T.C.
İSTANBUL MEDİPOL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİNİN VE AKTARILMASININ KARŞILAŞTIRMALI HUKUK AÇISINDAN İNCELENMESİ

UFUK İYİGÜN

SAĞLIK HUKUKU YÜKSEK LİSANS PROGRAMI

DANIŞMAN
Dr. Öğr. Üyesi. Esra ALAN

İSTANBUL-2023

T.C.
İSTANBUL MEDİPOL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİNİN VE AKTARILMASININ KARŞILAŞTIRMALI HUKUK AÇISINDAN İNCELENMESİ

UFUK İYİGÜN

SAĞLIK HUKUKU YÜKSEK LİSANS PROGRAMI

DANIŞMAN
Dr. Öğr. Üyesi. Esra ALAN

İSTANBUL-2023

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar tüm safhalarda etik dışı bir davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar çerçevesinde elde ettiğimi, bu tez çalışması ile elde edilen tüm bilgi ve yayınlara kaynak gösterdiğimi ve bu kaynakları kaynakçama koyduğumu, yine bu tez çalışmasında ve yazım aşamasında patent ve telif haklarını ihlal edecek bir davranışım olmadığını beyan ederim.

ÖNSÖZ

Kişisel veriler konusu, günümüzde hızla gelişen bilişim teknolojileri nedeniyle gündemde daha fazla yer edinmeye başlanmıştır. Bunun da en büyük nedeni kişilerin kendi verilerini kontrol edebilme çabası, bu kontrolün zayıfladığında meydana gelebilecek zararların yarattığı endişelerdir. Kişisel sağlık verileri ise bu verilerin daha hassas olan alt grubunu oluşturur. Bu verilerin korunması adına, gerek ülkemizde gerekse uluslararası mevzuatta sürekli yeni düzenlemeler yapılmaktadır. Sürecin dinamik yapısı, alandaki mevcut bilgiye hakim olmayı güçleştirmektedir. Uluslararası mevzuatın, özellikle Avrupa Veri Koruma Tüzüğü'nün bu alandaki öncü yapısı, ülkemizde uygulanmakta olan Kişisel Verilerin Korunması Kanununu da etkilemekte, bu bağlamda bu düzenlemelerin günden güne benzeşmeye başladığı görülmektedir. Bununla birlikte ülkemiz mevzuatında bu alanda henüz tamamlanmamış eksiklikler de vardır. Çalışmamızda, kişisel sağlık verileri özelinde olmak üzere bu farklılıkları incelemeye çalıştık.

Bu süreç boyunca, tez hazırlık ve yazım aşamasında desteklerinden sıklıkla yararlandığım başta tez danışmanım Dr. Öğr. Üyesi Esra Alan olmak üzere, engin bilgisinden, değerli katkılarından her zaman yararlandığım Prof. Dr. Fulya İlçin Gönenç, Prof. Dr. Gürkan Sert, Prof.Dr.Mehmet Akif İnanıcı, Prof.Dr.Ayşe Nuhoğlu, Doç.Dr. Hüseyin Melih Çakır hocalarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

DOKUZUNCU BÖLÜM

KİŞİSEL VERİLERİN AKTARILMASI

ONUNCU BÖLÜM

KİŞİSEL VERİ KORUMA KANUNU VE ULUSLARARASI VERİ KORUMA KANUNU KARŞILAŞTIRILMASI

KISALTMALAR

AB	:	Avrupa birliği
ABAD	:	Avrupa Birliği Adalet Divanı
AİHM	:	Avrupa İnsan Hakları Mahkemesi
AİHS	:	Avrupa İnsan Hakları Sözleşmesi
AK	:	Avrupa Konseyi
BŞK	:	Bağlayıcı Şirket Kuralları
GDPR	:	Avrupa Veri Koruma Tüzüğü
HHY	:	Hasta Hakları Yönetmeliği
KSVİMSY	:	Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik
KVKK	:	Kişisel Verilerin Korunması Kanunu
KVSYAY	:	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
OECD	:	Ekonomik İşbirliği ve Kalkınma Örgütü
VSSY	:	Veri Sorumluları Sicili Hakkında Yönetmelik
LGPD	:	Brazilian General Data Protection Law
CNIL	:	Fransa'nın veri koruma otoritesi

ÖZET

Kişisel veriler kavramı günlük hayatta, gittikçe artan bir şekilde karşımıza çıkmaktadır. Mevzuat düzenlemeleri, gelişen bilişim teknolojilerine ayak uydurmakta güçlük çekmektedir. Günümüzde bilginin yayılma hızı düşünüldüğünde kişilerin kendilerine ait veriyi korumaları, her geçen gün daha da zor bir hale gelmektedir. Kişisel sağlık verileri ise kişisel verilerin daha hassas korunması gereken bir alt koludur. Bu nedenle birçok ülke bu verilerin korunması için ek mevzuat düzenlemesi yapmakta, daha sıkı koruma ve denetleme mekanizmaları oluşturmaktadır. Her ne kadar Avrupa Birliği Genel Veri Koruma Tüzügü, tüm dünyada, gerek detaylı yapısı gerekse de pratiğe uygunluğu ve sürekli güncellenmesiyle ana mevzuat metni olarak kabul edilse ve düzenlemelerde yararlanılsa da, ülkesel ve bölgesel düzeyde bir takım farklılıklara rastlamak mümkündür. Ülkemizde yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu, içerik olarak ve uygulamasal olarak bir çok yönden Genel veri koruma tüzüğüne benzerlik gösterse de, bazı maddelerinin yeterli düzeyde detaylandırılmamış olmasından dolayı farklı yorumlara ve değerlendirmelere açık bir yapıdadır. Özellikle gelişen yapay zeka teknikleri kişisel sağlık verilerinin işlenmesi konusunu bazı durumlarda içinden çıkılması zor bir noktaya sürüklemiştir. Bu tür zorlukların gelecekte daha da artacağı öngörülmektedir. Kişisel sağlık verileri öncelikli olmak üzere tüm kişisel verilerin bilişim teknolojileri ile yayılması durumunda kişilerin zarar görmesini engellemek açısından unutulma hakkının kapsamı ve kullanılabilirliği farklı platformlarda tartışılmaktadır. Çalışmamızda bu çerçevede kanun ve uygulama farklılıkları değerlendirilmeye çalışılmıştır. Mevzuat düzenlemelerindeki bazı kavramsal farklılıklar ve bunların oluşturabileceği farklılıklara değinilmiştir. Bilişim teknolojilerindeki gelişime paralel olarak dünya çapında değişen mevzuatı takip etmek, ihlallerin oluşmasını azaltabilecek, kişilerin bu ihlallere bağlı zarar görmesini önleyebilecektir. Bu saiklerle çalışmamızda, kişisel sağlık verilerinin işlenmesi ve özellikle aktarımı konusunda KVKK ve tüzük düzenlemeleri temel alınarak, uluslararası hukuk temelinde karşılaştırma yapılmaya çalışılmıştır.

Anahtar Kelimeler: Kişisel Sağlık Verileri, Kişisel Verilerin İşlenmesi

ABSTRACT

The concept of personal data is increasingly used in daily life. Legislative regulations have difficulties in following up with the developing information technologies. Considering the speed of information spreading today, it is becoming more and more difficult for people to protect their own data. On the other hand, personal health data is a sub-branch of personal data that needs to be protected more sensitively. For this reason, many countries make additional legislative arrangements for the protection of this data, and establish stricter protection and control mechanisms. Although the General Data Protection Regulation of the European Union is accepted as the main legislative text and is used in regulations all over the world with its detailed structure, compatibility with practice and continuous updating, it is possible to encounter some differences at the national and regional level. Although the Law on the Protection of Personal Data No. 6698, which is in force in our country, is similar to the General Data Protection Regulation in many ways in terms of content and application, it is open to different interpretations and evaluations because some of its articles are not sufficiently detailed. Especially the developing artificial intelligence techniques have dragged the processing of personal health data to a difficult point in some cases. Such difficulties are expected to increase further in the future. The scope and usability of the right to be forgotten is discussed on different platforms in order to prevent people from being harmed in the event that all personal data, especially personal health data, are disseminated through information technologies. In our study, we tried to evaluate the differences in law and practice within this framework. Some conceptual differences in legislative arrangements and the differences that these may create are mentioned. In parallel with the developments in information technologies, following the changing legislation around the world will reduce the occurrence of violations and prevent people from being harmed due to these violations. With these motives, in our study, we tried to make a comparison on the basis of international law, based on the KVKK and General Data Protection Regulation regarding the processing and especially the transfer of personal health data.

Key Words: Personal Health Data, Personal Data Processing

GİRİŞ

Kişisel verilerin korunması kavramı, uzun süredir üzerinde çalışılan bir konu olmakla birlikte, bilişim teknolojilerinin akıl almaz bir hızda gelişmesiyle, kişisel verilere kolaylıkla ulaşılabilir olması bu alandaki çalışmaları arttırmıştır. Sağlık alanındaki kişisel verilerin daha hassas nitelikte veriler olması ve diğer kişisel veriler ile benzer riskler altında olması ise bu alanda önlem alınmasını ve yakın takibi zorunlu kılmaktadır. Ülkemizde bu alanda yasal düzenlemeler bir süredir yapılmaktadır. Henüz bu düzenlemelerin yeterli olduğunu söylemek ise mümkün değildir.

Avrupa Veri Koruma Tüzüğü(GDPR), dünya çapında şimdiye kadar yapılmış en teferruatlı kişisel veri koruma düzenlemesidir. Birçok ülke, işleyişi kolaylaştırmak ve uluslararası uygulamalarda senkronizasyonu sağlamak adına, bu düzenlemeyi temel alarak kanuni düzenlemeler yapmaktadır. Bununla birlikte ülkeler özelinde bir takım farklılıklar da zaman zaman görülebilmektedir. Özellikle GDPR'in oldukça detaylı düzenlenmiş olması, dünya ölçeğinde düzenlemelere temel teşkil etmesi ve ticari ilişkilerde uyumun sağlanması adına, birçok ülkenin bu düzenlemeyi baz alarak mevzuatlarını düzenledikleri görülmektedir. Ülkemizdeki kişisel verilerin korunması kanunu da(KVKK), GDPR ile paralellikler içermektedir. Ama henüz aynı teferruatlara sahip olmadığı açıktır.

Çalışmamızda sağlık alanındaki kişisel verilerin işlenmesi, yurtdışına aktarılması konusu temel olarak incelenmekle birlikte bu işlemlerin kişisel verilerin genel işlenme ilkeleriyle uyumlu olduğu düşünüldüğünde konunun daha iyi anlaşılabilmesi açısından, bu kısımların açıklanması gerekliliği açıktır. Bu nedenle çalışmamızda genel ilkeler üzerinden gidilerek ana konunun daha net bir şekilde anlaşılmasına çalışılacaktır. Mevzuat farklılıkları yeri geldikçe belirtilmekle birlikte, çalışmanın sonunda bu farklılıklara tekrar toplu olarak dikkat çekilecektir. Farklı düzenlemelere konu içerisinde değinilecek, fakat temelde ülkemizde yürürlükte olan KVKK ile GDPR düzenlemesi ana metin olarak karşılaştırılacaktır.

Kişisel verileri koruma hukuku, çok dinamik bir yapıda olduğundan ve uluslararası hukuk düzenlemeleri de düşünüldüğünde bilgilerin çok hızlı değişmesi, mevzuatın sürekli yenilenmesi durumu nedeniyle sınırlama yapılması zorunluluğu mevcuttur. Konu disiplinler arası çalışmayı gerektirmekte (Bilişim teknolojileri, medeni hukuk, borçlar hukuku, ceza hukuku, sağlık hukuku, ticaret hukuku gibi farklı hukuk alt dalları), bu nedenle konu oldukça geniş bir alanı içermektedir. Çalışmanın esas amaçlarından birisi ise ülkemiz mevzuatındaki düzenlemeler ile uluslararası hukuktaki diğer düzenlemeler arasındaki farklılık ve eksiklikleri özellikle sağlık hukuku bağlamında incelemektir.

Çalışmanın ilk kısmında kişisel verileri koruma hukukunun tarihsel gelişiminden bahsedilerek, bu sürecin zaman içerisinde gelişimi anlatılacaktır. Ardından kişisel verileri koruma hukukunda bulunan evrensel temel ilkeler açıklanacak, konunun devamında anlatılan kısmın net anlaşılabilmesi için kavramlar belirginleştirilecektir. Bu kısımda konu içerisindeki kavramlar başta GDPR olmak üzere, uluslararası hukuktaki bölgesel mevzuatlarla karşılaştırmalı olarak anlatılacaktır. Çalışmamızda özellikle konunun ehemmiyetine binaen, özellikle kişisel sağlık verilerinin işlenmesi aşamasında yeni teknolojilerin uygulanmasını(Özellikle yapay zeka uygulamalarının kişisel veri işlenmesi ve mahremiyet kavramalarına etkisi ve bununla ilgili düzenlemeler) ve yurtdışına aktarımı kısmı detaylandırılacak, bu konunun sağlık hukuku bağlamındaki değerlendirilmesi yapılacaktır.

BİRİNCİ BÖLÜM
KİŞİSEL VERİLERE İLİŞKİN TEMEL KAVRAMLAR

1. KİŞİSEL VERİ KAVRAMI VE TANIMLAR

1.1. Kişisel Veri

1.1.1. Kişisel Veri Tanımı

Veri kavramı, herhangi bir araştırmanın ana öğesi olarak tanımlanabilir.[1] Kişisel veriler hukukunda bazen veri kelimesi yerine 'enformasyon' ya da 'bilgi' kavramları kullanılmaktadır. Aslında bu kavramlar birbirleriyle eş anlamlı olmasalar da bu durumun esas nedeni kavramların esas içeriklerinin tam olarak anlaşılamamış olmasıdır.

Özellikle ülkemizde bu kavramların yanlış olarak birbirlerinin yerine sıklıkla kullanıldığı görülür. Oysa Avrupa'da bu kullanımlar daha düzenli ve yerli yerindedir. Temel olarak aradaki ayrım veri kavramının, bilgi kavramının özünde olmasıdır. Ancak üzerinde işleme faaliyeti yapılması sonrası veri, bilgiye dönüşür.

Bir kişiye ait olan tüm verilere kişisel veri adı verilir. KVKK'da bu tanım "kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgi" şeklinde düzenlenmiştir.[2] Benzer bir tanım GDPR'da da vardır. Fakat burada KVKK'dan farklı olarak daha detaylı bir açıklama mevcuttur. GDPR'a göre bahsedilen belirlenebilirlik kavramı

[1] www.tdk.gov.tr E.T:16.05.2023
[2] Kişisel Verilerin Korunması Kanunu (2016). Resmi Gazete sayı: 29677, 07.04.2016 http://www.resmigazete.gov.tr (E.T. 19.05.2023)

ilgili kişiye ait kimlik bilgisi, sosyal, kültürel, ekonomik durum bilgisi veya fiziki, psikolojik, çok sayıda bilgi üzerinden belirlenebilir kişiyi içerir.[3]

Kişisel veri kavramı Yargıtay 'ın bir kararında paylaşılmıştır. Buna göre, kişinin belirli bir çevrede paylaştığı fakat üçüncü kişilere sunmadığı, kişiliğe ait bir takım niteliklerini belirten, kimliğe ait bilgiler, cinsel, sağlık, politika ve benzeri konulardaki bilgilerini içeren ve bunlar aracılığıyla kişinin belirlenebildiği veriler, kişisel veriler olarak tanımlamıştır.[4]

Kişisel verinin tam olarak ne olduğunu tanımlayabilmek için öncelikle mevcut bir veri üzerinden değerlendirme yapmak gereklidir. Ardından bu verinin gerçek bir kişiye ait olduğu teyit edilmelidir. Diğer bir deyişle kişisel veri ancak gerçek bir kişiye ait olabilir. Bu veriler bazen objektif ve bazen de sübjektif nitelikler taşıyabilir. Kişilere ait kimlik bilgileri objektif nitelik taşırken düşünsel ve fikirsel bir takım değerlendirmeler sübjektif nitelik taşıyabilir. Bu durum her ikisinin de veri niteliğinde olması durumunu değiştirmez.[5]

Kişisel veriler, verilerin ortaya çıkışı açısından iki farklı başlık altında toplanabilir. Bunlardan ilki kişilere doğrudan ait olan isim, doğum gibi veriler olurken, diğerleri ise toplum içerisinde yaşama sebepli oluşturulan veriler olarak gruplanabilir. Fakat bu gruplamanın veri koruma açısından bir önemi bulunmamaktadır.[6]

---

[3] www.eur-lex.europa.eu E.T. 19.05.2023

[4] Yargıtay 12. Ceza Dairesi, T: 02.12.2015 E: 2015/4006 K: 2015/18748 https://barandogan.av.tr/blog/mevzuat/tck-madde-136-verileri-hukuka-aykiri-olarak-verme-veya-ele-gecirme-sucu.html E.T. 19.05.2023

[5] Aksoy HC. Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması. Ankara: Çakmak Yayınevi, 2010, s. 14.

[6] Dülger MV. Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 2015. 1(2), s. 44.

Bir verinin kişisel veri olarak kabul edilmesi, bu verinin gerçek kişiye ait olması ile mümkündür. Buradaki önemli nokta tüzel kişilere ait verilerin, kişisel veri olarak kabul edilmeyeceğidir. GDPR yürürlüğe girmeden önce bu duruma ait bir düzenleme, daha önce yürürlükte bulunan 95/46 sayılı Direktif'te[7] mevcut değildi. Kişisel verilerin korunması ile sağlanmaya çalışılan amacın kişi temel hak ve özgürlükleri olduğu düşünüldüğünde bu durum gayet makuldür. Tüzel kişiliklerin de bu veri korumasından faydalanmasını sağlamak, amaçtan uzaklaşmaya ve veri koruma etkisinin azalmasına yol açabilecektir.

Kişisel veri kavramının temelinde kişinin belirlenebilirliği durumu yatar. Ancak bu veriler, kişiyi belirleyebilmeyi sağlıyorsa ve kişiyi diğer kişilerden ayırt edebiliyorsa kişisel veri olarak kabul edilebilir. Bu kıstasa göre kişinin ismi, dernek üyelikleri, sağlık bilgileri vb. tüm veriler kişiyi belirlemeyi sağlayabilir. Bu durum somut olay özelinde incelenerek değerlendirilmeli, kişisel veri olup olmadığı kararı buna göre verilmelidir.[8]

Kişilere ait bazı veriler vardır ki bunlara genetik veriler, sağlık verileri, biyometrik veriler örnek olarak verilebilir ve bunlar çoğaltılabilir, kişinin doğrudan belirlenmesini sağlayabilir. Bazı durumlarda ise eldeki veri doğrudan kişiyi belirleyemese de ulaşılabilecek bazı ek veriler kişiyi belirli hale getirebilir. Burada belirlenebilirlik üzerinden kişisel veri tanımı yapılabilir. Breyer-Federal Republic of Germany kararı [9] bu açıdan önemlidir. Bu olayda davacı kendisine ait IP adresinin silinmesi talebiyle veri sorumlusuna başvurmuştur. Veri sorumlusu, veri sahibini belirleyebilmek için ek bilgiye ihtiyaç duymuştur ve IP verisinin kişisel veri olup olmadığı yönünde Avrupa Birliği Adalet Divanı (ABAD)'na soru yöneltmiştir. ABAD ise kişileri belirli kılan tüm verilerin kişisel veri olarak kabul edilmesi gerektiğini belirtmiş, değerlendirmenin bu şekilde yapılmasını istemiştir. Buradaki ek veriye ulaşma durumu özellik arz

---

7 95/46 sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi. www.eur-lex.europa.eu E.T. 19.05.2023

8 Küzeci E. Kişisel Verilerin Korunması, Oniki Levha Yayınları, İstanbul, 2020, 4. Baskı. s. 11.

9 ABAD- Breyer v. Federal Republic of Germany, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200442%22]} E.T: 19.05.2023

etmektedir. Önemli olan herhangi bir yolla ek veriye ulaşmak değildir. Veriye ulaşma durumu aşırı güçlüğe yol açmamalı ve yasa dışı yollardan olmamalıdır.[10]

Kişisel verilerin korunması başlığı detaylandırılmadan önce, konunun içerisinde sıklıkla geçen kişisel verilerin işlenmesi kavramı da netleştirilmelidir. Aslında bu kavram oldukça geniş bir içeriği barındırır. Kişisel verilerin işlenmesi denildiğinde kaydetme, silme, aktarma, düzeltme vb. birçok faaliyet girer. Tarihi gelişim incelendiğinde 108 sayılı sözleşmenin, korumak için esas olarak otomatik yollarla işlenen verileri önceledeği görülür. Sonraki düzenlemeler bunun dışındaki veri işleme faaliyetlerini de içermiştir. Ülkemizde uygulanmakta olan KVKK ise bir veri kayıt işleminin parçası olan tüm veri işlemeleri kapsayacak şekilde düzenlenmiştir. Yine konunun içerisinde sıklıkla geçen kavramlardan ikisi de veri sorumlusu ve veri işleyen kavramlarıdır. Veri sorumlusu esas olarak veri işleme faaliyetinin amaç ve organizasyonundan sorumlu olan gerçek veya tüzel kişi iken, veri işleyen ise veri sorumlusunun idaresi ve denetimi altında çalışan kişidir.

1.2. Kişisel Sağlık Verileri

1.2.1. Kişisel Sağlık Verileri Tanımı

Kişisel Sağlık Verisi kavramı, kanunda tanımlanmamış olmakla birlikte, Kişisel Sağlık Verileri Hakkında Yönetmelik[11] içerisinde tanımlanmıştır. Buna göre m.4/1/j bendinde Kişisel Sağlık Verisi, "Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgi" olarak tanımlanmıştır.

GDPR Md.4'de (Art.4 No:15) kişisel sağlık verileri şu şekilde tanımlanmaktadır: "*Sağlıkla ilgili veri, sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek*

[10] Yücedağ, Nafiye. Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, vol.75, no.2, 2017, s. 768.

[11] 21 Haziran 2019 Tarih ve 30808 Sayılı resmi gazetede yayınlanmıştır.

kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel ya da ruhsal sağlığına ilişkin kişisel verilerdir."[12]

Bu tanımlar ışığında değerlendirildiğinde 'Genetik ve Biyometrik veriler' bazı durumlarda sağlık verisi olarak değerlendirilmeyebilecektir. Bu durumun somut olay özelinde değerlendirilmesi uygun olacaktır.

