğinin korunması gibi kişilik haklarını ihlal edebilmektedir. Büyük veri analizi ile örneğin kanser gibi ölümü yakın olan bireylerin tespit edilebilmesi ve bu kişilere vefat ettikten sonra çeşitli uygulama hesaplarına ulaşabilecek kişiyi henüz vefat etmeden tayin edebilmeleri için bildirim gönderilebilmesi mümkündür. Hassas kişisel verilerin sınırlı sayıda belirtilerek işlenmesi için özel yükümlülükler öngörülmüş olmasına rağmen bu yükümlülüklerin yerine getirilmiş olup olmadığının denetimine ve yerine getirilmesi için gerekli önlemlerin alınmasına rağmen anonimleştirme unsuru neticesinde kişilerin bilgisi ve rızası olmaksızın verilerinin işlenmesi mümkündür. Toplumda herhangi bir kişinin takribi kalan ömrü yahut sağlık bilgilerine dayanarak ölme riski, kişinin kendisi veya yakın çevresinden önce ve hatta doktorundan önce büyük veri analizi yapan şirketlerce bilinebilmektedir. Özellikle sağlık sektöründe etik tartışmalarının güçlenmesi, kişisel verilerin işlenmesi ile özel hayatın gizliliğinin korunmasına yönelik mevzuattaki açıklıkların fark edilmesi ve toplumun bilinçlenmesine katkı sunmuştur. Ayrıca anonimleştirilerek "kişisel veri" niteliğini yitirdiği öne sürülen verilerin büyük veri bağlamında işlenmesindeki riskleri ve genel olarak anonimleştirme ile ortaya çıkabilecek sorunları göstermesi açısından da konu önemlidir. Kişilik hakları kapsamında kişisel verilerin ve özel hayatın gizliliğinin yeterli düzeyde korunabilmesi için mevzuatın gözden geçirilerek "anonimleştirme" konusundaki düzenlemelerin yeniden ele alınması ve

mümkün olduğu ölçüde daraltılması gerekmektedir. Düzenlemelerde bir değişiklik olmayıp anonimleştirilen verilerin işlenmesine devam edilmesi durumunda kişilik hakları ihlali devam edebileceğinden ihlalin önlenmesi için anonimleştirme metodları sınırlı sayıda belirtilmelidir. Bu bağlamda veri güvenliği ve gizliliğini tam olarak koruyucu homomorfik şifreleme gibi metodlar tek tek belirlenerek, bunların prototip uygulamaları geliştirilmelidir. Kişisel verileri anonimleştirmede homomorfik şifreleme gibi sınırlı sayıda metodun uygulanması zorunluluğu getirilmelidir.

KAYNAKÇA

Akkurt S S, "17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"", C. 65, S. 4, 2016, Ankara Üniversitesi Hukuk Fakültesi Dergisi, ss. 2605-2635.

Akkurt S S, "Açık Rıza", Kişisel Verilerin Korunmasına Akademik Bakış, Çağlayan Aksoy P / Aksoy H C (Ed.) Arkadaş Basım, Ankara, 2023, ss. 155-194.

Akkurt S S, Dijital Varlıkların Miras Yoluyla Bırakılması, Seçkin, Ankara, 2022.

Akkurt S S, "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Hâlinde Ortaya Çıkacak Cezaî Sorumluluğa Medenî Hukuk Bağlamında Bir Bakış", C. 25, S. 2, 2017, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, ss. 329-373.

Akkurt S S, "Kişisel Sağlık Verilerinin İşlenmesine ve Covid19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış", C. 19, S. 38 Covid-19 Hukuk Özel Sayısı, 2020, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, ss. 142-160.

Akkurt, S S, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", C. 2, S. 1, 2020, Kişisel Verileri Koruma Dergisi, ss. 20-32.

Akkurt S S, Sosyal Medyada Gerçekleşen İhlâller Karşısında Kişilik Hakkının Korunması, Seçkin, Ankara, 2019.

Aktan E, "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu" C. 1, S.1, 2018, Bilgi Yönetimi Dergisi, ss. 1-22.

Al-Mekhlal M / Khwaja A A, "A Synthesis of Big Data Definition and Characteristics", 2019, IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), ss. 314-322.