Dünya Sağlık Örgütü Anayasasında sağlık; *"* hastalık ve sakatlığın olmayışı değil, bedenen, ruhen ve sosyal yönden tam iyilik halidir*"* şeklinde tanımlanmıştır.[13] Kişisel sağlık verisi ise, "kimliği belirli ya da belirlenebilir gerçek bir kişinin sağlığıyla ilgili her türlü bilgi" yi ifade eder.[14] Bu bağlamda değerlendirildiğinde kişisel sağlık verisi kavramı, içerisinde kişinin hastalıkları, kullandığı ilaçlar, aldığı tedaviler, geçirdiği cerrahi işlemler, yapılan tetkikler, tahlil sonuçları vb. kişinin sağlığı ile ilgili birçok bilgiyi içerir.

Kişisel sağlık verileri KVKK'da özel nitelikli kişisel veri kategorisinde ele alınmıştır. Bu veriler niteliği itibariyle daha hassas verilerdir, daha özenle ve sıkı kontrol şartları altında işlenmelidir.[15] Buna yönelik bir yargıtay kararında kişisel sağlık verilerinin, kişinin toplumsal ve sosyal statüsünü etkileyebilecek fiziksel ve ruhsal bilgiler içerdiği belirtilmiştir.[16] Kişisel sağlık verileri genel olarak diğer özel nitelikli verilerden daha ayrıcalıklı olarak korunmaktadır. Bu verilerin işlenebilmesi için ilgili kişinin açık rızası alınmalıdır. Aksi durum ise ancak sır saklama yükümlülüğü olan kişilerce ya da bu yetkinin verildiği kuruluşlarca işlenebilmesi durumudur. Bu durum diğer özel nitelikli veriler için olmayan bir sınırlamadır.

---

[12] Çekin MS. Avrupa birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, Oniki Levha Yayınları. 3.Baskı, İstanbul, 2020, s.198.

[13] https://www.who.int/about/mission/en/ E.T.19.05.2023

[14] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik. RG, 29863, 20.10.2016 http://www.resmigazete.gov.tr E.T. 19.05.2023

[15] Akgül A. Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Yayımlanmamış Doktora Tezi, Kocaeli 2013, s.18.

[16] YCGK E: 2012/1510, K:2014/331 K.T:17.06.2014, (www.emsal.yargitay.gov.tr E.T:19.05.2023)

Kişisel sağlık verisi kavramı, içerisindeki kelimelerden yola çıkılarak değerlendirildiğinde; öncelikle bir veri olmalı, bu veri gerçek bir kişiye ait olmalı ve son olarak da bu veri ilgili kişinin sağlık durumuyla ilgili olmalıdır. İlgili kişinin aldığı sağlık hizmeti ile ilişkilendirilebilen veri ancak kişisel sağlık versi kategorisinde değerlendirilecektir. Bu şartları sağlamayan veri, kişisel sağlık verisi olarak nitelendirilemez.

Kişisel sağlık verileri, özellikle bu verilerin hassas veri olması ve özel korumaya ihtiyaç duyması gerekliliği de düşünülerek geniş yorumlanabilir. Bu durumun temel hak ve özgürlükleri koruma bağlamında fayda sağlayabileceği düşünülebilir. Kişisel sağlık verisi kapsamına, kişinin sağlığı ile ilgili gerçekleştirilen her eylem dahil edilmelidir.[17] Bu durum ile ilgili Bodil Lindqvist kararı mevcuttur. Bu kararda ABAD, kişişel sağlık verisi kavramının içerisine kişinin fiziki ve ruhsal verileri dahil tüm sağlık verilerinin alınması gerektiğini belirtmiştir.[18] Bu bakımdan AİHM'in Z./Finlandiya kararı[19] da önemlidir. Bu kararda AİHS 8. Maddede bahsedilen özel hayatın gizliliği ilkesine atıfta bulunularak kişisel sağlık verilerinin korunmasını temel hak ve özgürlükler kapsamı içerisinde değerlendirmiştir ve hukuk sisteminde temel ilkelerden biri olarak yer almıştır. Kişisel sağlık verilerinin korunması için harcanan çaba, mahremiyet ilkesinin sağlanması ile birlikte sağlık sistemine duyulan güveni ve sürekliliği sağlamak açısından da önem arz etmektedir.[20]

Kişisel sağlık verilerine ayrıcalıklı olarak önem atfedilmesinin ve korunmasının bir nedeni de kişilerin sağlık hizmetine erişimini sağlamaktır. Bu durum hem kişilerin daha sağlıklı olmasını ve dolayısıyla toplumun daha sağlıklı olmasını sağlayacak, hem de özellikle bulaşıcı hastalıklar bağlamında düşünülecek olursa sağlık hizmetlerinin etkin kullanımı sağlayabilecektir. Kişilerin, açıklandığı takdirde ayrıma ve dışlanmaya uğramasına neden olabilecek bir takım sağlık verilerinin, üçüncü kişilerin eline

[17] Ayözger Öngün AÇ. Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil 2. Baskı, Beta,2019, s. 32.
[18] ABAD 06.11.2003 C-101/01 http://curia.europa.eu/juris/liste.jsf?num=C-101/01) E.T:19.05.2023
[19] Avrupa İnsan Hakları Mahkemesi, Z/Finlandiya Davası, Başvuru Numarası: 22009/93 https://dergipark.org.tr/en/download/article-file/1671838 E.T:19.05.2023
[20] AİHS, https://www.echr.coe.int/documents/convention_tur.pdf E.T:19.05.2023

geçebileceği endişesi ile bu hizmetlerden kaçınmasını engelleyecek, önleyici ve kişileri bu anlamda ikna edici tedbirlerin alınması çok önemlidir.

Burada göze çarpan bir diğer husus da biyometrik ve genetik veriler hususudur. GDPR'da bu verilerin niteliğinin değerlendirilmesinde, somut olayda kullanılış amacı ve yeri değerlendirilerek karar verilmelidir. Kimlik tanımlama için kullanılacak olan yüz tanıma sistemleri ile güvenlik amacıyla kullanılan yüz tanıma sistemleri farklı kategorilerde değerlendirilebilecektir. Kişilerin sağlık hizmeti alırken bir takım genetik değerlendirmeler yapılması esnasında elde edilen veriler kişisel sağlık verisi kategorisine girecektir. Bu durumda her iki veri türü de koşulları oluştuğunda kişisel sağlık verisi olarak değerlendirilebilecektir. KVKK'da bu veriler ismen özel nitelikli kişisel veri olarak zikredilmiş olsa da kanun metninde tanımlanmamışlardır.[21] Bu durumun karışıklığa yol açmaması adına GDPR'a benzer şekilde açıklamaların yapılması, netliğin sağlanması işleyişin daha verimli olmasını sağlayacaktır.

1.3. Hassas Veri Kavramı

1.3.1. Hassas Verinin Tanımı

Her kişisel veri aynı önem ve etkiye sahip değildir. Bu nedenle kişisel veriler arasında bir takım gruplandırmalar yapılır. Burada ayrımki; açıklandığı takdirde kişilerin bundan zarar görmesi üzerinden yapılmaktadır. GDPR'da hassas veri, KVKK'da ise özel nitelikli kişisel veri olarak nitelendirilen bu grup veriler özel düzenlemeye tabi tutulmuşlardır. Bu veriler sıklıkla mevzuat düzenlemesinde sayma yöntemiyle(Numerus Clausus) düzenlenir. Bu nedenle belirtilen veriler dışındaki verilerin yorumlama yoluyla genişletilebilmesi mümkün değildir.[22]

[21] Yücedağ N. Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İÜHFM, C. LXXV, S. 2, 2017, S. 765-790.

[22] Ömür RC. Kişisel Sağlık Verilerinin Korunması ve Hastanelerin Sorumluluğu, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, İstanbul, 2018, C.15, S.1, s.136.

KVKK'da hassas veriler(Özel Nitelikli Kişisel Veri); KVKK m.6'da "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".[23] şeklinde düzenlenmiştir.

95/46 sayılı Direktif sonrası GDPR yürürlüğe girmiştir. Bu düzenlemeyle hassas veriler kavramında bir takım genişlemeler olmuştur ve kimlik tespitinde kullanılan biyometrik ve genetik veriler bu kategoriye alınmıştır. Diğer taraftan kişilerin cinsel eğilimleri de bu veri kategorisine dahil edilmiştir. Bu grup verilere ait veri işleme faaliyetleri özel koruma tedbirleri altında denetlenmektedir. Ülkemizde yürürlükte olan KVKK düzenlemesinde GDPR'dan farklı olarak, mahkeme kararları özel nitelikli kişisel veri kategorisinde değerlendirilmiştir. [24]

Kişisel sağlık verileri birçok mevzuatta, kişisel verilerin daha özellikli bir alt grubu olarak değerlendirilir. Bunun haklı bir takım nedenleri vardır. Bununla birlikte verileri kategorize etme konusu ise bazı yazarlarca halen tartışılmaktadır. Buna itiraz eden yazarların esas üzerinde durduğu nokta ise kişisel verilerin somut olay özelinde değerlendirildiğinde ancak hassas veri olup olmadığının değerlendirilebileceği, aksi durumda sadece sayma yöntemi kullanılarak yapılacak gruplandırmaların amaca hizmet etmeyeceği düşüncesindedirler. Aynı değerlendirmeye göre verilerin kategorilendirilmesi aşamasında tarafların menfaati, işlemenin olası neticeleri gibi verinin işlendiğinde ortaya çıkacak etkilerini değerlendirmek önem arz etmektedir.[25]

Diğer taraftan bazı yazarlar kişisel verileri gruplandırırken dikkate alınması gereken esas unsurun verinin işlenme amacı olduğunun düşünürler. Her durumda verinin

[23] KVKK md. 6. KVKK (2016). RG, 29677, 07.04.2016 http://www.resmigazete.gov.tr E.T:19.05.2023
[24] Küzeci, s. 251
[25] Simitis S. Revisiting Sensitive Data. 1999, s.8. https://rm.coe.int/09000016806845af E.T.19.05.2023

işlenme amacı üzerinden yapılacak değerlendirme işlenen verinin hassas bir içerik taşıyıp taşımadığı konusunda daha sağlıklı bilgi verecektir.[26]

Verilerin işlenmesi ile bilgiye ulaşılır. Bu durum işlenen veri ile birlikte ortaya çıkacak verinin içeriğini de etkiler. Kimi durumlarda ortaya hassas bir takım veriler çıkabilir. Burada yapılması gereken değerlendirme ortaya çıkan bilginin kanunda sayılan özel nitelikli verilerden birine dahil edilip edilmeyeceği değerlendirmesidir. Bu değerlendirmeyi olabildiğince sık yapmak ilgili kişiyi korumayı sağlayabilecektir.

Bu tür özel nitelikli verilerin tespiti özelinde değerlendirme yapan Küzeci'ye göre bu durumda bir takım hususların dikkate alınması gerekir. Özellikle verinin hangi amaçla işlendiği, ilgili kişiyi etkileyecek durum değerlendirmesi gibi hususlar incelenerek karar verilmelidir.[27] Koruyuculuğu arttırabilmek adına kişisel sağlık verilerinin geniş yorumlanması, aynı yorumlamanın verinin hasssaslığı değerlendirmesinde de yapılması önerilmektedir.

Hassas veri değerlendirmesinde yol gösterici olan bir takım mahkeme kaarları da mevcuttur. Bunlardan bir tanesi AİHM'in S.& Marper v-UK[28] kararıdır. Bu kararda kişinin hücre örnekleri, DNA profili ve parmak izi örneklerinin aynı etki derecesine sahip hassas veriler olmadığı değerlendirmesi yapılmıştır. Mahkeme, soruşturma ve kovuşturma esnasında alınan bu tür örneklerin etki değerlendirmesi yapılması gerektiğini belirtmiştir. Özellikle hücre örnekleri ve DNA bilgilerinin, kişiye ve aileye ait bilgiler içerdiği ve hatta etnik kökene ait bir takım verilere buradan ulaşılabileceği düşüncesinden hareketle gelecekte kişiye yönelik bir takım zararlar oluşturabileceği belirtilmiştir. Fakat aynı kararda parmak izi incelemesinin DNA ve hücre verilerine kıyasla daha az önemli olduğu belirtilmiştir. Böyle demekle beraber yine aynı kararda

[26] Aksoy, Hüseyin Can. Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması. Ankara: Çakmak Yayınevi, 2010, s. 33.

[27] Küzeci, s. 252

[28] S. And Marper v UK. Başvuru no. 30562/04 ve 30566/04, 04.12.2008 www.echr.coe.int E.T: 19.05.2023

mahkeme, parmak izi bilgilerinin saklanması konusunun da özel hayatının gizliliği çerçevesinde bir müdahale olduğunu kabul etmiştir.

İKİNCİ BÖLÜM
KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI HUKUKUNUN TARİHSEL GELİŞİMİ VE MEVZUAT DÜZENLEMELERİ

1. KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI HUKUKUNUN TARİHSEL GELİŞİMİ

Tababet uygulamaları bağlamında değerlendirildiğinde, kişisel sağlık verilerinin korunması konusu çok eskiden beri üzerinde konuşulan ve hekimler tarafından dikkat edilen bir husustur. Antik döneme ait kalıntılarda hekimin sır saklama ve kayıt tutma yükümlülüğünün varlığını gösteren örnekler mevcuttur. Bu örneklere Asur Kralı Asurbanipal(MÖ 688-627) döneminde bulunan tabletler içerisinde rastlanmaktadır. [29]

Antik dönemde hekimlerin tıbbi kayıt tuttuğunu gösteren kanıtlar yanında modern seviyede tıbbi kayıtlar 19. Yüzyılda başlamıştır. Dr. Henry S. Plummer bu kayıt sistemlerinin babası olarak bilinir. Dr. Plummer hasta kayıtlarını sistematik hale getirmiş, her hasta için düzenli ve ayrı kayıt dosyaları oluşturmuştur.[30]

Hekimlik mesleği, bir takım çalışma biçimlerini birlikte getirmiştir. Hekim-hasta ilişkisinin verimli olması ve uygun şekilde işlemesi için güven ilişkisinin kurulması gerekir. Güven ilişkisi ise mahremiyete saygı ile mümkün olur. Bu çerçevede düşünüldüğünde; hekimlik mesleğinin ilk dönemlerinde bile hekimin sır saklama yükümlülüğünün kendiliğinden gelişmiş bir yükümlülük olduğu tahmin edilebilir. Hipokrat yemininde hekimlere, hastaların bilgilerini gizleme, ifşa etmeme bir yükümlülük olarak yüklenmiştir. Sır saklama yükümlülüğü olarak adlandırılan bu durum zamanla hekimler dışında diğer bazı meslek gruplarına da getirilmiştir.[31]

---

[29] Er Ü. Sağlık Hukuku. Ankara, 2019, Savaş Yayınevi, 2. Baskı, s. 92

[30] Nelson CW. 90th Anniversary of the Mayo Medical Records System.72(8), 1997, s. 696. Elsevier Inc. www.mayoclinicproceedings.org/article/S0025-6196(11)63586-6/fulltext E.T. 19.05.2023

[31] Çelik Y. Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, TAAD, 32, 2017, s. 397.

Her ne kadar daha önceki zamanlara ait bir takım kişisel veri koruma önlemleri ve uygulamaları varsa da post-modern toplum yapısının gelişimi bu alanın gelişimine neden olmuştur. 1970'li yıllarda bu alandaki gelişmeler hız kazanmıştır. Öncülüğü ise Batı Avrupa toplumları yapmıştır. 1983 tarihli Alman Anayasa Mahkemesi kararı bu alanda temel kabul edilir. 'Nüfus sayımı Kararı'[32] olarak bilinen bu karar ile mahkeme, insan onuru ve kişinin maddi ve manevi hakkını serbestçe geliştirme hakkı çerçevesinde kişisel verilerin korunması gerektiğine hükmetmiştir. Kişilerin kendi bilgilerinin geleceğini tayin etme hakkı olarak da nitelendirilen enformasyonel self determinasyon hakkı sağlandığı takdirde kişilerin onurlu ve özgür bir birey olması mümkün olabilir.

Kişisel verilerin korunması hukuku çerçevesinde incelediğimizde 1970 yılında Almanya Hessen eyaletinde bir metin yazıldığını görürüz. Bu metin bu alanda yazılan ilk hukuk metni olarak kabul edilmektedir. Federal Almanya Veri koruma kanunu ise 1977 yılında yürürlüğe girmiştir.[33]

Bu sürecin başlamasıyla birlikte hem ulusal hem uluslararası alanda düzenlemeler yapılmaya başlamıştır. Bunlardan "Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" özellikle veri koruması için gerekli olan temel ilkeleri içermesi nedeniyle önemlidir. Bu ilkeler 1980 yılında OECD tarafından düzenlenmiştir. Bahsi geçen düzenlemede "veri kalitesi, bireyin katılımı, açıklık, sınırlılık, belirlilik, veri güvenliği ve hesap verilebilirlik" ilkeleri düzenlenmiştir. Metin herhangi bir bağlayıcılık gücüne sahip değildir. Uluslararası alanda yapılan ilk metin olması açısısından da önemlidir.[34]

Kabul edilen bir diğer sözleşme ise "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" dir.[35] Avrupa Konseyi tarafından 1981

---

[32] Küzeci, Elif. İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı. İnsan Hakları Yıllığı, Cilt 32, 2014, s. 53-75

[33] Küzeci, s. 110.

[34] http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransbord erflowsofpersonaldata.htm E.T. 19.05.2023

[35] www.tbmm.gov.tr/sirasayi/donem24/yil01/ss700.pdf E.T. 19.05.2023

yılında kabul edilmiştir. Bu sözleşmede geçen önemli bir husus, kişisel sağlık verilerinin hassas veri niteliğinde olduğunun kabul edilmiş olmasıdır. Ayrıca bu tür verilerin otomatik işleme tabi tutulabilmesi için iç hukukun yeterli koruma sağlamış olması şartı aranmıştır.[36]

Kişisel verilerin korunmasına yönelik yapılan düzenlemelerde önemli bir aşama 95/46/AT sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi " [37] dir. Bu düzenleme ülkemizde yürürlükte olan KVKK'nın düzenlenmesinde de temel alınan düzenlemedir. Direktif, Avrupa ülkelerinde uygulanması istenen kişisel verileri koruma kanununu oldukça detaylandırmış ve bu ülkelerin, uyum için gerekli düzenlemeleri yaparak iç hukuklarına aktarmalarını istemiştir. Bu düzenlemede hassas veri kategorisi oluşturulmuştur. Bu kategoriye kişisel sağlık verileri de eklenmiştir.

Bir diğer düzenleme 1997 tarihinde Avrupa konseyinin yayınladığı tavsiye kararıdır. "Tıbbi Verilerin Korunmasına İlişkin Tavsiye Kararı" olarak adlandırılan bu metinde kişisel sağlık verisi, "bireyin sağlığıyla ilgili olan bütün kişisel verileri ve genetik verilerle açık ve yakın bağlantısı olan verileri" şeklinde tanımlanmıştır. Aynı yıl içinde Avrupa Konseyi "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Hassasiyetinin Korunması Sözleşmesi" adlı sözleşmeyi düzenlemiştir. Bu sözleşmede yer alan "Özel Yaşam ve Bilgilendirilme Hakkı" başlıklı 10. maddesine göre; "Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir" denilerek kişisel sağlık verilerinin ilgili kişinin kararları doğrultusunda korunması gerekliliğini belirtmiştir.[38]

---

[36] Dülger, MV. Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti, İMÜHFD, s. 54

[37] https://kisiselveri.com/9546ec-turkce E.T. 19.05.2023

[38] Dülger, s. 55.

Kişisel veri koruma alanında yapılmış olan esas düzenleme GDPR olarak kabul edilmektedir. Bu metin 2016 yılında kabul edilmiştir. Yürürlüğe girmesi ise, 2018 yılında olmuştur ve yürürlüğe girmesi ile direktif yürürlükten kalkmıştır. Direktiften farklı olarak AB ülkelerinde uygulanma açısından değerlendirildiğinde tüzük olması nedeniyle ülkelerin iç hukukuna doğrudan geçmesi önemli bir husustur. Herhangi bir uyumlaştırma sürecine ihtiyaç duymamaktadır. Direktif, güncel teknolojik kavramlarla ilgili düzenlemeleri ve kavramları içerisinde barındırmaktadır.

2. KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI HUKUKUNUN KAYNAKLARI

Kişisel sağlık verilerinin korunması amacıyla yapılan hukuki düzenlemeler farklı düzenlemeler adı altında farklı alanlarda bulunabilir. Bu düzenlemeler gerek ulusal gerek uluslararası düzenlemeler şeklinde olabilir. Ayrıca mevcut düzenlemelerde temel hak ve hürriyetler içerisinde ya da özel hayatın gizliliği başlığı altında görülebilir. Sağlık Hukuku özelinde değerlendirdiğimizde ise bu düzenlemelere hekimin sır saklama yükümlülüğü, hasta mahremiyeti başlıkları altında rastlamak mümkündür. Bu düzenlemeler bazen de kişisel sağlık verisinin korunmasına yönelik olarak doğrudan kanun maddeleri içerisinde bulunabilir. Çalışmamızda bu düzenlemeler uluslararası kaynaklar ve ulusal kaynaklar başlıkları altında detaylandırılacaktır.

2.1. Uluslararası Kaynaklar

2.1.1. Avrupa İnsan Hakları Sözleşmesi

AİHS, 1950 yılında imzaya açılmıştır ve insan hakları temelinde en önemli kaynaklardan biri olarak kabul edilir. Fakat bu sözleşmenin içerisinde kişisel verilerin korunması alanının ayrı bir şekilde düzenlenmediğini belirtmek gerekir. AİHS m.8 özel yaşamın gizliliği hakkı başlığı altında bu konuyu düzenlenmiştir. Buna göre;

"1) *Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*"

Doğrudan kişisel verilerin korunması hakkından bahsedilmediği için bu ilkeyi kapsayıp kapsamadığı yönündeki değerlendirme için Avrupa İnsan Hakları komisyonunun kararlarına bakmak isabetli olacaktır. AİHM kararlarına bakıldığında özellikle 1980 sonrasında, bu alana yönelik kararların sayısında artış görülmektedir. AİHS özellikle, taraf devletlerin organlarınca yapılan veri işleme işlemlerine yönelik bir koruma sağlamaktadır. Özel kişiler tarafından ya da özel sektör tarafından işlenen verilerin ne şekilde korunacağı konusu bu sözleşmeye göre net değildir. Mahkeme önüne gelen somut olayı değerlendirirken, öncelikle oluşan durumun özel hayata dair olup olmadığı değerlendirmesi yapmaktadır. Bu da etki alanının bazı durumlarda daralmasına ve yetersiz kalmasına yol açmaktadır.

Verilen kararlar doğrultusunda değerlendirme yapıldığında 8. maddenin; kişisel verilerin resmi makamlarca toplanarak arşivlenmesi, telefon görüşmelerinin takibi, toplanan verilerin başlangıçta belirlenen amacı dışında kullanımı, çalışanların bilgisayarlarının takibi, emniyet güçleri tarafından parmak izi alınması, kişisel verilerin amacı dışında uzun süre tutulması gibi durumları kapsadığı görülmektedir.[39]

2.1.2. İnsan Hakları ve Biyotıp Sözleşmesi

Bu sözleşme, uzun adıyla "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi"[40] olarak bilinir. Bu sözleşme temel

[39] Küzeci, s.151-158.
[40] https://www.tbmm.gov.tr/kanunlar/k5013.html E.T:19.05.2023

olarak insan onuru kavramını ele alır. İnsanın sırf insan olmasından dolayı bazı haklara sahip olduğunu kabul eder. Sözleşme m.10'da "Özel Yaşam ve Bilgilendirilme Hakkı" başlığı altında kişisel sağlık verilerinin konumlandırıldığı ve korunduğu görülür.

2.1.3. Hasta Haklarına İlişkin Avrupa Statüsü

Hasta haklarına yönelik bu düzenleme 2002 yılında kabul edilmiştir. Düzenlemenin 6. maddesinde 'Özel ve Gizlilik Hakkı' başlığı altında kişisel sağlık verileri koruma altına alınmıştır. Bu maddeyle ilgili kişilerin, kişisel sağlık verisi olarak değerlendirilebilecek hastalıkları, yapılan işlemler, tanı ve tedaviye yönelik testler, girişimsel işlemler ve cerrahi işlemler sırasında mahremiyetinin sağlanması, bu işlemlere ait bilgilerin korunması ve gizliliğinin sağlanması da dahil olmak üzere sağlık hizmeti alma sürecindeki tüm bilgilerin korunması gerekliliği belirtilmiştir. Bu korumayı sağlayabilmek adına, yapılan tüm müdahaleler gerekli şartların sağlandığı bir ortamda ve hastanın onayı alınarak ve sadece orada bulunması gereken kişilerce yapılmalıdır. [41]

2.1.4. Amsterdam Bildirgesi

Uzun adıyla "Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi" [42] olarak da bilinen Amsterdam Bildirgesi 1994 yılında kabul edilmiştir. Bu bildirgede özellikle rıza kavramının üzerinde durulmuş ayrıca kişisel sağlık verilerinin işlenme sürecine hastanın tüm aşamalarda katılımının sağlanması için düzenlemeler getirmiştir. Bildirge m.4 "Mahremiyet ve Özel Hayat" başlığını taşır ve buna göre "1)Hastanın

[41] European Charter Of Patients' Rights. http://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf E.T: 19.05.2023

[42] Declaration on The Promotion of Patients' Rights in Europe http://www.nurs.uoa.gr/fileadmin/nurs.uoa.gr/uploads/Nomothesia_Nosilefton/Evropaika_keimena/eu_dec laration1994_1_.pdf E.T:19.05.2023

sağlık durumu, tıbbi durumu, tanısı, prognozu, tedavisi hakkındaki ve kişiye özel diğer tüm bilgiler, ölümden sonra bile gizli olarak korunmalıdır. 2) Hastaya ait bu bilgiler, yalnızca hastanın açık izni veya mahkemenin kesin isteği üzerine açıklanabilir. Hastanın tedavisi ile ilgili diğer sağlık personeline ihtiyaç söz konusu olduğunda hastanın onayı olduğu varsayılarak davranılır. 3) Hastanın kimliğine dair bilgiler korunmalıdır. Bu bilgilerin korunması usulüne uygun yapılmalıdır. 4) Hastalar, tanıları, tedavileri ve bakımları ile ilgili kayıtlara, diğer dosyalara, teknik kayıtlara ve tıbbi dosyalarına bakabilme ve kendi dosyalarının ve kayıtlarının kopyasını alabilme hakkına sahiptir. Bu hak üçüncü kişilerin bilgilerine bakabilmeyi içermez."

Kişisel sağlık verilerine ait yanlışlar olduğunu düşündüğünde ilgili kişi bu verilerin düzeltilmesini, değiştirilmesini isteyebilir. Zorunlu durumlar ve tedavinin gerektirmesi halleri dışında hastanın özel hayatına müdahale edilemez. Bu hallerde bile hastanın rızasının alınması ve mahremiyetine saygı gösterilmesi esastır.[43]

Bir diğer düzenleme Dünya Tabipler Birliği Lizbon Hasta Hakları Bildirgesidir. Burada da özel hayata saygı, kişisel sağlık verilerinin korunmasına yönelik düzenlemeler bulunmaktadır.[44]

BM Unesco Biyoetik ve İnsan Hakları Evrensel Bildirgesi de kişisel sağlık verilerinin korunmasının önemini vurgulayan bir düzenlemedir. Bu korumayı insan hakları, insan onuru ve mahremiyet temelinde düzenler.[45]

[43] Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi. http://www.saglikhakki.org/amsterdam1.htm E.T:19.05.2023

[44] Declaration of Lisbon. https://www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/ E.T:19.05.2023

[45] Biyoetik ve İnsan Hakları Evrensel Bildirgesi. http://www.unesco.org.tr/Content_Files/Content/Sektor/Sosyal_ve_Beseri_B/evrensel_bildirgesi.pdf E.T: 19.05.2023

2.1.5. Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme (108 Sayılı Sözleşme)

Avrupa Konseyi 108 Sayılı Sözleşmeyi 28 0cak 1981 yılında imzaya açmıştır. 1985 yılında beş ülke sözleşmeyi imzalamış ve böylelikle yürürlüğe girmiştir. 2023 itibariyle bu sayı 55 i bulmuştur.[46]

108 nolu sözleşme Avrupa Konseyi üyesi olmayan devletlerin de onayına açıktır. Sözleşme verilerin uluslararası akışına ve veri koruma ilkelerine uyumlu hale getirilebilmek için 20 Aralık 2018 tarihinde yenilenmiştir. Bu haliyle 108+ sözleşme olarak adlandırılmaktadır.

108 nolu sözleşmeyi Avrupa insan hakları sözleşmesi ile karşılaştırdığımızda; Avrupa İnsan Hakları sözleşmesinde kişisel verilerin korunmasının bir hak olarak düzenlenmediğini görürüz. Burada korumanın özel yaşamın gizliliği hakkı üzerinden değerlendirildiğini görürüz. Oysa bu, bazı durumlarda korumanın yetersiz olmasına yol açmaktadır. Ayrıca bilişim sistemleri ile kişisel verilerin işlenmesi durumunda korumanın yeterli olup olmadığı konusu tartışmalıdır.[47]

108+ sayılı sözleşme global olarak veri akışını düzenleyen kurallar oluşturma potansiyeli taşımaktadır. Bu nedenle, GDPR özellikle sınır ötesi veri akışı konusunda bu sözleşmeye atıf yapmaktadır. Böylelikle AB'ye üye olmayan bir devlete veri aktarımı yapılırken ve yeterli koruma sağlayıp sağlamadığı değerlendirmesi yapılırken 108 nolu sözleşmeye dahil olup olmadıkları değerlendirilecektir.

2.1.6. 95/46/AT Sayılı Kişisel Verilerin Korunması Yönergesi

Kişisel verilerin korunması amacıyla oluşturulmuş olan fakat yakın bir zamanda yürürlükten kaldırılan önemli metinlerden biridir. Fakat yalnız Avrupa birliği(AB)'nin

[46] 108 Nolu sözleşme. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf E.T:19.05.2023
[47] Küzeci, s.145

değil bir çok ülkenin hukuksal düzenlemelerini etkilemiştir. Avrupa Konseyi(AK) bünyesinde zaten var olan 108 Sayılı Kişisel Verilerin Korunması sözleşmesine rağmen AB bünyesinde yeni bir metnin oluşturulmasının esas nedeni farklı uluslara ait düzenlemelerin tek bir iç pazar oluşumunu engelleme tehlikesidir. AB Veri koruma yönergesinin esas özelliği zorlayıcılığıdır. Bu kurallara uyulması için denetimi sağlayacak birimler oluşturulmuştur. Bu yönergeye göre tamamen kişisel veya ailevi etkinlikler için yapılan veri işleme işlemleri kapsam dışında olacaktır.[48]

Bu yönerge ile kişisel verilerin üçüncü ülkelere aktarılması konusunda yeterli koruma düzeyine sahip olma kriteri getirilmiştir. Bu seviyedeki korumayı sağlamayan ülkelere veri aktarılması kural olarak yasaklanmıştır.

AB Adalet divanı kararları değerlendirildiğinde internet ortamında bilgilerin bulunması, üçüncü ülkelere veri aktarımının olduğunu göstermek için yeterli olmadığı görülmektedir. Bunun için kişisel veriler üçüncü kişilere doğrudan gönderilmelidir ya da internet sunucu altyapısı AB dışı bir ülkede bulunmalıdır. Yeterli korumanın net bir açıklaması olmadığından somut olay özelinde ve ilgili ülkenin hukuki düzenlemeleri, bu düzenlemelerin işleyiş biçimi, komisyonların yeterli denetimi yapıyor olması gibi bir takım değerlendirmelerin yapılması gereklidir. Bazı istisnai durumlar varlığında (bilgilendirmeye dayalı rıza alınması, aktarımın ilgili kişinin çıkarlarını koruma doğrultusunda bir sözleşmeye bağlı olarak yapılması, aktarımın önemli bir kamusal çıkarı koruması vb.) bu koruma aranmayacaktır.[49]

2.1.7. Genel Veri Koruma Tüzüğü

Bilişim teknolojilerindeki ilerlemeler ve veri bilimi alanındaki gelişmeler, kişisel veri koruma düzenlemelerinin bazı durumlarda yetersiz kalmasına yol açmıştır. Bu

[48] Küzeci, s.187-188.
[49] Küzeci, s.194-196.

gerekçeyle 1995 tarihli 95/46 sayılı direktif'i yürürlükten kaldıran GDPR düzenlemesi yapılmıştır.

GDPR düzenlemesi 2016 yılı itibariyle kabul edilmiştir. İki yıllık bir uyum süreci sonrasında ise Direktif'i ilga ederek yürürlüğe girmiştir. GDPR ile kişisel verilerin korunması alanına yeni kavramlar, yeni düzenlemeler getirilmiştir. Oldukça detaylı ve etkin bir düzenlemedir. Bu nedenle dünya çapında bir etkiye sahiptir. Özellikle uluslararası veri aktarımı konusunda daha sıkı kontroller öngörmektedir. Hassas veriler konusunda daha detaylı düzenlemeler içermektedir. Veri koruma etki değerlendirmesi ve veri ihlallerini bildirme zorunluluğu düzenlemenin getirdiği yeniliklerden bazılarıdır.[50] Bu alana kazandırılan kavramların başında ise 'unutulma hakkı', 'privacy by design'(veri koruma anlamında bu veriyi tutan, işleyen cihazların en baştan veri minimizasyonunu hedef edinecek şekilde dizayn edilmesi), 'privacy by default' vb. kavramlar tüzükte yer bulmuştur.

Tüzük, bu alana yeni kavramlar da kazandırmıştır. Doktrin ve yargı kararlarından aşina olunan fakat yasal metinlerde yer almayan "unutulma hakkına", Tüzükte yer verilmiştir. Ayrıca veri taşınabilirliği hakkı, başlangıçtan itibaren (privacy by default) ve tasarımdan itibaren (privacy by design) koruma kavramları Tüzük ile kişisel veri koruma terminolojisine kazandırılmışlardır. Tüzükte, kişisel sağlık verisinin tanımı yapılmış, hassas veri kategorisi içerisinde yer aldığı belirtilmiş ve hangi şartlar altında işlemenin hukuka uygun sayılacağına yer verilmiştir.

2.2. Ulusal Kaynaklar

2.2.1. Anayasa

Kişisel verilerin korunması alanı uzun yıllardır üzerinde konuşulan, tartışılan ve düzenlemeler yapılan bir alandır. Bununla birlikte birçok ülke hukukunda bu alan özel

[50] Akıncı, AN. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Kalkınma Bakanlığı, Çalışma Raporu-6, s. 14-19.

hayata saygı başlığı altında korunmaktadır. AİHS sözleşmesi m.8 de bu bakış açısıyla kişisel verileri korumaktadır. Ülkemizde ise anayasal düzeyde veri koruma, 2010 yılında yapılan değişiklikle dayanağını bulmuştur. Kişisel veri korumanın gelişim çizgisi incelendiğinde bazı kaynaklarca seyrin, 19. ve 20. yüzyılda haberleşme ve basın hürriyetinde yaşanan gelişmelere benzer şekilde olduğu belirtilmektedir. Bu haklar de özel hayatın gizliliği hakkı ile ilişki içerisindedir. Gelişim sürecince bu hakların önemi belirginleştikçe ayrı hukuki metinler düzenlenme yoluna gidilmiştir. Benzer durum kişisel verilerin korunmasında da görülmektedir.[51]

AY m.20 'Özel Hayatın Gizliliği' başlığını taşır. Bu maddenin 2. Fıkrası kişisel verilerin korunmasını düzenler. Buna göre: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."[52]

Ülkemizde kişisel verileri koruma çerçevesindeki gelişim ilk olarak 108 sayılı sözleşmenin 1981 yılında imzalanması ile başlamıştır. Daha sonra 2003 ve 2014 yıllarında iki kez kişisel verileri koruma kanunu için tasarı hazırlanmış fakat her ikisinde de yasalaşma süreci tamamlanamamıştır. 2016 yılına gelindiğinde yeniden bir tasarı hazırlanmış, bu sefer TBMM'de kabul edilerek yürürlüğe girmiştir.[53]

6698 sayılı Kişisel Verilerin Korunması Kanunu, 95/46 sayılı AB Direktifi temel alınarak hazırlanmıştır. Bu nedenle GDPR ile arasında bir takım değişiklikler, bazı konularda eksiklikler mevcuttur. GDPR'ın teferruatlı yapısı, alandaki teknolojik gelişmeleri barındırdığından bazı konularda daha detaylı ve daha işlevseldir. Bu

---

51 Kılınç D. Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. AÜHFD, 61(3), s. 1131

52 Küzeci, s. 291

53 Korkmaz İ. Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBB Dergisi,124, 2016, s. 86.

durumun yarattığı farklılıklar gelecekte yapılacak bir takım değişiklik ve düzenlemeler ile giderilmelidir.

KVKK'nın temel amacı adından da anlaşılacağı üzere kişisel verilerin korunmasını sağlamaktır. Bunu yaparken temel hak ve özgürlükleri korumak, özel hayatın gizliliği ilkesinin etkin bir şekilde kullanılmasını sağlamak üzere kişisel veri işleme faaliyetinde bulunan gerçek ve tüzel kişilerin hangi usül ve esaslarda çalışmaları gerektiğinin yol haritasını çizer. Yükümlülükleri belirler.

KVKK metninde kişisel sağlık verilerinin doğrudan tanımı yoktur. Sadece kanun metninde bu verilerin özel nitelikli veri kategorisinde olduğu belirtilmiştir. Kanun açık rızayı bu tür verilerin işlenmesi için şart koşsa da bazı istisnalar getirmiştir. Buna göre sağlık verisi yalnızca "kamu sağlığının korunması, koruyucu hekimlik, tıbbi tanı, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kimseler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir."

2.2.2. Kişisel Verilerin Korunması Kanunu

KVKK öncelikle Avrupa Birliği uyum komisyonunca tasarı halinde düzenlenmiş ancak 24.03.2016 tarihinde TBMM'de kabul edilerek kanunlaşmış ve 07.04.2016 tarihinde de resmi gazetede yayınlanarak yürürlüğe girmiştir.

KVKK, 95/46 AT Sayılı direktifi temel alarak düzenlenmiştir. Buna göre "kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi, manevi varlığı ile, temek hak ve özgürlükleri korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemek*"*tir.[54]

[54] Aksoy Hüseyin Can . Medeni Hukuk ve özellikle Kişilik hakkı yönünden kişisel verilerin korunması, Ankara, 2010, Çakmak yayınevi, s.106

KVKK'nin kişisel sağlık verileri bağlamında 6. Maddesi özel nitelikli kişisel verilerden söz eder. Özel nitelikli kişisel veri kavramı, GDPR'daki 'hassas veriler'in karşılığıdır. KVKK genel olarak özel nitelikli verilerin işlenemeyeceğini kabul etmiş, bununla birlikte bir takım istisnalar öngörmüştür. Bu istisnalar kanunda sınırlı sayıda kabul edilmiştir. Kişinin rızası, rızasını açıklayamayacak durumda olan kişinin, kendisi veya başkasının hayatını tehdit eden bir durum nedeniyle veri işlenmesinin zorunlu olması, ilgili kişiye yeterli korunma sağlanması koşuluyla, veri sorumlusunun kanunla tanınan hak ve yetkilerini kullanabilmesi veya yükümlülüklerini yerine getirebilmesi adına bu işlemenin zorunlu olması veya ilgili kişi tarafından alenen açıklanan veriler olması, bu tür özel nitelikli verilerin işlenebilmesi için aranan şartlardır.[55]

2.2.3. Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanun

1219 sayılı olan bu kanun 1928 yılında yürürlüğe girmiştir. Bu kanunun 70. Maddesinde tüm tıbbi işlemler için hastalardan rıza alınması gerektiği belirtilmiştir. Hastanın kısıtlı ve yaşı küçük ise bu rızanın çocuğun velisi ya da hastanın vasisi tarafından alınmasının gerektiği belirtilmiştir. [56]

2.2.4. Tıbbi Deontoloji Nizamnamesi

1960 tarihli ve 1517 sayılı bu nizamnamenin 4. Maddesi hekimin sır saklama yükümlülüğünden söz eder. Bu şekilde kişisel sağlık verilerinin korunmasını da sağlar. Burada istisna kanuni zorunluluk olması durumudur. Ayrıca hekim her hangi bir nedenle hastasının kimlik bilgilerini açıklamamalıdır. Hasta hekim ilişkisinde edindiği

[55] Yılmaz SS. Tıp Alanında Kişisel Verilerin Korunması. Seçkin yayınevi, 4. Baskı, Ankara, 2020, s.138

[56] Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanun (1928). RG, 863, 14.04.1928 http://www.resmigazete.gov.tr E.T:19.05.2023

tüm bilgileri hekimin sır saklama yükümlülüğü çerçevesinde korumakla yükümlüdür.[57]

2.2.5. Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik

KSVİMSY 2016 yılında resmi gazetede yayınlanarak yürürlüğe girmiştir. Fakat bu yönetmeliğin yürütmesi, Türk Dermatoloji Derneği ve Türkiye Psikiyatri Derneği'nin başvurusu sonucu durdurulmuştur. Gerekçe olarak o tarihte henüz kişisel verileri koruma kurulunun oluşturulmaması ve öngörülen tedbirlerin bu nedenle alınamaması olarak belirtilmiştir. Bu karar sonrası Sağlık Bakanlığınca "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik" metni yayınlanmıştır.[58]

Yönetmelikte yapılan değişiklik sonrası bu kez de Türk Tabipleri Birliği ve Türk Diş Hekimleri birliği yürütmeyi durdurma talebiyle başvurmuşlardır. Danıştay 15. Dairesi başvuruyu haklı bulup, gerekçesinde, kanuna aykırı olduğu kararı alınan yönetmeliğin birkaç maddesinin değiştirilerek kanuna uygun hale getirilemeyeceğini belirtmiştir.[59]

Kişisel sağlık verileri, hassas veriler olmaları nedeniyle özenle korunması gereken verilerdir. Bu korumanın yokluğunda ilgili kişilerin sosyal, ailevi, mesleki alanlarda geri dönüşü olmayan ciddi zararlara uğrayabilmesi mümkündür. Bu nedenle yürütmesi durdurulan yönetmelikle getirlmek istenen merkez sağlık veri sistemi oluşturulması ve tüm sağlık verilerinin buraya aktarılması durumu ortadan kalkmıştır. Bu uygulama hakkın özüne dokunur niteliktedir. Ayrıca kişisel sağlık verilerinin anonimleştirilmeden kullanılması, sağlık bakanlığı görevlilerinin sınırsız ve

[57] Tıbbi Deontoloji Nizamnamesi. http://www.mevzuat.gov.tr/MevzuatMetin/2.3.412578.pdf E.T:19.05.2023

[58] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (2017). RG, 30250, 24.11.2017 http://www.resmigazete.gov.tr/eskiler/2017/11/20171124-1.htm E.T. 19.05.2023)

[59] 09.10.2018 T. 2018/1490 E. http://emsal.danistay.uyap.gov.tr E:T:19.05.2023

kontrolsüz bir şekilde bu verilere ulaşabilmesi gibi kanuna aykırı düzenlemeler yürürlükten kaldırılmıştır.[60]

2.2.6. Hasta Hakları Yönetmeliği

23420 sayılı HHY, 1/8/1998 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiştir, Uluslararası alanda gelişmelere uygun bir şekilde düzenlenmiş olan önemli bir metindir. İçerisinde kişisel sağlık verilerinin korunması ile ilgili önemli birçok düzenleme bulunur. Yönetmeliğin md.5/f de özel hayatın gizliliği ve aile hayatın gizliliğine atıf yapılmıştır. Md.16-17 ise kişinin kendisi ile ilgili kişisel verileri hakkında tayin hakkından söz edilir. Buna göre kişiler, kendilerine ait verilerin eğer bir takım yanlışlar mevcut ise düzeltilmesini ve değiştirilmesini talep hakkına sahiptir. Bu durum enformasyonel self determinasyon hakkı olarak da tanımlanır. Yönetmelik kişisel sağlık verilerinin korunması bağlamında dayanak olması açısından önemlidir.