Alçın A A, "Türk Hukukunda Kişisel Sağlık Verileri Ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü", C. 13, S. 51, 2022, Türkiye Adalet Akademisi Dergisi (TAAD), ss. 365-410.

Araştırma Verileri Yönetimi Eğitim Portalı, "Verinin Anonimleştirilmesi". https://acikveri.ulakbim.gov.tr/acik-veri-acik-bilim/bolum-3-veri-isleme/3-4-verinin-anonimlestirilmesi/ (s.e.t. 17.02.2023).

Balaban F, Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara, 2023.

Balaban F / Kulular İbrahim M A, "Sosyal Medya Ve Unutulma Hakkı: Meta Threads Örneği", C. 5, S. 2, 2023, Bilişim Hukuku Dergisi, ss. 1-30.

Cox M / Ellsworth D, "Application-Controlled Demand Paging for Out-of-Core Visualization", 1997, IEEE Visualization, ss. 235-244.

Çayır F, "Pandemi Takip Uygulamaları Ve Kişisel Verilerin İzlenmesi Raporu", 2020, Alternatif Bilişim Derneği.

https://ekitap.alternatifbilisim.org/pdf/covid19-pandemi-takip-uygulamalari-raporu.pdf (s.e.t. 13.01.2023).

Çekin M S, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayili Kanun Çerçevesinde Kişisel Verilerin Korunmasi Hukuku, On İki Levha, İstanbul, 2020.

Çelik B, "Uygulamaların Mobil Uyumlu Sitelere Tercih Edilmesinin 4 Önemli Nedeni", 2018. https://blog.mobiroller.com/tr/uygulamalarin-mobil-uyumlu-sitelere-tercih-edilmesinin-4-onemli-nedeni/ (s.e.t. 10.01.2023).

Çobanoğlu N, Kurumsal ve Uygulamalı Tıp Etiği, Efil Yayınevi Yayınları, Ankara, 2009.

Daçe R / Nardalı, S, "Markaların Mobil Uygulamalarının Satın Alma Eğilimi Üzerine Etkisi ve Starbucks Örneği", C. 4, S. 1, 2021, Journal of Business, Innovation and Governance, ss. 12-26.

Doğan B, Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, Adalet Yayınevi, Ankara, 2023.

Dülger, M V, "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", C. 1, S. 2, 2015, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, ss. 43-80.

Ekin B, Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, Yayınlanmamış Yüksek Lisans Tezi, İhsan Doğramacı Bilkent Üniversitesi, Ankara, 2020.

Erdoğan B, "Ücretsiz Uygulamalara Dikkat: Kişisel Verileriniz Hedef Olabilir", 2021. https://www.hurriyet.com.tr/teknoloji/ucretsiz-uygulamalara-dikkat-kisisel-verileriniz-hedef-olabilir-41782207 (s.e.t. 12.01.2023).

European Court of Human Rights, "Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı". https://www.echr.coe.int/Documents/Guide_Art_8_TUR.pdf (s.e.t. 22.12.2022).

European Court of Human Rights, "Case of Leander v. Sweden". https://hudoc.echr.coe.int/rus?i=001-57519 (s.e.t. 24.12.2022).

Ganeshkumar C / Sankar J G / David A "Adoption of Big Data Analytics: Determinants and Performances Among Food Industries", C.14, S. 1, 2023, International Journal of Business Intelligence Research, ss.1-17.

Gürsel Düğmeci E / Düğmeci F, "Özel Hayatın Gizliliği Kapsamında Kişisel Verilerin Korunması Yöntemlerinden Biri Olarak Erişimin Engellenmesi" Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış, Kaya C (Ed.), Oniki Levha Yayıncılık, İstanbul, 2023, ss. 291-330.

Hakeri H / Söğüt İ S, "Tıp Hukuku Açısından Bulaşıcı Hastalıklar", C.1, S. 64, 2020, Adalet Dergisi, ss.57-85.

Help Centre, "Terms of Use". https://www.facebook.com/help/instagram/581066165581870 (s.e.t. 18.12.2022).

Karlı İ / Doğru S / Doğru Y B, "Akıllı Telefonların Uygulama İzinleri Üzerine Bir Farkındalık Çalışması", C. 9, S. 30, 2018, AJIT-E: Online Academic Journal of Information Technology. https://dergipark.org.tr/tr/download/article-file/1113741 (s.e.t. 11.01.2023).