Yönetmeliğin 21. maddesi "Mahremiyete saygı gösterilmesi" başlığını taşır. Mahremiyete saygı gösterilmesi, kişinin sağlık hizmeti alırken her aşamada gözetilmesi gereken bir durumdur. Hastanın her koşulda gizlilik ilkesi içerisinde tanı ve tedavi hizmetlerine ulaşması sağlanmalıdır. Zorunlu haller dışında hastanın özel ve aile hayatına müdahale niteliği oluşturacak davranışlardan sakınılmalıdır. [61]

Yönetmeliğin 23. Maddesi 'Bilgilerin gizli Tutulması' başlığını taşır. Bu durum doğrudan kişisel sağlık verileri ile ilgilidir. Hastaya ait olan verilerin gizliliği esastır, kanuni bir takım zorunluluk halleri dışında veya hastanın rızası dışında üçüncü kişilerle paylaşılmamalıdır. Hatta kişinin rızası olsa bile kişilik haklarını sınırlayıcı hatta bu

[60] Dülger, Murat Volkan. Kişisel Sağlık Verileri Yönetmeliğinin Yürütmesinin Durdurulmasına İlişkin Danıştay'ın 09.10.2018 Tarihli Kararına İlişkin Değerlendirme, s.10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792286 E.T:19.05.2023

[61] Hasta Hakları Yönetmeliği (1998). RG, 23420, 01.08.1998. http://www.resmigazete.gov.tr E.T:19.05.2023

haklardan tamamen vazgeçmeyi içeren rıza durumunda bile bu verilerin açıklanması sorumluluğa yol açabilir.

2.3. Kişisel Verilerin Korunması Kanunu Kapsamındaki Yönetmelikler ve Diğer Düzenleyici İşlemler

Kişisel verileri koruma hukuku alanında ülkemizde yürürlükte olan temel kanun 6698 sayılı KVKK'dır. Bu kanuna dayanarak detaylandırılan düzenleyici işlemler mevcuttur. Bunlar; "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (KVSYAY)"[62] ve "Veri Sorumluları Sicili Hakkında Yönetmelik (VSSY)tir.[63]" Bu amaçla çıkarılan diğer düzenlemeler ise; "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"[64] ve "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"[65] dir. Kişisel Verileri Koruma Kurulunun "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili kararı bu düzenlemeler arasında sayılabilir.[66]

Tüm bu düzenlemeler kişisel veri koruma alanında işleyişi düzenleyen, usul ve esasları belirleyen önemli metinlerdir. Çalışmamız içerisinde konu bütünlüğü açısından bu düzenlemelerin detayına girilmeyecektir.

---

62 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik (2017). RG, 30224, 28.10.2017 http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm E.T: 19.02.2023

63 Veri Sorumluları Sicili Hakkında Yönetmelik (2017). RG, 30286, 30.12.2017. http://www.resmigazete.gov.tr/eskiler/2017/12/20171230-7.htm E.T: 19.02.2023

64 Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ (2018). RG, 30356, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm E.T:19.05.2023

65 Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ (2018). RG, 30356, 10.03.2018 http://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm E.T:19.05.2023

66 https://kvkk.gov.tr/Icerik/4110/2018-10 E.T19.05.2023

ÜÇÜNCÜ BÖLÜM
KORUNMASI GEREKEN BİR HAK OLARAK KİŞİSEL VERİLERİN KORUNMASI HAKKI VE YAKIN DİĞER HAKLAR İLE İLİŞKİSİ

1. KİŞİSEL VERİLERİN KORUNMASI HAKKI

Kişisel verilerin korunması hakkı uygulamada bazı haklar ile etkileşim içerisindedir. Bu haklar bazı durumlarda birarada çalışrken bazı durumlarda birbirleriyle çatışan haklar durumuna geçebilir. Bu haklardan bazıları daha önce bahsedildiği üzere özel yaşamın gizliliği hakkı, düşünceyi açıklama özgürlüğü , bilgi edinme hakkı, haberleşme özgürlüğü vb. haklardır.[67] Zaman zaman oluşabilecek bu çatışma hallerinin çözümü somut olay özelinde ve orantılılık ilkesi ile dengelenerek bulunmalıdır.

Kişisel verilerin korunması bağlamında temelde gözetilen hususun ne olduğu konusunda Kıta Avrupası ve ABD farklı değerlendirmeler yapmaktadır. ABD özelinde kişisel verilerin korunması kavramı bir ekonomik hak olarak değerlendirilirken Kıta Avrupası'nda bu hak, insan hakları çerçevesinde incelenir.

Kişisel verilerin korunması hakkını ekonomik hak olarak değerlendiren ABD görüşü, temelde kendi hukuki yapısı çerçevesinde bu değerlendirmeyi yapmıştır. Amerikan hukukuna göre özel yaşamın gizliliği korunmaktadır. Bunun içerisine kişisel verilerin korunması da girer. Bu haklar anayasada düzenlenmemiştir. Kişisel verileri ekonomik bir hak değerlendirmenin farklı yorumlamaları vardır. Bunlardan ilki mülkiyet hakkı teorisidir. Buna göre amaç kişisel verilere mülkiyet hakkı tanıyarak kişinin denetiminin sağlanması ve korumadan yararlanabilmesidir. Bu görüşü savunan yazarlar, kişisel veri sahibini bireylerin, verileri kullanıldığı durumda karşılığını alabileceklerini, özel hayatın gizliliğine önem verenlerin bu izni vermeyeceklerini, diğerlerinin ise istediği kişi veya şirketlere satabileceğini öne sürmektedir. Yine bu görüşü savunanlara göre kişisel verilerin kötüye kullanılması durumunda kişinin

[67] Küzeci, s.66.

doğrudan dava açma veya zararının giderilmesi için talepte bulunma imkanı doğmasıdır. Ekonomik yaklaşım ile ilgili endişelerden birisi ise tarafların eşit olmadığı durumlarda bu durum dezavantaj oluşturabilmesidir. Daha varlıklı olan kesim diğerlerinin verileri üzerinde inisiyatif kazanabilecek, hatta kişilerin kendi verilerinin denetimini kaybetmesi sonucu doğabilecektir.

Bir diğer görüş ise fikri mülkiyet kavramı üzerinden konuya yaklaşır. Fakat kişisel verilerimizin fikir ürünü olarak nitelendirilmesi çok makul değildir ve kişisel verileri korumak bu şekilde olanaklı görülmemektedir.[68]

Daha az destek bulan güven teorisi veya ticari sırlara uygulanan bazı hükümlerle koruma yaklaşımları da mevcuttur. Konuyu çok genişletmemek adına bu görüşlerin detayına girilmeyecektir.

Kişisel verilerin korunmasını insan hakkı olarak değerlendiren görüşe göre, özellikle günümüz bilişim teknolojileri ile birlikte kişisel verileri işlenen, aktarılan, toplanan bireylerin aleyhine ortaya çıkan dengesizliğin giderilmesi, doğrudan insan onuru ve kişiliğin serbestçe geliştirilmesi hakkı ile ilişkili olarak değerlendirilir. Kişisel verilerin insan hakkı olarak değerlendirilmesi, kişilerin bu verilerin nerede, ne şekilde işlendiği, nereye aktarıldığı konusunda da bilgi sahibi olabilme hakkını tanır. Kişisel verilerinin sürekli toplandığı, takip edildiği düşüncesi kişinin kişiliğini serbestçe geliştirebilmesinin önünde de ciddi bir engel oluşturur. Kişisel verilerin korunmasını insan hakkı olarak değerlendiren yaklaşım kişinin *özneden nesneye dönüşmesini önleyici bir yol* olarak değerlendirilir.[69]

[68] Küzeci, s.71.
[69] Şimşek O. Anayasa Hukukunda Kişisel Verilerin Korunması. Beta, İstanbul, 2008, s.112.

2. ÖZEL YAŞAMIN GİZLİLİĞİ HAKKI

Özellikle Anglo-Amerikan sisteminin olduğu ülkelerde özel yaşamın gizliliği hakkı, kişisel verilerin korunması hakkını içerir şekilde düzenlemektedir. Oysa her ne kadar yakın ilişki içerisinde de olsalar, bazı noktalarda birbirlerinden ayrılmaktadırlar.

Özel yaşam alanı denilen kavram tanımlanması güç ve sınırları her zaman keskin bir şekilde belirlenemeyen bir kavramdır. Genel olarak kişinin diğer insanlardan tamamen uzak tuttuğu sır alanı ile sadece belirli kişilerle paylaştığı özel yaşam alanını kapsadığı kabul edilir. Bu iki alan dışında kalan ve genel yaşam alanı olarak da adlandırılan alan da tamamen korumasız değildir. Kamuya ait alanlarda kişinin görüntüsünün, ses kaydının alınması hala tartışmalara yol açsa da bu alanda da temel ilkelere uyulmalıdır.[70]

3. DÜŞÜNCEYİ AÇIKLAMA ÖZGÜRLÜĞÜ

Düşünceyi açıklama özgürlüğü denildiğinde bu bazı eylemleri içinde barındırır. Öncelikle bunun için kişinin serbest bir şekilde bilgi ve düşüncelere ulaşabilmesi gerekir. Bununla birlikte sahip olduğu fikirleri rahatlıkla açıklayabilmesi, bunu toplu halde ya da bireysel olarak yapabilmesi gerekir. Aynı şekilde düşünceyi açıklama yollarının seçimi de kişinin kendi iradesince ve istediği biçimde olabilmelidir. Ancak bu şekilde düşünceyi açıklama özgürlüğünden bahsedilebilir.[71]

Kişisel verilerin korunması hakkı bazı durumlarda düşünceyi açıklama özgürlüğü ile çatışabilir. Özellikle bu konuda magazin basını denilen bir kavram öne çıkmaktadır. Bu alanda çalışan basın mensupları bu tür kişisel verilere ulaşmaya çalışırken, diğer yandan bu kişiler bu tür verilerin paylaşılmasını engellemeye çalışabilmektedir. Bu çatışmaya Amerikan hukukunda *'kamusal figür'* olarak tanımlanan bir kavramın oluşumuna yol açmıştır. Buna göre bu konumda olarak değerlendirilen kişilerin özel yaşamın gizliliği hakkının diğer kişilere nazaran daha kısıtlı olduğu kabul

[70] Küzeci, s.80
[71] Tanör, Bülent. Türkiye'de insan hakları sorunu, BDS yayınları, 3. Baskı, İstanbul, 1994, s.59

edilmektedir. Fakat bu durum kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı arasında doğrudan bir çatışmayı göstermez. Burada önemli olan, dengenin sağlanması ve orantılılık ilkesinin olaya özgü koşullara uygulanmasıdır.[72]

4. BİLGİ EDİNME HAKKI

Bilgi edinme hakkı ve kişisel verilerin korunması hakkı, bilgi toplumlarında birbirlerini tamamlayan bir yapıya sahiptirler. Genellikle bu hakların kullanımını denetleyen yapılar da aynı çatı altındadır. Kişiler, devlet tarafından kendileri ile ilgili tutulan verilere ulaşmayı talep edebilirler. Bu devletin şeffaflığı ile ilgilidir. Kişisel verilerin korunması ile ilgili ilkeler ise özellikle kişinin verilerine, bilgi edinme hakkı çerçevesinde ulaşmak isteyen kişiler açısından bariyer oluşturur. Eğer kişisel verilere ulaşım hiçbir engel olmazsa kişiler verileri üzerindeki denetimlerini kaybederler. Yönetimde genel olarak şeffaflık ilkesi geçerli iken, devlet bünyesinde toplanan kişisel veriler için bu ilke geçerli değildir. Burada önemli olan bilgi edinme hakkının işlevselliğini yitirecek kadar sınırlama yapılmamasıdır.[73]

Mahremiyet hakkı her ne kadar üzerinde çok eski zamanlardan beri tartışılan bir konu olsa da, özellikle bilişim teknolojilerinin gelişmesi ile birlikte üzerine hassasiyetle eğilinmesi gereken bir duruma evrilmiştir. 1960 lı yıllardan itibaren verilerin otomatik olarak işlenmesini sağlayan bilişim teknolojileri ile birlikte bu veriler belirli merkezlerde toplanmaya ve işlenmeye başlamıştır. Bu veri bankaları özellikle devletlerin bireyler üzerinde bilgi hakimiyetlerini arttırma riski taşıyacağından, bireyler tarafından bir takım koruyucu taleplerin oluşturulmasına zemin hazırlamıştır.

Kişisel verilerin korunması temelde devlete karşı bireyin özerkliğinin korunması ve demokratik toplumun devamlılığı için zorunludur.[74] Bu konu ile ilgili Avrupa'daki ilk mevzuat düzenlemesi 7 Ekim 1970 tarihinde Almanya Hessen eyaletinde düzenlenen

[72] Küzeci s.95
[73] Küzeci, s.105-106
[74] Küzeci, s.52

Kişisel verilerin korunması kanunudur.[75] Bu düzenlemede, kişisel verilerin yetkisi olmayan üçüncü kişilerden korunması, veri işleyen kişilerin sır saklama yükümlülüğü ve kişisel verilerde olan yanlışların düzeltilmesini talep etme hakkı düzenlenmiştir.[76] Almanya'da 1977 yılında Federal Veri Koruma Kanunu yürürlüğe girmiştir. Fransa'da veri işleme Hürriyetler Kanunu (Loi informatique et libertés) 6 Ocak 1978 tarihinde kabul edilmiştir. Bu kanunla "bağımsız bir idarî otorite" olarak yetkilendirilmiş olan CNIL (Bilişim ve Özgürlükler Ulusal Komisyonu/Commission Nationale de l'informatique et desLibertés) kurulmuştur. Bu Komisyonun bağımsız nitelikte olması önemlidir ve esas olarak Fransız Veri Koruma kanunun, pratikte uygulanmasını sağlamakla yükümlüdür.[77]

Kişisel verilerin korunması ile ilgili mevzuat İngiltere'de 1998(Veri koruma Kanunu), Avusturya'da 1980(Federal Kişisel Verilerin Korunması Kanunu), İsviçre'de 1992(Federal Veri Koruma Kanunu) yılında yürürlüğe girmiştir. İngiltere'de mevcut mevzuatın uygulanması ile ilgili kurum ICO (The Information Commissioner's Office / Bilgi Komiserliği Ofisi) adında, malî yönden Adalet Bakanlığı'na bağlı bir kurumdur. Bu nedenle kurumun bağımsız olduğunu söyleyebilmek pek mümkün değildir. [78]

Kişisel verilerin korunması alanında en önemli kararlardan bir tanesi Alman Federal Anayasa Mahkemesi'nin 'Nüfus Sayımı' kararıdır(15 Aralık 1983). Buna göre Federal Anayasa Mahkemesi kişisel verilerin korunmasını, insan onuru ve kişilik hakkı çerçevesinde ele almıştır. Kişisel verileri meşru bir dayanağa bağlı olmaksızın toplanan, işlenen ya da aktarılan bir kişinin hürriyetinden bahsedilemeyeceği ve kendisiyle ilgili bilgilere başkalarının sahip olduğu bilinciyle hareket eden bir bireyin

---

[75] Rodriguez R, Wilson J, Petra J, Schanz SJ. The Regulation of Privacy and Data Protection in The Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to personal-Identifiable Health Databases, Washington 2001, s.76.

[76] Çekin, s.5

[77] U.S. Congress, Office of Technology Assessment: Federal Government Information Technology: Electronic Record Systems and Individual Privacy, Washington 1986, s.151 https://ota.fas.org/reports/8606.pdf E.T:19.05.2023

[78] Taylor MJ. Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge 2012, s.147

hür kararlar alamayacağı ve kişiliğini geliştiremeyeceği belirtilmiştir. Federal mahkeme otomatik veri işlemenin tehlikelerine değinmiş ve demokratik düzenin temeli olan farklı fikirlerin çatışmasını engelleyeceği ihtimalini belirtmiş ve bu nedenle kişisel verilerin korunmasını temel bir hak olarak tanımlamıştır. [79]

Avrupa Birliği bünyesindeki ilk düzenleme ise 95/46/EC nolu yönergedir. Daha sonra 2016/679 no'lu düzenleme ile GDPR yürürlüğe girmiştir.

Türk Hukukunda 5982 sayılı kanun md.2 çerçevesinde Anayasa'nın 20. Maddesine eklenen 3. Fıkrasında, "Herkes, kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunlarla düzenlenir." denilmektedir.

5237 sayılı Türk ceza kanununda Kişisel verilerin hukuka aykırı kaydedilmesi suçu (md.135) Hukuka aykırı verilmesi ya da elde edilmesi suçu (md.136) ve yok edilmemesi suçu (md.138) hallerinde cezai yaptırımlar bulunmaktadır.[80] Daha sonra Türk Hukukunda 7.4.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanununu yasalaşmıştır. Kişisel Verileri Koruma Kurumu da yönetmeliklerle detaylı düzenlemeleri yapmaya devam etmektedir.[81]

[79] Çekin, s.7
[80] Dülger, s.305-382
[81] Çekin, s.9

DÖRDÜNCÜ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI KANUNUNDA ADI GEÇEN BAZI KAVRAMLAR VE BU KAVRAMLARIN ULUSLARARASI MEVZUAT İLE KARŞILAŞTIRILMASI

1. KVKK'DA KULLANILAN BAZI KAVRAMLAR

1.1. Kişisel Veri

Kanundaki tanımına göre kişisel veri "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak belirtilmiştir. Burada gerçek kişi kavramı önemlidir. Artık hayatta olmayan insanlar kural olarak bu kanunun kapsamı dışındadır. Eğer ölen kişiye ait olan veri hayatta olan bir kişiyi de etkiliyorsa kişisel veri olarak kabul edilmesi söz konusu olabilecektir. Özellikle genetik hastalıklar bu konuda önem arz etmektedir.

1.2. Belirlenebilirlik

Bu kavrama göre verinin sadece kendisi, ilgili kişiyi tespit için yeterli değildir. Ancak diğer verilerle birleştirildiğinde kişiyi belirleyebiliyorsa belirlenebilirlikten söz edilebilmektedir.

Belirlenebilirlikten söz ederken bahsedilen diğer veriler açısından iki durum mevcuttur. Bunlar mutlak belirlenebilirlik ve nisbi belirlenebilirlik durumlarıdır. Mutlak belirlenebilirlikten kasıt veri sorumlusunun sahip olup olamayacağına bakılmaksızın diğer verilere birleştirildiğinde belirlenebilirlik sağlanabilmesi durumudur. Oysa nisbi belirlenebilirlik için veri sorumlusunun kimliği, bilgisi gibi durumlar göz önünde bulundurulacaktır.

1.3. Kişisel Verilerin İşlenmesi

Kanunda bu kavram "kişisel verilerin 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 işlem" denilerek detaylandırılmış ama bunlarla sınırlandırılmamıştır.

AB Yönergesi'ne göre ise: "Kişisel Verilerin işlenmesi, toplama, kaydetme, düzenleme, saklama, uyarlama veya değiştirme, geri alma, danışma, kullanma, ileti ile açığa çıkarma, yayma veya başka şekilde oluşturma, sıraya koyma veya birleştirme, engelleme, silme veya yok etme gibi otomatik olan ya da olmayan araçlarla, kişisel veri üzerinde uygulanan her türden işlem veya işlem dizisi anlamına gelir." [82]

1.4. Veri Sorumlusu

KVKK'na göre veri sorumlusu "Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmaktadır. Buna göre veri sorumlusu, veri koruma hukuku çerçevesinde yapılması gereken tüm organizasyonel ve yönetsel süreçlerin, belirlenen amaç doğrultusunda yapıldığını, hesap verilebilirlik ilkesi gözetilerek bütünsel olarak sağlamak yükümlülüğü altındadır.[83]

1.5. Veri İşleyen

Bu kavramın genel olarak veri sorumlusu kavramından ayırt edilmesi önemlidir. Esas olarak veri sorumlusunun gözetimi ve belirlediği amaç doğrultusunda çalışan veri

[82] AB yönergesi md. 2b
[83] Çekin, s.48-49

işleyenin sorumluluğu, veri sorumlusuna oranla hayli kısıtlı olmakla beraber müteselsil bir sorumluluğun olduğu değerlendirilebilir.

2. KİŞİSEL VERİLERİN KORUNMASI KANUNUNDA ADI GEÇEN BAZI KAVRAMLARIN ULUSLARARASI MEVZUAT İLE KARŞILAŞTIRILMASI

2.1. KVKK'daki Veri Sorumlusu ve Veri İşleyen Kavramının Uluslararası Hukuk İle Karşılaştırılması

108+ sayılı Kişisel Verilerin İşlenmesine Karşı Bireylerin Korunmasına ilişkin Sözleşme 17-18 Mayıs 2018 yılında Danimarka'da imzalanmıştır. Amaç, daha önce imzalanmış olan 108 sayılı sözleşmenin GDPR'a uyumlu hale getirilmesidir. Sözleşmenin 2. Maddesinde 'kontrolör' ve 'işlemci' kavramları tanımlanmıştır. Bu kavramlar sırasıyla KVKK'daki 'Veri sorumlusu' ve 'Veri İşleyen kavramlarına benzer içerikler taşımaktadır. Sözleşmede kontrolör, "Tek başına veya başkalarıyla birlikte veri işleme konusunda karar verme gücüne sahip olan gerçek veya tüzel kişi, kamu otoritesi, hizmet, ajans veya herhangi bir diğer organ" işlemci ise, "denetleyici adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi, hizmet, ajans veya başka herhangi bir kuruluş" olarak tanımlanmıştır.

GDPR m.4'te kontrolör, "Kişisel verilerin işlenmesinin amaçlarını ve araçlarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer organ' işlemci ise 'kişisel verileri denetleyici adına işleyen gerçek veya tüzel kişi, kamu otoritesi, ajans veya başka bir organ" olarak tanımlanmıştır.

KVKK'ya göre her ne kadar veri sorumlusu ve veri işleyen kavramı birbirinden ayrı olarak tarif edilmiş olsa da emir verme, bağımlı olma gibi durumları birlikte değerlendirdiğimizde bu iki kavram arasındaki ayrımın bazı durumlarda net olmadığı görülebilecektir. Örneğin bazı durumlarda veri işlemcisi, veri sorumlusunun bulunduğu ve organize ettiği alan dışında olabilecektir. Bu durumda denetimin nasıl sağlanacağı konusu gündeme gelebilir. Ayrıca bu kavramlar arasındaki organizasyon,

veri minimizasyonu, ihlallerin engellenmesi, veri aktarımının sınırlandırılması gibi kişisel verileri ve kişileri koruyacak şekilde yapılmalıdır. Bu durumla uyumlu olarak veri sorumlusu ve veri işleyen kavramlarının aynı anda, birlikte ve aynı çatı altında bulunabileceğini göz önünde bulundurmak önemlidir. Bu kavramlar konusunda keskin değerlendirmeler yapmak yerine uygulanabilir ve duruma göre yaklaşımlar daha kullanışlı olacaktır. Bazı durumlarda veri sorumlusu görevlerini veri işleyenlere devrederek yürütebilmektedir. Bu durumun bilinmesi ve kabul edilmesi sorumluluk rejimi açısından daha pratiktir.[84]

2.2. Kişisel Sağlık Verisi/Özel Nitelikli Kişisel Veri

Kişisel veriler '*kimliği belirli ve belirlenebilir bir kişiye ait tüm veriler*' olarak tanımlanırken kişisel sağlık verisi, kişinin herhangi bir sağlık kurumunda aldığı sağlık hizmeti sırasında yapılan tüm işlemler olarak nitelendirilebilir. Bu veriler, kişilerle ilgili sağlık meslek mensuplarının edinebileceği tüm veri olarak da değerlendirilebilir. Sağlık ile ilgili kayıt altına alınan, arşivlenen de dahil olmak üzere, hizmet sunumu öncesinde, sırasında, sonrasında elde edilen tüm veriler hassas veri niteliğinde olup KVKK'nın 6. Maddesi kapsamında 'Özel Nitelikli Kişisel Verilerin İşlenme Şartları' başlığı altında düzenlenmiştir.

GDPR md.4 f.15 de sağlık verilerinin tanımı yapılmıştır. Bu tanıma göre kişinin sağlık durumu hakkındaki verileri dahil kişinin fiziksel ve zihinsel sağlığı ile ilgili her türlü veri kişisel sağlık verisi tanımı içerisine dahildir. Kişinin mevcut sağlık verisi yanında klinik tüm tanıları, muhasebe ve özel sağlık sigortasına ilişkin veriler, fitness verileri gibi bazı verilere kadar bu aralık genişletilebilir. Bu bilgilere doğrudan ulaşılabileceği gibi bazen de verilerin birleştirilmesi yoluyla ulaşılabilir. Örneğin kişi adına satın alınan bir protez cihazı bilgisine fatura yoluyla ulaşılabilir ve bu bilgiyle kişiye hangi

[84] Yılmaz SS. Tıp Alanında Kişisel Verilerin Korunması. Seçkin yayınevi, 4. Baskı, Ankara, 2020, s.67-71

ameliyat yapıldığı bilgisi tahminlenebilir. [85] Yenilenen 108+ sayılı sözleşmede, hassas kişisel veriler sınırlı sayıda sayılmış ve şu başlıklar halinde kategorize edilmiştir;

- Genetik Veriler
- Suç ve Ceza mahkumiyetine ilişkin veriler ile güvenlik tedbirine ilişkin veriler
- Biyometrik veriler
- Irk, etnik köken, politik görüş, sendika üyeliği, dini ve diğer ilaçları
- Sağlık ve cinsel verileri

Böylelikle hassas veri kategorisinin genişletildiği, genetik ve biyometrik veri kategorilerinin 108+ sözleşmesine eklendiğini görülmektedir.[86]

Teknolojinin ve bilişim sisteminin gelişimi, bilişim sistemlerinin tıpta yaygın bir şekilde kullanımı sonrası, sosyal güvenlik merkezi kayıtları, özel ve kamu hastanesi kayıtları, eczane kayıtları belirli merkezlerde toplanmaktadır. Bu kayıtlar MEDULLA adı verilen bir sistemde toplanmaktadır. Ayrıca hasta bilgileri e-nabız denilen sistem üzerinden kişi, grup ya da kurumlar tarafından görülebilmektedir. Bu bilgilere hekimler, yardımcı sağlık personeli, Sosyal Güvenlik kurumu çalışanları, bazı durumlarda maliye bakanlığı ve adli makam çalışanları ulaşabilmektedir.

Hekimlik Meslek Etiği Kuralları md.9 da "Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz. Hastanın onam vermesi ya da sırrın saklanmasının hasta ya da öteki insanların yaşamını tehlikeye sokması durumunda, hastanın kişilik haklarının zedelenmemesi koşuluyla, hekim bu sırrı saklamakla yükümlü değildir. Yasal zorunluluk durumlarında hekimin rapor düzenlemesi de, meslek sırrının açıklanması anlamına gelmez. Hekim, tanık ya da bilirkişi olarak mahkemeye çağrıldığında olayın meslek sırrı olduğunu ileri sürerek bu görevlerinden

[85] Yılmaz SS. Tıp Alanında Kişisel Verilerin Korunması. Seçkin yayınevi, 4. Baskı, Ankara, 2020, s.58-59

[86] https://www.coe.int/en/web/data-protection/convention108-and-protocol E.T:30.4.2023)

çekilebilir.” denilmektedir. Mevzuat düzenlemelerinden açıkça görülebileceği üzere kişisel sağlık verilerinin paylaşılması sıkı koruma önlemleri altındadır.[87]

Bu yükümlülük hekimler için olmakla birlikte aynı şekilde diğer sağlık meslek mensupları için de geçerlidir. Ayrıca meslek sırrı kavramı teknolojini gelişimi ve verilerin bilişim platfomlarınca hızlı paylaşımı bu yükümlülüğü daha önemli hale getirmektedir.[88]

[87] https://www.ttb.org.tr/kutuphane/h_etikkural.pdf E.T:30.04.2023

[88] Yılmaz SS. Tıp Alanında Kişisel Verilerin Korunması. Seçkin yayınevi, 4. Baskı, Ankara, 2020, s.63

BEŞİNCİ BÖLÜM
KANUNDA ESAS ALINAN TEMEL İLKELER

Bu ilkeler KVKK Md. 4 de düzenlenmektedir.

1. KİŞİSEL VERİ İŞLENMESİNİN KURAL OLARAK YASAK OLMASI

Kişisel verilerin işlenmesi, kanunda belirtilen meşru gerekçeler olmadıkça, kural olarak yasaktır. Meşru gerekçeler; kanunda açıkça belirtilmesi ya da kişini açık rızasının olmasıdır.

2. HUKUKA VE DÜRÜSTLÜK KURALLARINA UYGUNLUK

Hukuk kurallarına uygunluk aslında hukuk devleti ilkesinin bir sonucudur. Dürüstlük kurallarına uygunluk ilkesinin amacı ise kişisel veri işleyenlerin, kanunun kendilerine verdiği yetkiyi kullanırken bile, bunun kötüye kullanımını engellemektir.

Hukuk kurallarına uymanın sınırları yasalarla belirlenebilirken, dürüstlük kurallarına uyma kuralının çerçevesini çizmek çok kolay değildir. Medeni hukuk açısından değerlendirilecek olursak "Dürüstlük kuralı bir kimseden namuslu, dürüst bir insan olarak beklenen davranışı ifade eder. Bir davranışın bu nitelikte olup olmadığı, toplumda egemen olan ahlaki ölçülere, geçerli adetlere, hakları sağlayan ilişkilerin amacına göre tayin edilir."[89]

3. AMACA BAĞLILIK İLKESİ

Kanunda md. 4'de belirtilen amaca bağlılık ilkesinin esas gayesi; verinin hangi amaçla işleneceği bilgisinin önceden belirlenmesiyle, ilgili kişinin neye rıza verdiğini bilmesi, aynı zamanda veri sorumlusunun da hangi amaçla veri işleyeceğinin net bir

[89] Oğuzman K, Barlas N. Medeni Hukuk 15. Baskı, Vedat kitapçılık, İstanbul, 2008 s.222

çerçevesinin çizilmesi ve buna yönelik davranmasının sağlanması, gereksiz ve ölçüsüz veri işlemenin önüne geçilmesidir.[90]

Ayrıca kişisel verilerin belirli amaç doğrultusunda işlenmesi sürecinde ortaya çıkabilecek yeni durumlarda ilgili kişinin yeniden rızasının alınması gerekecektir. Bu durum kanunda "Sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5. Maddede düzenlenmiş olan kişisel verilerin işlenme şartlarından birinin gerçekleşmesi gerekecektir." şeklinde belirtilmiştir.

4. ŞEFFAFLIK İLKESİ

Bu ilkenin esas amacı kişisel verisi işlenen kişinin, bu verilerin akıbeti ile ilgili takibi sağlayabilmesi, diğer bir ifade ile kişisel verisi üzerindeki hakimiyetinin devamlılığıdır.[91] KVKK Md. 10 ve 11 de bu ilkeden bahsedilir. Şeffaflık ilkesinin şekli ve maddi olarak iki boyutundan bahsedilebilir. [92]

Şekli boyut açısından bakılacak olursa, aydınlatma yükümlülüğünü yerine getirirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir. Açık, sade ve anlaşılır bir dil kullanılmalıdır. Maddi boyutta ise aydınlatmanın içeriği önem kazanır. Buradaki bilgilendirme veri sorumlusunun kimliği, verinin hangi amaçla toplanacağı gibi bilgileri sağlarken, aynı zamanda kişilere yanlış verileri düzeltme, silinmesini isteme gibi haklar da sağlar.

---

[90] Çekin, s.65
[91] Çekin, s.70
[92] Aşıkoğlu Şİ (2019). Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-, Kişisel Verileri Koruma Dergisi. 1(2), 41-65.

5. DOĞRU VE GÜNCEL OLMA

KVKK'ya göre veri sorumlusu, kişisel verilerin doğruluğu ve güncelliği konusunda dikkat ve özen yükümlülüğüne uygun davranmakla ve gereken önlemleri almakla yükümlüdür.

6. İŞLENDİKLERİ AMAÇLA SINIRLI VE ÖLÇÜLÜ OLMA

Kişisel veri işleme işlemlerinde ölçülülük esastır. Buna göre; eğer belirtilen amaca başka bir takım araçlarla ulaşılabiliyorsa kişisel veri işlenmemelidir. Ama bu mümkün değilse, burada kullanılacak olan metod veri minimizasyonu da denilen, kullanılacak minimum veriyle belirtilen amaca ulaşılabilmesi çabası olmalıdır.

KVKK'da bu durumu somutlayan bir açıklama mevcut değilken, tüzükte bu durumun gerçekleştirilebilmesi açısından asgari miktarda veri işlemenin sağlanması ve bunun için teknik ve organizasyonel bir takım önlemlerin alınmasını emretmektedir.(Privacy by Design, Privacy by Default)

Kişisel verilerin '*bir gün gerekli olursa'* mantığıyla bir amaç doğrultusunda olmaksızın kullanılması, kişilerin kendilerini özgürce ifade etmesini engelleyebilir. Bu durum kişilerin maddi-manevi bütünlüğü, kişiliğini geliştirme hakkı, suçsuzluk karinesi gibi demokratik toplumun temel değerlerine gölge düşürebilir.[93]

[93] Küzeci, s.231

ALTINCI BÖLÜM
KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

AY m.20 f.3'de kişisel verilen "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği hüküm altına alınmış ve temel bir hak olarak nitelendirilmiştir. KVKK md.5 ve devamında kişisel verilerin işlenme şartları düzenlenirken aynı zamanda md. 4'de belirtilen temel ilkelere de uymak gerekecektir.[94] Bu bağlamda Anayasada geçen açık rıza kavramının hukuki değerlendirmesini yapmak önemlidir.

1. AÇIK RIZA

Gerek basit nitelikte kişisel veriler, gerekse kişisel sağlık verileri gibi özel nitelikli kişisel verilerin işlenmesi genel olarak ilgili kişinin rızasına bağlıdır. KVKK md. 3 de açık rıza kavramı detaylandırılmıştır. Buna göre "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" tanımlaması yapılmıştır. Kanunumuza göre rıza gösteren kişinin ayırt etme gücüne sahip olması zorunludur.[95] Bu açıdan ayırt etme gücüne sahip olanlar, 18 yaşından küçük olsa bile geçerli rıza açıklamasında bulunabilirler.[96] Tüzük Md.8'e göre 16 yaşından büyük çocukların rızalarını meşru kabul edilirken bundan daha küçüklerde yasal temsilcinin rızasını aranacaktır. Üye ülkelere bu sınırı 13 yaşa kadar çekebilme yetkisi tanınmıştır.

Alınacak açık rızanın veri işleme faaliyetinden önce olması esastır. Aksi durumda tam aydınlatma gerçekleşmemiş olacağından sonradan alınan rıza meşru ve geçerli olmayacaktır.

---

[94] Çelikel S. Kişisel Verilerin İşlenmesinde, Açık Rıza HukukaUygunluk Nedeninin, 95/46 Sayılı Direktif ve Gdpr'la Karşılaştırmalı Olarak İncelenmesi, Uyuşmazlık Mahkemesi Dergisi - Yıl 9, Sayı 17, Haziran 2021, s. 161-190

[95] Cassani C. Hukuka Uygunluk Nedeni Olarak Hukukta Rıza, TBB Dergisi, Sayı 77, 2008, S.236-248

[96] Uçak M.Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası, Kişisel Verileri Koruma Dergisi. 3(1),2020, s.41-60

Açık rızanın metninin içeriğinde; veri sorumlusunun kimlik bilgileri, kişisel verinin işlenme amacı, açık rızayı geri alabilme imkanı, yeterli koruma durumu, yurt dışına aktarılan verilere dair riskler hakkında bilgiyi içermelidir.

Açık rıza, ilgili kişinin talebi üzerine geri alınabilir. "Kişisel Verilerin Silinmesi, Yok edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" md. 5 de "kişisel veri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde ilgili kişinin rızasını geri alması" durumunda artık kişisel veri işlenme koşullarının karşılanamadığı açıktır. Fakat bunun yöntemi yönetmelikte açık değildir. Açık rıza geri alındığında o zamana kadar ki veri işleme geçersiz olmamakla birlikte ileriye yönelik bir veri işleme faaliyeti gerçekleştirilmeyecektir.

Açık rıza için belirtilen genel açıklamalar dışında, kişisel sağlık verilerinin işlenmesi açısından önemli olan bir diğer husus ise HHY 23. md. uyarınca "alınan açık rızanın bile, ilgili kişinin haklarından tamamen vazgeçmesini, bu hakların devrini veya sınırlandırılmasını meşru kabul etmediği"dir. Bu düzenlemeler kişiliğin korunması ile ilgili düzenlemeler ile uyuşmaktadır. Fakat burada üzerinde durulması gereken bir diğer husus, tıbbi müdahaleler kapsamında alınan hasta rızasının öncesinde, bilgilendirmenin yapılması ardından alınan açık rızanın geçerliliği konusudur. Burada ayrımı yapılması gereken husus Hasta Hakları yönetmeliğinde belirtilen rızanın, kişisel verilerin işlenmesine yönelik değil, kişiye yapılacak tıbbi müdahaleye, beden bütünlüğüne yapılacak müdahaleye dair olduğudur. Bu nedenle kişisel verilerin işlenmesi için alınan rızayı, Hasta Hakları yönetmeliğinde bahsedilen rızadan ayırt etmek ve bunu bilgilendirme kısmında açıkça belirtmek gereklidir. Veri koruma hukuku açısından hastalardan alınan rıza için esas gereklilik ise hür irade ile alınmış olmasıdır. İlgili kişi üzerinde baskı kurulması, uygulanacak tıbbi girişiminin bu rızanın verilme koşuluna bağlanması, ölçülülük ilkesini aşacak şekilde şartlar koşulmamasına dikkat edilmesi konusu önem arz etmektedir.[97]

[97] Çekin, s.200

2. KANUNDA ÖNGÖRÜLEN HUKUKA UYGUNLUK SEBEPLERİ

Öncelikle şu belirtilmelidir ki tüm hukuka uygunluk sebepleri aynı öneme sahiptir. Aralarında hiyerarşik bir sıralama mevcut değildir.[98] KVKK md.5 e göre "Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgisi olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi" durumunda açık rızaya ihtiyaç duyulmayacaktır. Bunun gibi durumlarda sözleşme ilişkisi, taraflar gibi kavramlar değerlendirmeye alınacaktır.

Kanunda belirtilen bir diğer durum ise meşru menfaat durumudur. Buna göre; "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" durumunda açık rızaya ihtiyaç duyulmayacaktır.

Kişisel Sağlık Verileri hakkında yönetmelik md.6 çerçevesinde "Sağlık hizmeti sunumunda görevli kişiler, ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla erişebilir." Bu yönetmelik içerisinde hangi görevlinin ne kadar süre bu verilere ulaşabileceği, hatta ilgili kişinin istemesi halinde, sadece sağlık görevlisine vereceği bir şifre ile bu verilere ulaşabilmesi imkanı sunulmaktadır. Aynı yönetmelik md.7 de kişisel sağlık verilerine bakanlık birimlerinin erişimi konusu düzenlenmiştir. Bu verileri kimlerin, hangi şartlarda işleyeceği belirlenmiştir.

Ayrıca kişisel sağlık verilerine avukatların erişimi de belli şartlara bağlanmıştır. Kişisel sağlık verileri hakkında yönetmelik md. 10'da bu verilere avukatların ulaşımı için genel vekaletin yeterli olmadığı, "ilgili kişinin özel nitelikli kişisel verilerinin işlenmesi ve aktarılmasına ilişkin açık rızasını düzenleyen özel bir hüküm bulunması" gerektiği belirtilmiştir.

[98] Yücedağ, s.765-790.

Aynı yönetmelikte çocukların sağlık verilerine erişimi konusu da düzenlenmiştir. Buna göre "Ebeveynler, çocuklarına ilişkin sağlık kayıtlarına herhangi bir onaya ihtiyaç duyulmaksızın e-nabız üzerinden erişebilir. Ayırt etme gücüne sahip çocuklar, sağlık geçmişlerine ebeveynlerin erişimini e-nabız üzerinden izne tabi tutabilir." (md.8)

Bunlar dışında kişisel Sağlık verilerine ulaşım yetkisi bazı kanunlarca tanınmaktadır. 5502 Sayılı Sosyal Güvenlik Kurumu Kanunu md.35 5.fıkrasında ilgili kanunun verdiği görevleri yerine getirmek amacıyla kişisel verileri işleyebilmekte, bu yetkinin dışında kalan hallerde ise 10/12/2003 tarih ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun eki (I) (II) (III) (IV) sayılı cetvellerde yer alan kanunlarda belirtilen görevleri yerine getirebilmek adına ihtiyaç duyduğu sağlık verisi dışındaki kişisel veriler ile ticari sır niteliğindeki verileri paylaşabilmektedir. Yine bilimsel araştırma, planlama, istatistik amaçlar için kamu idareleri bu verileri araştırma yapan kamu personeli, bilimsel dernekler ve üniversiteler gibi kurumlarla ücretsiz olarak paylaşabilir. Ayrıca Sağlık Bakanlığı ve bağlı kuruluşları, kamu ve özel sağlık kuruluşları, sağlık mesleği mensuplarına sağlık hizmeti almak için başvurulduğunda bu kişiler, "sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri" işleyebileceklerdir.[99]

[99] Çekin s.202-203.

YEDİNCİ BÖLÜM
KİŞİSEL VERİLERİN İŞLENMESİ VE YAPAY ZEKA KULLANIMI

1. ALANDA KULLANILAN BAZI TERİMLER VE KİŞİSEL VERİLERİN KORUNMASI İLE İLİŞKİSİ

1.1. Veri Madenciliği

Veri madenciliği yöntemlerinin kullanılmasının sağlayacağı ana fayda büyük boyutlardaki veri kümeleri içinden yeni ve daha önce bilinmeyen bir takım bilgilere ulaşılmasını sağlayabilmesidir. Ulaşılan sonucu gelecekte olası bir takım tahminlemeleri sağlar.[100]

Veri madenciliğinin en önemli amacı ise bir araya getirilmiş verilerin kendi içlerinde istatistiksel yöntemler ile incelenip istenilen veya ilgili kuruma kullanılması için değerlendirilip, kullanıma başlanmasıdır ve böylelikle veri madenciliğinde rahat bir şekilde mantıksal kurallara veya görsel materyallere dönüştürebilecek nitel modellerin elde edilmesini sağlamış olur.

Veri madenciliği yöntemleri, büyük veri setleri içerisinde toplanmış veriyi işleyerek ve istatistiki metodlar kullanarak bir takım mantıksal kural ve görsellere aktarılabilecek modellemeler yapar.[101]

Veri madenciliği uygulamaları ile kişisel verilerin açıklanması, mahremiyetin sağlanması, sır saklama yükümlülüğü gibi kavramların karşıtlıklar içerdiği düşünülür. Gerçekten de amacı, olabildiğince büyük veri kümeleri içerisinde yeni bağlantılar

[100] Uzun , Uzun FN, Çakar E. Veri Madenciliği ve Kullanım Alanları. Uluslararası Mühendislik, Doğa ve Sosyal Bilimler Sempozyumu Isens-21 Ana Teması "Enerji ve Toplum" 25-28 Kasım 2021 Batman Üniversitesi. https://www.researchgate.net/publication/356819774_VERI_MADENCILIGI_VE_KULLANIM_ALANLARI_DATA_MINING_AND_AREAS_OF_USE E.T:19.05.2023

[101] Özeke S.Veri Madenciliği Modelleri ve Uygulama Alanları. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi 2, 200, .s.65-82

keşfetmek olan veri madenciliği yöntemleri, kişisel veri güvenliğinden ziyade bu veriler arasındaki ilişkilere odaklanır ve veri kümesi büyüdükçe bu yöntemlerin başarı oranı artar. Bu konuda bir karar şöyledir: "1993 yılında Amerika'da Maryland eyaletinde yaşayan insanlara daha iyi bir sağlık hizmeti vermek için tüm sağlık kayıtları elektronik bir ortama aktarılmıştır. Bir banker bu verilere erişerek kayıtları inceleyip kendi müşterilerinin hastalıklarını tespit etmiş ve ölümcül hastalığı olan müşterilerinden borçlarını ödemesini istemiştir."[102] Bu konuda benzer örneklere ulaşabilmek veya olası durumları öngörebilmek mümkündür.

Veri madenciliği yöntemleri kullanılırken kişisel verilerin korunması konusu, veriler toplanırken, işlenirken, saklanırken vb her aşamada gözetilmelidir. Kişisel verilerin saklanırken kodlanması, bilgilerin açığa çıkmasının önlenmesi, gereken koruma önlemlerinin her aşamada alınması oluşabilecek ihlallerin engellemesini sağlayacaktır.[103]

1.2. Anonimleştirme

Kişisel Verilerin Korunması Kanunu m.3/b bendinde, anonim hale getirme kavramı tanımlanmıştır. Buna göre, "anonim hale getirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir şekilde belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi" dir. Bu tanımdan, mevcut verilerin gerçek kişilerle ilişkilendirilmemesi gerektiği anlaşılır. Yani, işlenen verilerin anonim hale getirilmesi, veriye ait olan kişiyle veri arasındaki bağın koparılması ve kimin verisi olduğunun belirsizleştirilmesidir.