Kaya C, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", C. LXIX, S.1-2, 2011, İÜHFM, ss. 317-334.

Kayaköy Taş M, Pazarlama İletişiminde Sosyal Medya Kullanımı: Sigorta Pazarına Bir Uygulama, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014.

KOIOS Kişisel Verilerin Korunması Hukuku Çalışma Grubu, "Avrupa İnsan Hakları Mahkemesi (26 Mart 1987, Başvuru No: 9248/81) Leander/İsveç Karar Özeti (Madde 8, 10 ve 13)". https://kisiselveriihlali.com/Anasayfa/wp-content/uploads/2021/11/Bay-Leander-Isvec-AIHM-Karar-Ozeti.pdf (s.e.t. 24.12.2022).

Kulular İbrahim M A, "Legal Challenges of Artificial Intelligence in Healthcare", Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence, Kılıç M / Bozkuş Kahyaoğlu S (Ed.) Springer Publishing, Singapore, 2023, ss. 147-160.

Kulular İbrahim M A, "Protection of Privacy Against IT", The Palgrave Handbook of Global Social Problems, Baikady R ve diğerleri (Ed.), Palgrave Macmillan, Cham, 2022.

Kulular İbrahim M A, "Psikolojik Planlı Eskitme ve COVID-19 Pandemisinde Durum", C. 12, S. 47, 2021, Türkiye Adalet Akademisi Dergisi (TAAD), ss. 391-406.

Kulular İbrahim M A, "Rıza, Üstün Nitelikte Özel Ve Kamusal Yarar Bağlamında Hukuka Uygunluk Nedenleri", C. 9, S. 2, 2019, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, ss. 305-333,

Kurşun A, "Büyük Veri ve Sağlık Hizmetlerinde Büyük Veri İşleme Araçları", C. 24, S. 4, 2021, Hacettepe Sağlık İdaresi Dergisi, ss. 921-940.

Küzeci E, "Anayasal Bir Hak: Kişisel Verilerin Korunması", S. 128, 2011, Bilişim Dergisi, ss. 142-149.

KVKK, Özel Nitelikli Kişisel Verilerin İşlenme Şartları. https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari (s.e.k. 15.02.2023).

OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (s.e.t. 29.12.2022).

Official Journal of the European Union, Eur-Lex, "General Data Protection Regulation". https://eur-lex.europa.eu/eli/reg/2016/679/oj (s.e.t. 03.11.2023).

Oral T, "Hekimin Aydınlatma ve Hastanın Rızasını Alma Yükümü", S. 2, 2011, Ankara Barosu Dergisi, ss. 185-209.

Polat E, "Sağlıkta Kişisel Veriler; Etik, Hukuk ve Günümüz Uygulamalar". https://pharmaino.com/saglikta-kisisel-veriler-etik-hukuk-ve-gunumuz-uygulamalar/ (s.e.t. 28.12.2022)

Sağbaş E A, / Ballı S, “Akıllı saat algılayıcıları ile insan hareketlerinin sınıflandırılması” C. 21, S. 3, 2017, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, ss. 980-990.

Sarıkaya B, “Big Data ve Kişisel Verilerin Korunması”, Hukuk ve Bilişim Dergisi. https://hukukvebilisim.org/big-data/ (s.e.t. 13.12.2022).

Somer P, “Tıbbi Kayıtlar”, 2010, Ankara Barosu III. Sağlık Hukuku Kurultayı, 2010.
http://copy.ankarabarosu.org.tr/Siteler/2012yayin/2011sonrasikitap/3.saglik-hukuku-kurultayi-son.pdf (s.e.t. 30.12.2022).

Sönmez S, “Leander / İsveç Davası”. https://sonersonmez.av.tr/kisisel-verilerin-korunmasi-kanunu/ (s.e.t. 24.12.2022).

Terzioğlu Bebitoğlu B / İlbars H, “Kişisel Verilerin Klinik Araştırmalarda Kullanımına İlişkin Yasal Düzenlemeler”, C. 25, S.1, 2020, Anatolian Clinic the Journal of Medical Sciences, ss. 66-72