Anonim hale getirme işlemi, Kişisel Verilerin Korunması Kanunu'nun 7. maddesine göre, verinin silinmesi veya yok edilmesinin yerine kullanılan bir yöntemdir ve verinin

[102] Kavza U. Veri Madenciliğinde Mahremiyetin Sağlanması. Yüksek Lisans Tezi s.28 https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=xTa-XDxJAvrCwUNtUHrd0w&no=vM_N3O0hF6zmfUGJEoWB1w E.T:19.05.2023

[103] Doğan D. Kişisel Verilerin Korunmasında Veri Madenciliği Etkisi: Online Mahremiyetin Sonunda mıyız? Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri 23-25 Ocak 2013 – Akdeniz Üniversitesi, Antalya. https://ab.org.tr/ab13/kitap/dogan_AB13.pdf E.T:19.05.2023

muhafaza edilmesini sağlar. Anonim hale getirme, silme veya yok etme işlemlerinden farklı olarak, veriye erişmek mümkün olmasına rağmen, veriyi sahibiyle ilişkilendirmek mümkün değildir. Kişisel verilerin herhangi bir araştırma ya da çalışmada kullanılabilmesi için anonimleştirilmesi gereklidir. Bu şekilde elde edilen veriler üçüncü kişilere aktarılabilir veya yayınlanabilir. "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkındaki yönetmelik"te md.7'de anonimleştirme işlemine ilişkin usul ve esaslar düzenlenmektedir. Buna göre;

"*MADDE 7-(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir*."

Anonimleştirme işleminin yapılabilmesi için aranan şartlar yönetmelik md.10/2 de düzenlenmiştir. Buna göre;

"*Madde10-(2): 'Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir*."

Bu yönetmelik maddesi, kişisel verilerin anonim hale getirme şartlarını içermektedir. Burada dikkat edilmesi gereken husus, işlem sonrası bu verinin yeniden kişisel veri haline dönüştürülememesidir.

Bir diğer konu da kişisel verilerin üzerindeki bu işlemlerin yapılma süreleridir. Yasal bir sebep, açık rıza veya meşru menfaat gibi nedenlerle işlenen bir verinin sürekli olarak saklanması hukuka uygun değildir. Veriyi işlemeyi gerektiren sebep ortadan kalktıktan belirli bir süre sonra, bu üç işlemden biri gerçekleştirilmelidir. Bu konuda, "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında yönetmelik" uygulanır. İlgili yönetmelik md.11'de süreler düzenlenmiştir.

"*MADDE 11 – (1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. (2) Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez. (3) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir. (4) Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.*"

Kişisel verileri ilgili kişinin talep etmesi halinde, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında yönetmeliğin 12. maddesine göre, ilgili kişinin başvurusu üzerine veri sorumlusunun işlem yapma yükümlülüğü daha kısa bir süreyle sınırlanmıştır.

"*MADDE 12–(1) İlgili kişi, Kanunun 13 üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü*

kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder. c)Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir."

Anonimleştirme, kişisel verilerin korunmasında önemli bir araç olarak kabul edilmelidir. Birçok alanda bu bilgilerin doğrudan bir şekilde, belirli bireylere bağlı olarak saklanması gerekmeyebilir. Özellikle istatistiksel verilerin gerekli olduğu, planlama gibi amaçlarla yapılan işlemlerde bu durum açıkça görülebilir. Anonimleştirme, bu tür işlemlerin etkin bir şekilde gerçekleştirilmesine yardımcı olurken, aynı zamanda bireylerin kişisel verilerinin korunma hakkının zarar görmemesini sağlar.

Günümüzde modern hukuk sisteminde, kişinin en önemli hak sahibi olarak kabul edildiği düşünüldüğünde, kişisel verilerin anonim hale getirilmesi bireyin haklarının korunması için son derece önemli bir kavramdır. Anonimleştirme işlemi, kişisel verilerin korunması hukukunun en önemli prensiplerinden biridir. Hem teknik bir işlem olarak hem de hukuki ilişkinin tarafları için sorunları ortadan kaldıran bir yöntem olarak görülmektedir. Bu nedenle, anonimleştirme konusu sürekli güncelliğini koruyan ve üzerinde çalışmaların yapıldığı bir alan haline gelmiştir. İşlenen veya kaydedilen verilere ilişkin amacın belirli bir süre sonra ortadan kalkması, bu verilerin silinmesini veya anonim hale getirilmesini gerektirir.

Anonimleştirme, hem toplumun çeşitli amaçlarını yerine getirmeye yardımcı olurken hem de bireylerin kişisel verilerinin gizliliği ve korunması hakkını sağlayan önemli bir kavramdır. Anonim hale getirme, veri koruma düzenlemelerinde ve uygulamalarında merkezi bir konumda yer almaktadır ve veri sorumluları için önemli bir sorumluluk ve gereklilik olarak kabul edilmektedir.

Veri sorumlusu diğer veri işleme durumlarında olduğu gibi anonim hale getirme işlemlerinde de tüm önlemleri almak yükümlülüğü altındadır. Anonimleştirme işlemi daha önce de bahsedildiği üzere kişisel verinin tabiri caizse kişiliksizleştirme işlemidir. Böylelikle veri daha önce ait olduğu kişi ile hiçbir şekilde eşleştirilimez hale getirilir. Bir diğer deyişle veri ayırt edilme özelliğini kaybeder. Anonim hale getirme işlemleri için farklı yöntemler uygulanabilmektedir. Çalışmamızda bu yöntemlerin detaylarına girilmeyecek sadece adlarını verilerek geçilecektir. Bu yöntemler:

"*1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemler*

a. Değişkenleri Çıkartma

b. Kayıtları Çıkartma

c. Bölgesel Gizleme

ç. Alt ve Üst Sınır Kodlama

d. Örnekleme

2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

a. Mikro Birleştirme

b. Veri Değiş-Tokuşu

c. Gürültü Ekleme

ç. Tekrar Örnekleme

3. Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemleri

a. K-Anonimlik

b. L-Çeşitlilik

c. T-Yakınlık"[104]

Verinin anonimleştirme işlemi, bir veri işleme faaliyeti olup olmadığı konusu hala tartışılmaktadır. Ancak her durumda, kişinin bu konuda bilgilendirilmesi ve verinin anonimleştirileceği ve saklanacağı konusunda rızasının alınması önemlidir. Öte yandan, özdeşleştirme kavramı da önemli bir konudur. 95/46 direktifinde, anonim hale getirilen verinin başka bir organizasyonda tanımlanabilir hale gelmemesi gerektiği

[104] Atagün ÖF. Kişisel Veri Koruma Hukukunda Anonimleştirme https://www.omeratagun.com/files/Kisisel%20Veriler%20Anonimlestirme.pdf E.T:19.05.2023

belirtilmektedir. Bu nedenle, verinin özdeşleştirme yoluyla yeniden tanımlanabilir hale getirilebilme olasılığı, anonimleştirme işleminin bir veri işleme faaliyeti olarak kabul edilmesini haklı çıkarır. Ancak takma ad kullanımı veya veri kümesi ayrıştırılması gibi yöntemler kullanıldığında, veri sahibine ulaşmak için ek bilgilere ihtiyaç duyulabilir. Bu bilgilere erişimin, gizliliği özenle korunarak engellenmesi önemlidir. Özellikle sağlık alanında yapılan klinik çalışmalarda bu durum büyük önem taşır. Kişisel sağlık verisi kullanılan kişinin ismi, e-posta adresi gibi doğrudan tanımlayıcı veriler, anonimleştirilmez ve gerekli önlemler alınmazsa mahremiyet ihlali riski ortaya çıkabilir.[105]

1.3. Büyük Veri

Bilişim teknolojilerinin gelişmesiyle birlikte veri üretimi önemli ölçüde artmıştır. 2020 yılında yapılan bir çalışmada, sosyal paylaşım sitelerindeki veri miktarı değerlendirilmiştir. Bu çalışmaya göre, her dakikada Facebook'ta 147.000 fotoğraf yüklenmekte, Instagram'da 347.222 hikaye paylaşılmakta, YouTube'a 500 saatlik video yüklenmekte ve WhatsApp'ta ise 41.666.667 adet mesaj gönderilmektedir.[106]

Farklı kaynaklardan elde edilen bu bilgilerin bir araya getirilmesiyle "büyük veri" (Big Data) kavramı ortaya çıkmaktadır. Büyük veri için tek bir tanım olmasa da, genel olarak üç temel özelliği kabul edilmektedir. Bunlar:

- Yüksek hızda oluşturulması
- Formatları farklı verilerden oluşması
- Çok büyük boyutlarda olması

Normal veri işleme yöntemleri bu özelliklere sahip verileri işlemek için yetersiz kalmaktadır. Bu nedenle, yapay zeka teknikleri büyük verinin işlenmesinde kullanılmaktadır. Yapay zeka, büyük veri setlerini analiz etmek, desenleri tanımak ve

[105] Yılmaz, s.75-76
[106] https://www.domo.com/data-never-sleeps E.T 14.05.2023

değerli bilgiler çıkarmak için kullanılan bir dizi algoritma ve teknolojiyi içermektedir. Bu sayede, büyük veri kaynaklarından elde edilen bilgiler daha etkili bir şekilde kullanılabilmektedir.[107]

1.4. Makine Öğrenmesi ve Yapay Zeka

Yapay Zekanın da kabul edilmiş tek bir tanımı yoktur. Avrupa komisyonu tarafından hazırlanan raporda Yapay zeka " *belirli bir amacı gerçekleştirmek için belirli bir seviyede özerklik içerisinde çevresini analiz edip kararlar alarak zeki davranışlar sergileyen sistemler"* olarak tanımlanmaktadır.[108]

Avrupa Komisyonunun oluşturduğu uzman grubu ise "*İnsanlar tarafından tasarlanan, veri toplayarak çevresini kavrayabilen, bu veriyi yorumlayan, ve bu veriden elde edilen bilgiyi değerlendirerek karmaşık amaçlara ulaşmak için atılması gereken adımları belirleyen, fiziksel ve dijital dünyada etki doğuran yazılım ve donanım sistemleri"* olarak tanımlamıştır.[109]

Yapay zeka sistemleri, insan bilişsel fonksiyonlarına benzer şekilde çalışmayı hedefleyen sistemlerdir. Bu konuda birçok farklı tanım bulunmasına rağmen, çoğu kaynak benzer içeriklere sahiptir. Genel bir tanım üzerinde anlaşmaya varılmamasının bir diğer nedeni, toplumsal bir algıyı içermesidir. Özellikle bir dönem "yapay zeka" olarak tanımlanan bir sistem, toplum tarafından alışıldıkça artık yapay zeka olarak adlandırılmamaktadır. [110]

Makine öğrenmesi algoritmaları, matematiksel tekniklerin bilgisayarlar aracılığıyla veriler üzerinde kullanılmasıyla çalışan gelişmiş sistemlerdir. Bu algoritmalar,

[107] https://digital-strategy.ec.europa.eu/en/policies/big-data E.T: 14.05.2023
[108] https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe E.T.14.05.2023
[109] https://digitalstrategy.ec.europa.eu/en/policies/expert-group-ai E.T:14.05.2023
[110] https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf E.T:14.05.2023

verilerden öğrenerek yeni sonuçlara ulaşabilir, daha isabetli ve verimli tahminler yapabilir.[111]

Ancak kişisel verilerin işlenmesi aşamasında bu tekniklerin kullanılması bazı ihlallere yol açabilir. Öncelikle, bu tekniklerin etkili bir şekilde kullanılabilmesi için çok sayıda veriye ihtiyaç duyulmaktadır. Bu, kişisel verilerin korunmasıyla ilgili temel ilkelere, özellikle veri minimizasyonu ilkesine ihlal riski oluşturmaktadır.

Diğer bir durum, büyük verilerle çalışan bu sistemlerin yüksek işlem gücüne sahip bilgisayarlarla çalışması ve sonuç olarak insanlar tarafından tespit edilemeyecek bağlantıları belirleyebilmesi ve bu bağlamda çok sayıda veriden kişisel veri niteliğindeki verilere ulaşabilmesidir. Bu, kişisel veri kavramının genişlemesi anlamına gelmektedir. Bir başka konu ise kullanılan yapay zeka tekniklerinin matematiksel hesaplamalarla sonuca ulaşması ve nasıl bir sonuca ulaşıldığı konusunun tam olarak bilinememesidir. Bu durum "kara kutu" problemi olarak adlandırılmaktadır. Bu durum, kişisel verilerin hukuka uygun olarak işlenmesi, şeffaflık ilkesi, veri sorumlusunun aydınlatma yükümlülüğü ve verisi işlenen kişinin bu işleme faaliyeti hakkında bilgi edinme hakkı açısından sorunlar ortaya çıkarabilir.[112]

2. YAPAY ZEKANIN KİŞİSEL VERİ KAVRAMINA ETKİSİ

Kişisel Veri kavramı KVKK'da "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veri" olarak tanımlanmış olsa da bu tanıma göre verinin kişisel veri olup olması hali bazı durumlarda detaylı incelemeyi gerektirebilmektedir. Üstelik bu değerlendirme sadece veri sorumlusu ve veri işleyen kavramlarından daha da ötelere ulaşabilmektedir.

[111] https://multimedia.europarl.europa.eu/en/webstreaming/panel-for-future-of-science-and-technology_20221128-1500-SPECIAL-STOA E.T:14.05.2023

[112] Büyüksağiş E. Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 18 (2021): 529-541

Bazı durumlarda veri, kişisel veri değil iken, bazen aynı veri durumun değişmesi ile kişisel veri olarak değerlendirilebilmektedir. Örneğin IP numarası olarak da bilinen bilgisayarların kimlik numaraları, bu konuda uzman olmayan kişiler tarafından, doğrudan kişiyle ilişkilendirilecek bir veri olmadığından kişisel veri olarak nitelendirilecekken, aynı durum bu alanda çalışan bir bilişim uzmanı tarafından özellikle de bu IP numarasının kime ait olduğu bilgisine ulaşabilecek bir uzman olduğunda kişisel veri niteliği kazanacaktır. Bu değerlendirmede objektif ve sübjektif değerlendirme makuliyet sınırları içerisinde ele alınmalıdır.[113]

Bu bağlamda bir diğer örnek de telefon şifreleridir. Şifreli bir telefonun her ne kadar şifresi teorik olarak kırılabilir olsa da bu şifre kişisel veri olarak kabul edilemez. Ancak şifre kırılır ve telefon numarasına erişilebilir hale gelirse bu veri kişisel veri olarak değerlendirilebilir.[114]

Bu durumu özellikle kişisel sağlık verileri bağlamında değerlendirecek olursak sigorta şirketlerinin özellikle bu verilere ulaşmak ile ilgili kazançları ve çabaları aşikardır. Böylelikle yapay zeka aracılı ya da aracısız toplanacak bu bilgi ciddi ihlallere ve mağduriyetlere yol açabilecektir. Sigorta şirketleri kişisel sağlık verisi üzerinden bu kişileri sigortalamamak ya da daha yüksek rakamlar üzerinden sigortalamak yoluna gidebileceklerdir. Yapay zeka sistemleri üzerinden bu bilgilere ulaşılabilir hatta henüz hastalık gelişmeden tahminlenebilir olması ciddi endişeler oluşturabilecek bir konudur.

Yapay zeka algoritmalarıyla bu endişelerin artmasının haklılığını destekleyen bir olay 2016 yılında yaşanmıştır. Bu olayda; 2016 yılında Avustralya Sağlık Bakanlığı tarafından hasta kimliğine ait veriler anonimleştirilerek hasta harcamalarına dair

[113] Aksoy Retornaz E, Güçlütürk O. Gelişen Teknolojiler ve Hukuk II: Yapay Zeka, Oniki levha Yayınları, İstanbul 2021, s.280
[114] https://www.europarl.europa.eu/stoa/en/home/highlights E.T:14.05.2023

veriler yayınlanmıştır. Bu verilerin yayınlanmasından 6 ay sonra Melbourne üniversitesinde yapılan bir çalışmada bu verilerin sahibi olan kişilere ulaşılmıştır.[115]

Günümüzde giyilebilir cihazlar üzerinden kişisel sağlık verileri toplanabilmektedir. Yapılan bir çalışmada, toplanan bu veriler anonimleştirildikten sonra bile makine öğrenmesi yolu ile kişisel veriye ulaşılması sağlanabilmiştir. Bu çalışma toplam 4720 yetişkin ve 2427 çocuğun kişisel sağlık verisi üzerinden yapılmıştır.[116]

Bir diğer örnek Netflix platformu tarafından, platform değerlendirmelerinin bulunduğu verilerin, kişiliksizleştirme işlemi yapıldıktan sonra sadece kamuya açık amazon yorumları kullanılarak, bu veriler üzerinde kişisel verilerin tespit edilmesi olayıdır.[117]

Tüm bu örnekler göstermektedir ki makine öğrenmesi ve yapay zeka teknikleri, anonimleştirilmiş, kişiliksizleştirilmiş verinin yeniden kişisel veri haline getirilebilmesini sağlayabilecektir. Mevcut yöntemlerin geliştirilmesi, bu konuda mevzuat güncellemelerinin süratle ve teknolojiyi takip eder şekilde yapılması önem arz etmektedir.

Yapay zeka teknolojileri, eldeki verilerden daha önce bilinmeyen yeni kişisel verilerin keşfini sağlayabilir. Yüz fotoğrafı verisi üzerinden cinsel yönelim tespiti yapılmasıyla ilgili çalışma, yapay zeka tekniklerinin bu alandaki potansiyelini göstermektedir. Bu çalışmada, derin sinir ağları kullanılarak 35.326 yüz görüntüsünden özellikler çıkarılmış ve cinsel yönelimi sınıflandırmayı amaçlayan bir makine öğrenme algoritmasına giriş olarak kullanılmıştır. Tek bir yüz görüntüsü verildiğinde, sınıflandırıcı eşcinsel ve heteroseksüel erkekleri vakaların %81'inde ve kadınların

[115] Culnane C. Health Data in an Open World. https://arxiv.org/abs/1712.05627 E.T:14.05.2023

[116] Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning. JAMA Netw Open. 2018 Dec 7;1(8):e186040. doi: 10.1001/jamanetworkopen.2018.6040. E.T:14.05.2023

[117] https://courses.csail.mit.edu/6.857/2018/project/Archie-Gershon-Katchoff-Zeng-Netflix.pdf E.T 14.05.2023

vakalarının %71'inde doğru bir şekilde ayırt edebilmiştir. İnsan değerlendiricilerin doğruluk oranları ise daha düşük çıkmıştır (%61 erkekler için ve %54 kadınlar için). Ancak kişi başına beş tane yüz görüntüsü verildiğinde algoritmanın doğruluk oranı sırasıyla %91 ve %83'e yükselmiştir. Sınıflandırıcı tarafından kullanılan yüz özellikleri, sabit özellikler (örneğin burun şekli) ve geçici özellikler (örneğin bakım tarzı) gibi farklı özellikleri içermektedir. Bu çalışma, yapay zeka teknolojilerinin bazı kişisel özellikleri tespit edebileceğini ve bu durumun kişisel veri alanında endişelere yol açabileceğini göstermektedir. Özellikle, insan beyninin algılayabileceğinden veya yorumlayabileceğinden daha fazla bilgi içeren yüzler gibi görsel veriler, yapay zeka algoritmaları tarafından analiz edilerek kişisel özelliklerin keşfedilmesine olanak sağlayabilir.Bu tür çalışmalar, kişisel veri gizliliği ve koruması açısından önemli tartışmaları beraberinde getirmektedir. Verilerin gizliliğinin ve anonimliğinin korunması, teknolojik gelişmelere ayak uyduracak mevzuat ve düzenlemelerin yapılması önemlidir. Ayrıca, yapay zeka sistemlerinin etik ve sorumlu kullanımı da dikkate alınmalıdır.[118]

Yapay zeka teknikleri ve makine öğrenmesi araçlarının bir özelliği, veri ile çalışarak elde ettikleri sonuçların ihtimale dayalı olmasıdır. Bu sistemler, veri analizi ve örüntü tanıma yoluyla belirli bir görevi gerçekleştirmek için verilerden öğrenir ve sonuçları tahmin eder. Yapay zeka ve makine öğrenmesi algoritmaları, veriye dayalı istatistiksel hesaplamalar yapar ve sonuçları olasılık değerlendirmeleri şeklinde sunar. Bu, elde edilen sonuçların mutlak doğruluk taşımadığı anlamına gelir.[119]

Avrupa Birliği Adalet Divanı (ABAD), kişisel veri kavramının geniş yorumlanması ve korunmasıyla ilgili bir dizi önemli karara imza atmıştır. Bu kararlar, gerçekliği kesin olmayan bazı değerlendirmelerin kişisel veri olarak kabul edilmesi gerektiğini vurgulamaktadır. Örneğin, ABAD'ın 2014 yılında verdiği bir kararda, kişisel verilerin tanımlanabilen gerçek kişilerle ilişkilendirilebilir olmasının yeterli olduğu

[118] Wang Y, Kosinski M. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. J Pers Soc Psychol. 2018 Feb;114(2):246-257. doi: 10.1037/pspa0000098. PMID: 29389215. https://pubmed.ncbi.nlm.nih.gov/29389215/ E.T 14.05.2014

[119] Retornaz, Güçlütürk. s.282

belirtilmiştir. Bu kapsamda, gerçekliği kesin olmasa bile bir değerlendirmenin bir kişiyle ilişkilendirilebilir olduğu durumlarda, bu değerlendirmeler kişisel veri olarak kabul edilebilir.

3. KİŞİSEL VERİ KORUMASINDA YAPAY ZEKÂ DÖNEMİNİN OLUŞTURDUĞU SORUNLAR

Yapay zekâ teknolojileri ile birlikte en sıklıkla dile getirilen risklerden biri de, kişisel verisi işlenen veri sahiplerinin mahremiyet haklarının ihlalidir. Buna yönelik sıklıkla mevzuat düzenlemeleri yapılsa da gelinen süreçte bu ihlallerin önlenmesi bağlamında yeterli koruma sağlanamamıştır.[120]

Kişisel verilerin işlenmesi, aktarılması, depolanması, silinmesine ilişkin işlemlerin özellikle bilişim teknolojileri ile birlikte alternatiflerinin artması, temel hak ve özgürlükler temelinde korunmalarının nasıl sağlanacağını konusunu gündeme taşımıştır.[121]

Bu bağlamda, kişisel verilerin korunması konusu, verilerin sadece miktarının değil, aynı zamanda niteliğinin de değişime uğraması nedeniyle farklılaşmaktadır.[122]

Klasik anlayışın bu değişimi yakalayabilmesi için, temel yaklaşım ve değerleri koruyarak, sürece yeni araçlar ekleyerek, uyum sağlayacak şekilde bir esneklik kazanarak mümkündür.

Kişisel verilerin korunması konusunda düzenlemeler genellikle iki ana yaklaşım çerçevesinde ele alınmaktadır: Kara Avrupası Hukuk Sistemi ve Anglo-Sakson Hukuk Sistemi. Kara Avrupası Hukuk Sistemi, temel olarak kişisel verileri sosyal ve hümanist bir perspektifle ele alır. Bu yaklaşıma göre kişisel veriler, temel insan hakları ve kişilik

[120] Civelek, DY. Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi. Ankara: Bilgi Toplumu Dairesi Başkanlığı.2013, S.3
[121] Civelek . s.6
[122] Big Data is Better Data. https://www.ted.com/talks/kenneth_cukier_big_data_is_better_data E.T.19.05.2023

hakkı bağlamında değerlendirilir. Kişisel veri kavramı, anayasal bir temel hak olarak kabul edilir ve özel hayatın gizliliği (mahremiyet) gibi koruma altında olan değerlerle ilişkilendirilir. Özel hayatın gizliliği, medeni hukuk terminolojisinde yer alan "kişilik hakkı" kapsamında değerlendirilen kişisel değerlerin bir parçasıdır.[123] AB'ne üye devletler, hukuk sistemlerini uyumlu hale getirmek amacıyla bu temel yaklaşımı benimseyerek mevzuatlarında değişiklikler yapmaktadır. Anglo-Sakson Hukuk Sistemi ise kişisel verilerin korunması konusunda farklı bir yaklaşım sergiler. Bu yaklaşıma göre kişisel veriler, ekonomik ve iktisadi bir bakış açısıyla mülkiyet ve/veya fikri haklar bağlamında değerlendirilir.[124] Kişisel veri, sadece sahibinin kişiliğinin bir uzantısı olarak değil, aynı zamanda ilgili kişiliğin bir ürünü olarak da görülür. Bu yaklaşımda kişilik hakkının korunması amaçlanırken, kişiliğin dışında olan ve kişiliğe bağlı olarak ortaya çıkan bir ürün olarak da düşünülür.[125] Bu farklı yaklaşımların temelinde, toplumsal ve kültürel farklılıklar, hukuki gelenekler ve değerler yatmaktadır. Her iki yaklaşım da kişisel verilerin korunmasına önem vermektedir, ancak farklı vurgular yapmaktadır. Bu iki grubun yaklaşımları arasındaki farklılık özellikle AB mevzuatının kişisel verileri detaylı kanuni düzenlemelerle korunmasıdır. AB mevzuatı bu konuda oldukça detaylı ve etkili düzenlenmiştir.

Kişisel verilerin korunması konusunda farklı düzenlemeler ve yaklaşımlar mevcuttur ve bunlar beraberinde hukuki ve pratik sorunlar da getirir. ABD'nin kişisel verilerin korunması düzenlemeleri genellikle piyasa odaklıdır ve ticaret ve sanayinin ihtiyaçlarına göre pragmatik bir yaklaşım sergiler. Bu durum, kişi güvenliği ve kişisel verilerin korunmasının felsefi ve hukuki dayanakları açısından eleştirilebilir bir noktadır. ABD'de kişisel verilerin korunması genellikle sektörel bazda düzenlenir ve kişiyi tanımlayan bilgilerin korunmasına odaklanır. Bu durum, AB'deki gibi tek bir yasayla kişisel verilerin korunmasını amaçlayan bütüncül bir yaklaşımdan farklıdır. Bu farklılıkların bazıları hukuk sisteminin ilkelerinden kaynaklanırken, bazıları teknolojik ilerlemelerden ve uluslararası rekabetten kaynaklanmaktadır. Ayrıca,

[123] Hatemi H. Kişiler Hukuku. İstanbul, On İki Levha, 9.baskı 2021, s. 66

[124] Aksoy HC. The Right to Personality and It's Different Manifestations as the Core of Personal Data. Ankara Law Review, 5(2), s.235-249.

[125] Akkurt SS. Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış. Kişisel Verileri Koruma Dergisi, 2(5), 2020, s. 21

uluslararası rekabet de kişisel verilerin korunması konusunda sorunlar yaratabilir. Farklı ülkelerin farklı düzenlemeleri ve yaklaşımları olduğunda, veri akışı, veri işleme süreçleri ve uluslararası işbirliği konularında zorluklar ortaya çıkabilir. Bu durum, kişisel verilerin etkili bir şekilde korunmasını ve veri aktarımlarının güvenliğini zorlaştırabilir.[126]

Algoritma yazan kişiler genellikle temel hukuki bilgiler konusunda bilgilendirilmemişlerdir. Bu nedenle, algoritmalarla işlenen ve otomatik olarak verilen kararlarla bazı temel hak ve özgürlüklere zarar verebileceklerini tahmin edemeyebilirler. Oysa yapılan bazı çalışmalarda bu ihtimalin olduğu gösterilmiştir. Bazı algoritmalar ayrımcılığa yol açabilir.[127]

GDPR, algoritmik kararların insan denetiminden geçirilmesini ve ilgili kişinin açık rızası olmadan doğrudan uygulanmasını yasaklamaktadır. GDPR, kişisel verilerin işlenmesi ve korunması konusunda AB'de uygulanan temel bir düzenlemedir ve algoritmik kararlar konusunda da önemli düzenlemeler getirmektedir. GDPR'nin 22. maddesi, otomatik işleme (algoritmik kararlar da buna dahildir) tabi tutulan kişilerin, bu işlemin nedenini, mantığını ve onunla ilgili potansiyel sonuçları hakkında açık bir şekilde bilgilendirilmelerini ve bu kararlara itiraz etme haklarını vurgular. İlgili kişiler, algoritmik kararların yalnızca insan denetiminden geçirildikten sonra uygulanmasını talep edebilirler. Bu düzenlemeler, algoritmik otoriteryanizmin önüne geçmek ve kişisel verilerin korunması konusunda şeffaflığı ve insan denetimini sağlamak amacıyla getirilmiştir. GDPR'nin bu hükümleri, kişisel verilerin işlenmesi ve algoritmik kararların kullanılması sürecinde bireylerin haklarını korumayı hedefler. Bununla birlikte, GDPR'nin tam uygulanması ve algoritmik kararların denetimi konusunda bazı zorluklar mevcuttur. Algoritmaların karmaşıklığı, şeffaflık eksikliği ve karar verme süreçlerinin tam olarak anlaşılamaması gibi faktörler, etkili denetim ve açıklık sağlama konusunda zorluklar yaratabilir. Bu nedenle, ilgili otoritelerin,

[126] Abudureyimu Y, Oğurlu Y. Yapay zekâ uygulamalarının kişisel verilerin korumasına dair doğurabileceği sorunlar ve çözüm önerileri. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 20(41),2021, s. 765-782.

[127] Mittelstadt BD, Allo P, Taddeo M, Wachter S, Florid L.The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2016. https://doi.org/10.1177/2053951716679679

şirketlerin ve toplumun algoritmik kararların etkilerini anlamak, denetlemek ve düzeltmek için sürekli çaba göstermesi önemlidir.[128]

6698 sayılı KVKK düzenlenirken model olarak 95/46/AT Direktifi alınmıştır. Bu nedenle Direktif sonrası yürürülüğe giren GDPR düzenlemesi, KVKK'da yer almamıştır. Bunun sonucu olarak salt otomatik bireysel kararlar, insan denetiminden geçmeksizin ülkemiz hukukunda uygulanabilmektedir.

KVKK'nın bu eksikliği ek düzenlemeyle aşması gerektiği açıktır. Algoritmik kararlar neticesinde ortaya çıkan zararlarda sorumluluğun belirlenmesi, kapsamın ne olacağı konusu doktrinde henüz yeterince incelenmemiştir. Kişisel verilerin korunması hakkı 2010 yılında AY md. 20'ye eklenen bir madde ile anayasal dayanağa kavuşmuştur. Bu hak yapay zeka kullanımı sonrası ortaya çıkan zararlar durumunda da kullanılabilecektir.[129]

Ülkemizde yürürlükte olan kanuna göre, kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Bu tanıma göre, kişisel veri, bir kişiyi doğrudan tanımlayan bilgilerin yanı sıra, bu bilgilerle ilişkilendirilebilir veya belirlenebilir olan diğer bilgileri de içerir. İlk durumdaki veriler, kişiyi doğrudan tanımlayan bilgileri içerir. Örneğin, ad, soyad, doğum tarihi gibi kişisel bilgiler, kimliği belirli bir kişiyi açık ve net bir şekilde tanımlar. İkinci durumdaki veriler ise, başka bilgilerle birleştirildiğinde kişiyi belirleyebilir hale gelir. Örneğin, bir kamera kaydı, kişinin yüzünün görüntüsünü içerir ve bu görüntü diğer verilerle ilişkilendirildiğinde kişiyi belirlemek mümkün hale gelir.[130]

KVKK'nun 6. maddesi 2. fıkrasına göre kişisel veriler özel nitelikli kişisel olarak diğer verilerden farklı bir kategoriye sokulmuş ve değerlendirmeye alınmıştır. Buna göre, ister belirli ister belirlenebilir olsun, KVKK'nun 6. maddesinin 1. fıkrasında özel

[128] Aksoy HC. Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme, Kişisel Verileri Koruma Dergisi. 4(2), 2022, s.69-87
[129] Büyüksağiş E. Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı, YÜHFD, C.XVIII, 2021/2, s.529-541.
[130] Akkurt, s.20-32

nitelikli olarak tanımlı sınırlı sayıdaki kişisel verinin ilgili kişinin rızası olmaksızın işlenemeyeceği hükme bağlanmıştır. Md. 6/1 de söz edilen bu 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 durumları ile biyometrik ve genetik bilgilerini içeren veriler" dir.

Kişisel verilerin işlenmesi ile oluşacak kararlar insan denetiminden geçen ve doğrudan algoritmalar aracılığıyla otomatik olarak oluşturan kararlar olarak ikiye ayrılabilir. Bu ayrımın KVKK açısından değerlendirildiğinde özel bir durum oluşturduğu görülür. KVKK her iki karar açısından ayrım yapmaz. Özel nitelikli verilerin bile otomatik işlemlerle işlenmesi Türk hukukunda yasaklanmamıştır. Bu durum, dünyadaki ve özellikle Avrupa'daki gelişmelerle[131] uyumlu değildir. Diğer taraftan AY'nın 17. maddesi ile güvence altına alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkına zarar verebilecek bir durum yaratabilir. Aynı tezatlık Anayasa'nın 20 ve 22. maddelerinde düzenlenen özel hayatın gizliliği ilkesiyle de mevcuttur.

Türk hukukunda algoritmik kararların hukuki niteliği ve beraberinde getirdiği sonuçlar henüz tanımlanmamıştır. Ancak, AB Tüzüğü bu tür kararları özel bir düzenlemeye tabi tutmuş ve önemli bir etkisi olan salt otomatik kararları genel olarak yasaklamıştır. AB tüzüğü ilgili kişinin durumunu önemli ölçüde etkileyen veya hukuki sonuçlar doğuran salt otomatik kararları toptan yasaklama yoluna gitmiştir. Bu tüzüğün 22. maddesinin 1. fıkrası gereğince, kişisel verilerinin salt otomatik yollarla işlenmesi ve bunun neticesinde kendilerini önemli ölçüde etkileyen kararlara tabi olmama hakkına sahiptirler.

[131] Mendoza I, Bygrave LA. The Right Not to Be Subject to Automated Decisions Based on Profiling (May 8, 2017). Tatiani Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou (eds.), EU Internet Law: Regulation and Enforcement (Springer, 2017, Forthcoming), University of Oslo Faculty of Law Research Paper No. 2017-20, Available at SSRN: https://ssrn.com/abstract=2964855

Salt algoritmik karar yasağının istisnaları, AB Tüzüğü'nün 22. maddesinin 2. fıkrasında sınırlı sayıda olarak düzenlenmiştir.. Buna göre, otomatik bireysel kararların;

> "*Veri öznesi ile veri sorumlusu arasında bir sözleşmenin kurulması ya da ifası için gerekli olması; AB ya da veri sorumlusunun tabi olduğu üye devlet hukukunun izin vermesi ve veri öznesinin hak ve özgürlükleri ile meşru menfaatlerini güvence altına almaya yönelik olması ; Veri öznesinin AB Tüzüğü'nün 15. maddesi uyarınca veri sorumlusundan aldığı bilgi üzerine kişisel verilerinin işlenmesine rıza göstermesi hallerinde, veri öznesinin kişisel verilerinin işlenmesine dayanan ve kendisi hakkında hukuki sonuçlar doğuran ya da ciddi derecede etkileyen kararlara konu olmama hakkı istisnaen sınırlandırılmış bulunur*."

95/46/AT ile temel alınarak hazırlanan KVKK metni, 7 Nisan 2016 tarihinde yürürlüğe girmiştir. GDPR ise sadece 1 hafta sonra 14 Nisan 2016'da kabul edilmiş ve 24 Mayıs 2018 tarihinde yürürlüğe girmiştir. AB Tüzüğü'nün 4. maddesinin 4. fıkrasındaki tanıma göre "profil çıkarma, kişisel verilerin, gerçek kişilerin çeşitli kişisel özelliklerini değerlendirme, özellikle iş performansını, ekonomik durumunu, sağlık durumunu, kişisel tercihlerini, ilgi alanlarını, güvenilirliğini, davranışlarını, konumunu ve hareketlerini belirleme ya da tahmin etmede kullanılacak şekilde otomatik yollarla işlenmesi"dir. otomatik bireysel işlemlerin sadece profil çıkarmadan ibaret olmadığı bilinmelidir.[132]

AB Tüzüğü'nün algoritmik kararları genel olarak yasaklayıp temel hak ve özgürlükleri korurken istisnai durumlar altında hukuka uygun olarak kabul etmesinin sebeplerinden biri, bu tür kararların mevcut ayrımcılığı daha geniş kitlelere yayma potansiyeline sahip olması ve özellikle kırılgan gruplar aleyhine adaletsizliklere yol açabilmesidir. Algoritmanın davranışını iki faktör etkiler. Bunlardan ilki kod diğeri ise istatistiksel verilerdir. İşlenen verilerin neler olduğu ve algoritmanın işleyişi genelde modelleme temellidir. Modellemeler genellikle karmaşık yapılar içerir. Kullanılan modellemeler

[132] Gianclaudio M. Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations, Computer Law & Security Review, Volume 35, Issue 5, 2019,

uç değerlerin etkisini ortadan kaldırarak işlem yükünü azaltabilir ve hedefe yakın optimal çözümler üretebilir. Ancak, hukuki alanda, bu uç değerler kırılgan grupları marjinalleştirebilir ve ayrımcılığa yol açabilir.[133] Bu modellemelerde derin öğrenme algoritmaları sıklıkla kullanılır. Fakat yapılan deneysel çalışmalar, bu yöntemlerin uygulanması ile oluşturulacak kararların objektiflikten uzak olabileceğini düşündürmektedir.[134] Bu nedenle, mevcut veriler kullanılarak oluşturulan algoritmaların esas olarak önyargılara dayandığını göstermektedir.

KVKK madde 11/1/g bendinde itiraz hakkı tanınmıştır. Bu hak otomatik sistemlerle veri işlenmesi sonrası oluşan zarar durumlarını düzeltmek için düzenlenmiştir. Fakat burada ana sorunun ortadan kaldırılması yerine zarar oluştuktan sonra tazmin edilmesi yolu çok uygun değildir. Diğer taraftan bu algoritmalar tarafından yaratılan bu durumun nasıl oluştuğunu ilgili kişi genellikle bilemez. Dolayısıyla itiraz hakkının kullanılabilmesi de bu şekilde pek mümkün gözükmemektedir. Oluşan durum geri dönüşsüz olabilir.

Mevcut hukuki düzenlemeler bağlamında algoritmaların hukuki bir kişiliği olamaz. Avrupa Parlamentosu 27 Ocak 2017 tarihli bir raporunda bu konuda bir adım atmıştır. Yapay zekalara hukuki kişilik tanınması yönünde öneri ve tavsiyelerde bulunmuştur.[135] Türk doktrininde buna yönelik değerlendirmeler de yapılmıştır.[136] Fakat son noktada bu önerilerin oluşturabilecekleri problemler nedeniyle süreç ilerlememiştir.

Salt algoritmik kararlar nedeniyle açılacak davalarda muhatap gösterilebilecek kişiler, hukuki gerekçeler ve taleplerin kapsamı henüz net bir şekilde belirlenmemiştir. Birçok durumda, algoritmanın kararının bir fırsatın kaçırılmasına neden olduğu iddia

[133] Yann LeCun, Yoshua B, Geoffrey H. Deep Learning, Nature 2015, s. 436 vd.
[134] Sloan H, Warner R. Beyond Bias: Artificial Intelligence and Social Justice, Virginia Journal of Law and Technology 2020, s. 1 vd.
[135] European Parliament Report, Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL) https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html E.T:19.05.2023
[136] Yantaç C, Falcıoğlu, MÖ. Yapay Zeka, İnsan ve Hukuk, Beykent Üniversitesi Hukuk Fakültesi Dergisi 2020, s. 31 vd.

edilebilir, ancak bu iddianın uygun illiyet bağı içinde oluşturduğu maddi zararın kanıtlanması zor olabilir. Kişilik hakkının ihlali, manevi tazminat taleplerine de yol açabilir. Manevi tazminat, duyulan acı ve elemi kısmen gidermeyi amaçladığı düşüncesiyle birlikte caydırıcılık unsuru da dikkate alınarak değerlendirilir. Yargıtay içtihadı, manevi tazminat taleplerinin daha sık gündeme gelmesine yol açabilecek bir yönde evrilmiştir. Avrupa Parlamentosu, bu tür riskleri göz önünde bulundurarak, yapay zekanın neden olduğu zararlardan sorumluluğu düzenleyen bir Tüzük tasarısı kabul etmiştir. Bu tasarı, yapay zeka teknolojilerinden kaynaklanan zararların tespiti ve bu zararlardan kimin sorumlu olduğunun belirlenmesi için bir çerçeve sunmayı amaçlamaktadır. Bu tasarı, yapay zeka kullanımıyla ilgili sorumluluk ve tazminat konularında daha açık kurallar getirmeyi hedeflemektedir. Ancak, Türk hukukunda henüz benzer bir düzenleme bulunmamaktadır ve bu konuda ayrıntılı bir mevzuat eksikliği vardır. Bu nedenle, Türk hukuku, yapay zeka ve algoritmik kararlarla ilgili sorumluluk ve tazminat konularını daha iyi ele alabilmek için KVKK gibi mevcut mevzuatı revize etmeli ve bu teknolojilere ilişkin net kurallar ve standartlar oluşturmalıdır. Bu, hem bireylerin haklarını korumak hem de adil bir hukuki çerçeve sağlamak açısından önemlidir.[137]

Oluşabilecek zararın sorumluların belirlenmesi ve tazminin bu doğrultuda yapılması gereklidir. Bu algoritmik platformları kullanan işletmelerin bu bağlamda organizasyon sorumluluğuna gidilebilmesi mümkün gözükmektedir. İşletmeler, TBK'nın 114. maddesinin 2. fıkrasına dayanarak, uygun düştüğü ölçüde sorumluluklarını kabul etmelidir. Bu durumda, işletme ile veri öznesi arasında sözleşmesel bir ilişki olsa bile, veri öznesi zararının tazminini isteyebilir ve bu talep haksız fiil sorumluluğuna dayandırılabilir. Bu bağlamda, Türk hukukunun KVKK'yı revize ederek algoritmik kararlar ve yapay zeka teknolojileriyle ilgili daha spesifik düzenlemeler getirmesi gerekmektedir. Bu düzenlemeler, işletmelerin sorumluluklarını belirlemek, veri öznesinin zararlarını tazmin etmek ve temel hakları korumak için daha etkili bir

[137] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU(2020)654178_EN.pdf E.T:19.05.2023

mevzuat sağlamayı amaçlamalıdır. AB Tüzüğü'nün 15. maddesinin 1. fıkrasının (h) bendi ve 22. maddesi, bu şekilde oluşan kararlarla kişilik haklarının ihlaline karşı etkin bir koruma sağlamaktadır. Bu korumayı KVKK'ya yansıtacak bir hüküm eklenmesi gerekmektedir. Bu hüküm ile ilgili kişilerin, kişisel verilerinin işlenip işlenmediğini bilme hakkına sahip olması ve işleme faaliyeti varsa, otomatik karar verme sürecinin olup olmadığı, kullanılan mantık ve öngörülen sonuçlar hakkında mümkünse anlamlı bilgiler edinme imkanı elde etmeleri sağlanmalıdır. Bu tür işlemler için ilgili kişinin açık rızası gereklidir ve açık rıza olmadığı durumlarda alınan algoritmik bireysel kararlar geçersiz sayılmalıdır.[138]

4. YAPAY ZEKANIN KİŞİSEL VERİLERİN İŞLENMESİ HUKUKUNA HAKİM OLAN İLKELERLE İLİŞKİSİ

Kişisel verileri koruma mantığının işler hale getirilebilmesi için bu işleme faaliyetinin belirli şekillerde kısıtlanması ihtiyacı olduğu aşikardır. Yapay zeka bağlamında değerlendirildiğinde KVKK m.4'de belirtilen ilkelerin bu şekilde teker teker gözden geçirilmesi yararlı olacaktır:

"M.4/2: Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:
(a) Hukuka ve dürüstlük kurallarına uygun olma
(b) Doğru ve gerektiğinde güncel olma
(c) Belirli, açık ve meşru amaçlar için işlenme
(d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma
(e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"

Bu madde çerçevesinde şekli açıdan sınırlı sayıda görüntüsü verse de ilkelerin geniş şekilde kaleme alınması, uygulamada başka ilkelerin de bu kapsam içerisine alınmasını mümkün kılmıştır. Bu durum ile ilgili bir örnek şudur: GDPR m.5 ve Brazilian General Data Protection Law(LGPD) m.6'da hesap verilebilirlik ilkesi ayrı

[138] Büyüksağiş, s.529-541

bir maddede düzenlenmiştir. Oysa KVKK'da böyle bir durum söz konusu değildir. Bununla birlikte KVKK m.10 ve devamında düzenlenen maddeler ile veri sorumlusunun yükümlülüklerine ilişkin maddeler bu ilkenin KVKK açısından da geçerli olduğunu düşündürmektedir. Kurul bu durumu destekleyen bir karara imza atmıştır. Kararda meşru menfaat istisnasının kapsamını incelerken açık bir şekilde 'Açıklık ve Şeffaflık' ilkelerinin dikkate alınması gerektiğine vurgu yapmıştır.[139]

Yine LGPD'de m.6 da 'ayrımcılık yapmama' ilkesi ayrıca düzenlenmişken bu ilke KVKK ve GDPR'de ayrıca düzenlenmemiştir. GDPR nin başlangıç kısmında bu ilkeye değinilirken KVKK'da özel nitelikli kişisel verilerin korunması kısmında değinilmiştir.

KVKK m.6 da bu durum *"bu verilerin başkası tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları dikkate alınmakta, bu sebeple bu tür veriler özel nitelikli veri olarak kabul edilmektedir."* denilerek ifade edilmektedir.[140]

4.1. Hukuka ve Dürüstlük kurallarına Uygun Olma

Hukuka ve dürüstlük kurallarına uygun olma, kişisel verileri işleme faaliyetleri tüm aşamalarında uygulama bulur. Geniş bir ilkedir ve diğer ilkeleri de kapsayıcı özellik taşır. Hukuka uygunluk mevzuat düzenlemelerine uygun olmayı belirtirken, dürüstlük kurallarına uygunluk medeni kanun md.2 bağlamında değerlendirilir. Bu durum somut olay özelinde değerlendirilir. Dürüstlük kuralı, özellikle mevzuata uygun olmakla birlikte ilgili kişilerin menfaatlerini olumsuz etkileyebilecek durumlarda kullanılır.[141]

[139] https://www.kvkk.gov.tr/Icerik/5434/2019-78 E.T 16.05.2023
[140] Retornaz, Güçlütürk, s.287
[141] Dülger, s.264

Şeffaflık ilkesi, GDPR madde 5/1-a'da açıkça belirtilmesine rağmen KVKK da bu durum söz konusu değildir. GDPR kapsamında şeffaflık, kişisel verisi açıklanan kişiye bu durumun kolay anlaşılabilir ve özlü bir şekilde iletilmesi durumudur.[142]

Bu durum yapay zeka teknolojileri ile yapılan işleme faaliyetlerinde KVKK ve kurul uygulaması için bir kontrol noktası oluşturacaktır. Bununla ilgili bir örnekte işe alım sırasında yapay zeka destekli değerlendirme sağlayan bir model, cinsiyete dayalı ayrımcılık yapabileceğinden hukuka ve dürüstlük kurallarına aykırı bir durum yaratabilecektir. Amazon tarafından geliştirilen bir modelin, cinsiyet ve performans üzerinden yaptığı değerlendirmelerde kadın çalışan adaylara ayrımcılık yaptığı saptanmış ve bunun sonucunda yine amazon tarafından geri çekilmiştir.[143]

Benzer durumların özellikle makine öğrenme temelli modeller tarafından kişisel sağlık verileri üzerinden ayrımcılığa yol açabilmesi mümkündür. Bu açıdan değerlendirildiğinde ilkenin dikkatlice uygulanması kişilerin ayrımcılığa uğramaması açısından önemlidir. KVKK'da şeffaflık ilkesinin doğrudan belirtilmemiş olması, bu ilke üzerinden değerlendirmeyi gerekli kılmaktadır.

4.2. Doğru ve Gerektiğinde Güncel Olma

Kişisel verilerin doğru olması, gerektiğinde güncel olması durumu ayrı ayrı değerlendirilmesi gereken hususlardır. Kişisel verilerin özellikle yapay zeka-makine öğrenmesi temelli teknolojilerle çalışıldığında bir takım yanlış sonuçlara ulaşılabilmesi mümkündür. Yapay zeka temelli öğrenme modellerinin özellikle yanlış veri ile işlendiğinde yanıltıcı sonuçlar üretebilmesi mümkündür. Yanlış veri miktarı az olduğunda bu ihtimal nispeten düşükken, bu oran arttığında bu tür yanlış sonuçlara ulaşılması durumu risk yaratır. Kişisel sağlık verilerinin işlenmesi özelinde düşünüldüğünde, gerektiğinde güncel olma ilkesinin çok anlam ifade etmeyeceği görülür. Asıl olan bu platformlar için sürekli güncelliğin sağlanması ve doğru bilgi ile

[142] GDPR Recital 58
[143] https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G E.T:15.05.2023

sistemin beslenmesidir. Gerektiğinde güncel olma durumu bazı adli süreçler için verinin değiştirilmemesi gerekliliği durumlarında uygulama alanı bulabilir.

4.3. Belirli Açık ve Meşru Amaçlar İçin İşlenme

Özellikle yapay zeka sistemleri ile kişisel verilerin işlenmesi faaliyetleri açısından, amacın belirli ve meşru olması çok önem arz etse de, özellikle büyük veri ile çalışılan veri işleme faaliyetlerinde bu amaçtan sapabilmek çok olasıdır. Bu nedenle baştan amaç açık bir şekilde belirlense de denetim mekanizmalarının aralıklı olarak yapılması, ulaşılan sonuçlar üzerinden geriye dönük değerlendirmeler yapılması, özellikle kara kutu problemi de düşünüldüğünde dikkatli davranmak ihlallerin oluşumunu azaltabilecektir. Kişisel sağlık verileri özelinde yapay zeka uygulamalarını düşündüğümüzde; her ne kadar birçok ülkenin benzer yaklaşımlarla bu tür verileri koruduğunu görsek de yapay zeka alanının bilinmezleri, mevzuatsal korumayı, her ihlal öncesinde mümkün kılmamaktadır.

4.4. İşlendikleri Amaçla, Bağlantılı, Sınırlı ve Ölçülü Olma

Bu ilke temelde veri toplamadan önce veri sorumlusunun belirlediği amaç doğrultusunda ve gerekli olan minimal veri ile işleme faaliyetinin gerçekleştirilmesini sağlamaya çalışır. Önceki madde ile devamlılık arz eder. Fakat burada KVKK ile GDPR arasında bir farklılık mevcuttur. Bu durum 'yeni amaçlar için işleme' durumunda söz konusu olur. GDPR'a göre geçerli bir hukuki sebep varlığında kişisel verilerin başlangıçta belirtilen amaçla uyumlu olmak kaydıyla yeni bir amaçla işlenebileceğini kabul eder. Bu durum GDPR m.6/4' de şu şekilde ifade edilmiştir. "Kişisel verilerin başta toplandıkları amaçlardan farklı amaçlar için işlenmesine sadece baştaki amaçlarla uyumlu amaçlar için işleme halinde izin verilmelidir. Bu durumda baştaki amacın dayandığı hukuki sebepten ayrı bir hukuki sebep gösterilmesi gerekli değildir." KVKK'da ise bu duruma izin verilmemektedir. KVKK m.4 de "Sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, kişisel verilerin işlenme şartlarının ayrıca sağlanmış olması gerekecektir." denilerek her amaç değişikliğinin yeniden bilgilendirme ve onayı

gerektirdiğini belirtmiştir. Bu durumu da özellikle kişisel sağlık verileri ve yapay zeka teknolojileri kullanımı açısından değerlendirecek olursak; KVKK'daki düzenlemenin özel nitelikli veri için daha koruyucu olduğu, fakat özellikle kişisel sağlık verilerinin kullanıldığı bilimsel araştırmalar açısından gelişmeyi engelleyici bir unsur olabileceği endişesi vardır. Burada makul ve ölçülü değerlendirmelerin her olay özelinde değerlendirilmesi uygundur. GDPR'daki mevzuat farklılığının uygulama pratiği değerlendirilerek, koruyucu mekanizmaları zayıflatmadan bu süreci kolaylaştıracak düzenlemeler sağlanabilir.

Bu madde bağlamında GDPR ile KVKK arasında bir farklılık daha vardır. Bu da veri minimizasyonu ilkesidir. Bu ilke GDPR'da açıkca belirtilmektedir. KVKK'da ise veri işlemenin, amaçla sınırlı ve ölçülü olması ilkesinden ve dürüstlük kuralına uygunluk ilkesinden hareketle uygulama alanı bulmaktadır.[144]

Bu doğrultuda verilen bir karar; talep edilenden daha fazla veri aktarması nedeniyle veri sorumlusunu "amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi" ne uymadığı gerekçesiyle idari yaptırıma çarptırmıştır.[145]

4.5. Öngörülen veya Amaç için Gereken Süreler Kadar muhafaza Edilme

Bu ilke veri işlemenin amacının gerçeklemesi ile ya da başlangıçta belirlenen sürenin bitmesi ile verinin silinmesi gerekliliğini belirtir. Bu durumu kişisel sağlık verileri ve yapay zeka modelleri kullanımı özelinde değerlendirecek olursak bir takım sıkıntılarla karşılaşırız. Bunlardan ilki büyük sağlık verisiyle çalışan ve öğrenen yapay zeka sistemlerinin bu verilere sürekli ihtiyaç duymasıdır. Bir diğer durum ise daha önce de belirtildiği üzere bu sistemlerin kişisel veriler anonimleştirilse bile kişisel veriye dönüştürme becerileridir. Bu durum yakın gelecekte bir takım ihlallerle karşılaşacağımızın göstergesidir.

---

144 Retornaz, Güçlütürk, s.296

145 https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik- E.T:15.05.2023

SEKİZİNCİ BÖLÜM
İLGİLİ KİŞİNİN HAKLARI VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

KVKK md.11 ilgili kişinin haklarını düzenlemektedir. Bu düzenlemeyle, yapılan veri işleme faaliyetinin hukuka uygunluğu ilgili kişi tarafından denetlenebilmekte, veri işleme süreci takip edilebilmekte, aykırılık tespit edildiğinde ise, düzeltilmesini ya da zararın tazminini istemesi mümkün olabilmektedir.

Verisi işlenen kişinin bu faaliyetinin takibini yapabilmesi ve gereklilik halinde müdahale edebilmesi için veri sorumlusuna başvuru gerekebilecektir. Bunun usul ve esasları "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ" kapsamında düzenlenmiştir. Bu kapsamda veri sorumlusuna yapılacak başvuru "yazılı olarak veya kayıtlı elektronik posta(KEP) adresi, güvenli elektronik imza, mobil imza, ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla" yapılabilecektir.

Veri sorumlusu bu başvuruların etkin bir şekilde yapılabilmesi için gereken tüm idari ve teknik tedbirleri almak yükümlülüğü altındadır. Tebliğin 6. maddesine göre başvuru veri sorumlusu tarafından kabul edilir. Reddedilmesi durumunda bunun gerekçelendirilmesi gerekir. Verilen cevapta ilgili kişinin "adı, soyadını, Türkiye Cumhuriyeti vatandaşları için T.C kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirime esas elektronik posta adresini, telefon ve faks numarasını, talep konusunu ve veri sorumlusunun başvuruya ilişkin açıklamalarını" içermelidir. md.7 de bu başvuru usulü ile ilgili ücret konusu düzenlenmiştir. 10 sayfaya kadar ücret alınmayacağı, gereklilik halinde talep edilecek ücretin kayıt ortamının (CD, flash bellek vs.) maliyetini geçemeyeceği belirtilmiştir. Burada önemli olan kısım, ilgili kişinin hakkı kullanmasının önünde bir ücret engelinin bulunmamasını sağlamaktır.

Veri sorumlusuna başvurunun etkin kullanımını sağlamak esas amaç iken, diğer taraftan hakkın kötüye kullanımını da engellemek, düzgün işleyişi sağlamak açısından elzemdir. Bu bağlamda sırf veri sorumlusuna zorluk çıkarmak amacıyla yapılan başvurular, hakkın kötüye kullanımı yasağına aykırı oldukları takdirde dikkate alınmamalı, cevaplanmaması durumunda yaptırım uygulanmamalıdır. Buradaki zorluk bu şekilde başvuru olduğunun ispatı noktasındadır.

1. İLGİLİ KİŞİNİN HAKLARI

1.1. Kişisel Verisinin İşlenip İşlenmediğini Öğrenme Hakkı

Bu hakkın etkin bir şekilde kullanımı, veri sorumlusunun bilinmesi ve ilgili kişinin veri sorumlusuna kişisel verisinin işlenip işlenmediği konusunda başvurusu ile mümkün olacaktır. İlgili kişi işlenen, depolanan kişisel verisi olup olmadığı hakkında bilgi talep edebilecektir. İlgili kişinin kişisel verisi işlenmemiş olsa bile talep halinde verisinin işlenmediği bilgisi verilmelidir. Sessiz kalma ya da soruyu cevaplamama durumunda veri sorumlusu kanundan doğan yükümlülüğünü yerine getirmiş sayılmayacaktır.[146]

1.2. Kişisel Verisi İşlenmişse Buna ilişkin Bilgi Talep Edebilme Hakkı

Kişisel verisi işlenen kişi, bu veri işleme işlemi hakkında bilgi talep edebilir. Burada işlenen kişisel verilerin neler olduğu, niteliği, kapsamı gibi sorular gündeme gelir. Bilgilerin kontrolü ve gerektiğinde düzeltme, silme işleminin efektif kullanımı söz konusu olduğunda bu verilerin ilgili kişiye tam olarak iletilmesi gerektiği sonucuna varılabilir. Tüzük kapsamında değerlendirildiğinde bu konuda bir takım tartışmalar olduğu görülmektedir. Tüzük md.15/1'de talep edilebilecek veri kategorileri belirtilirken f.3 'de işlenen kişisel verilerin bir nüshasının ilgili kişiye verileceğinden bahsetmektedir. Bilgi talep etme hakkı dar yorumlandığında; verilerin işleme amaçları, verinin türü, kişisel verilerin açıklandığı ya da açıklanacağı üçüncü ülkeler ve

[146] Korkmaz, İbrahim. Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme. Türkiye Barolar Birliği Dergisi, 2016 (124), s.81-152

uluslararası kuruluşlar, kişisel verilerin saklanması için öngörülen süre, bu sürenin belirlenmesinde kullanılan kriterler, itiraz, düzeltme ve silme hakkının etkin kullanılabilmesi için profil çıkarma, otomatik işleme yoluyla işlenen bilgilerin varlığı gibi bir takım bilgilere ulaşılabilmesi sağlanmalıdır.

Tüzük md.15 f.1'de bahsedilen hususlar ilgili kişiye ait tüm aşamaları kapsamayabilir. Almanya'nın Baden Württemberg Eyaletinde İş mahkemesine konu olan olayda iş sözleşmesi feshedilen bir işçi kendisine ait tüm belgeleri talep etmiştir. Bilgi talep hakkı geniş yorumlandığında ilgili kişiye ait tüm dökümanlar, e-posta iletileri, kişinin adı geçen tüm evrakların verilmesi gerekecektir. Bu durum, bu dökümanlarda ismi geçen 3. Kişilerin kişisel verilerinin de verilmesine, bazı durumlarda ticari sır niteliğindeki bilgilerin paylaşılması gibi durumları oluşturabilecektir. Dolayısıyla bazı mağduriyetler ve menfaat çatışmaları gündeme gelebilecektir. Ayrıca bu talep ölçülülük ilkesi çerçevesinde değerlendirilmelidir.

1.3. Kişisel Verilerin Amacına Uygun Kullanılıp Kullanılmadığını Öğrenme Hakkı

KVKK md.4 f.2/b/c ye göre kişisel veriler "belirli, açık ve meşru amaçlar için" işlenmelidir. İlgili kişinin bu amaçlar konusunda bilgilendirilmesi alınacak rızanın geçerliliğini de sağlayacaktır. İlgili kişi böylelikle bu amaç doğrultusunda kullanılan kişisel verisinin, ölçülülüğünü, gerekliliğini değerlendirebilme imkanına sahip olacaktır. Öte yandan belirlenen amaç doğrultusunda gerekli olan güvenlik önlemleri düzenlenebilecek ve ihlali durumunda tazminat hakkı gündeme gelecektir.

1.4. Yurt İçinde veya Yurt Dışında Kişisel Verilerin Aktarıldığı Üçüncü Kişileri Bilme Hakkı

İlgili kişiye tanınan bu hak yine denetim hakkı ile yakından ilgilidir. KVKK md.8 ve 9 da belirtilen aktarma hallerinde ilgili kişinin bu süreci takip edebilmesi mümkün olabilmekte, olası bir ihlalde müdahale edebilmesine imkan sağlamaktadır.

1.5. Kişisel Verilerin Eksik veya Yanlış İşlenmesi Durumunda Bunların Düzeltilmesini İsteme Hakkı

Bu düzenleme ilgili kişinin, kişisel verisi ile ilgili eksiklerin tamamlanması veya yanlışlık varsa düzeltilmesi hakkını tanımlar. KVKK'da "*eksik veya yanlış işlemenin düzeltilmesi"* düzenlenmiş olmasına rağmen bu ifadenin "*tamamlanması ve ya düzeltilmesi*" şeklinde değiştirilmesi, daha iyi ifade etmesi açısından uygun olacaktır. Nitekim Tüzükte bu iki hak ayrı şekilde tanımlanmıştır. Düzeltme hakkı AY md.20 de açıkça düzenlenmiştir. Ayrıca bu hak KVKK md.4 f/2-b çerçevesinde düzenlenen "doğru ve gerektiğinde güncel olma ilkesi" ile de uyumludur. Burada bir diğer önemli konu; verinin doğruluğuna nasıl karar verileceğidir. Subjektif değerlendirmelerin dikkate alınması durumunda ortaya çıkabilecek sorunlar göz önüne alındığında, burada objektif değerlendirme üzerinden doğruluğu kabul etmek uygun görünmektedir. Veri yanlış olmasa bile anlamı muğlak ve yanlış anlaşılmalara müsaitse bu durumun da düzeltilebilmesi uygun olacaktır. Değer yargılarına ait veriler kişilik hakkı ve mahremiyet ilkelerine müdahale niteliği taşıyorsa bunun kişisel veri olarak değerlendirilmesi mümkündür. Özellikle değer yargıları bir takım somut olaylara dayandırılıyorsa, örneğin kişinin ırkı, dini ve medeni hali gibi bilgiler üzerinden değer yargısına varılıyorsa burada kanunun koruması altına alınması uygun olacaktır.[147]

İlgili kişinin verisini düzeltme talebi olduğunda bazen bu durumun içerisine üçüncü kişilerin de kişisel verileri dahil olabilmektedir. Bu durumda somut olayın özelinde değerlendirme yapılarak karar verilmesi gerekebilmektedir. Böyle durumlarda bile kişinin verisinin düzeltilmesini talep etme hakkı vardır.

Kendisine talepte bulunulan kişisel veriyi düzeltme isteğini gerekli şekilde yerine getirmeyen veri sorumlusunun sorumluluğu söz konusu olacaktır. Çünkü bu durumda

[147] Çekin, s.125-126

KVKK md. 4 f/2-b de bahsi geçen "*doğru ve güncel olma*" ilkesine aykırı veri işleme söz konusu olacaktır.[148]

1.6. Kişisel Verilerin Silinmesini veya Yok Edilmesini İsteme Hakkı

İlgili kişi KVKK md.7 çerçevesinde "kişisel verilerinin silinmesini ya da yok edilmesi" ni talep edebilir. Bu maddeye göre veri işlemesini gerektiren sebep ortadan kalktığında verilerin silinmesi ya da yok edilmesi ilgili kişi tarafından talep edilebilir. Bu durum "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" kapsamında düzenlenmiştir. İlgili yönetmelik md.5 f.2 de veri işlenme şartlarını ortadan kaldıran haller şu şekilde belirtilmiştir:

"a) *Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,*
b) *Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi*
c) *Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması*
ç) *Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması*
d) *Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,*
e) *İlgili kişinin, kanunun 11 inci maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,*
f) *Veri sorumlusunun, ilgili kişi tarafından kişisel verilerin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya kanunda öngörülen süre içinde cevap vermemesi hallerinde; kurula şikayette bulunulması ve bu talebin kurul tarafından uygun bulunması,*

[148] Çekin, s.127

g) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

ğ) Kanunun 5 inci ve 6 ıncı maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması"

Bu şartlar gerçekleştiği takdirde, ilgili kişiye ait kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekecektir. Silinme kavramı ile bahsedilen durum yönetmelik md.8 de düzenlenmiş ve detaylandırılmıştır. Buna göre; silinme, "tamamen ya da kısmen otomatik yollarla işlenen kişisel verilerin silinmesi; söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirilmesi" durumudur. Kişisel verilerin silinmesi diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise*;*

"*a) Kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi,*

b) Başka herhangi bir kurum, kuruluş ve/veya kişinin erişimine kapalı olması

c) Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması, kaydıyla kişisel veriler silinmiş sayılacaktır."

Yönetmelik md.9 f/1'de yok edilme kavramı; "bilgilerin saklandığı veri saklamaya elverişli tüm fiziksel kayıt ortamlarının tekrar geri getirilemeyecek ve kullanılamayacak hale getirilmesi" olarak tanımlanmıştır. Bu maddede herhangi bir istisna düzenlenmemiştir.

Yönetmelikte (md.10 f/1) bahsi geçen kişisel verilerin anonim hale getirilmesi kavramı ise şu şekilde tanımlanmıştır: "*Kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi*" Fakat bu durumun uygulanması ilerleyen teknoloji ile birlikte zorlaşmakta, hatta imkansızlaşmaktadır. Bununla ilgili AOL ve Netflix firmalarınca yayınlanan müşteri

verilerinin New York Times gazetecileri tarafından diğer bazı bilgilerle eşleştirilerek bazı kişilere ait kimlik tespitini sağlayabilmişlerdir.[149]

1.7. Düzeltme, Silme ya da Anonim Hale Getirme Taleplerinin Üçüncü Kişilere bildirilmesi Hakkı

İlgili kişiye ait kişisel veriler bazı durumlarda sadece veri sorumlusunda kalmamakta üçüncü kişilerle de paylaşılmaktadır. Bu durum özellikle internet ortamında paylaşılan veriler için geçerlidir. Böylelikle paylaşılan bu veri birçok arama motorunda dolaşır hale gelmektedir. Paylaşılan kişisel veri birçok platforma yayıldığından kişilerin geleceğini etkileyebilmektedir. Bu nedenle bu hakka 'unutulma hakkı' da denilmektedir. Bahsedilen durumda veri üçüncü kişilerle de paylaşıldığından, sadece veri sorumlusunun verileri silmesi yeterli olmayacak, üçüncü kişilerin de verileri silmesi, yok etmesi ya da anonim hale getirmesi gerekecektir.

Bu açıdan KVKK, direktif md. 12 b/c yle uyumlu olarak ilgili kişiye verilerinin düzeltilmesi, silinmesi ya da yok edilmesini isteme hakkının yanı sıra bu talebin üçüncü kişilere bildirilmesini talep etme hakkı da tanımıştır. Burada her ne kadar düzeltme, silme ve yok etmeden bahsedilmiş olsa da anonim hale getirme işleminin de bu işlemlerle birlikte düşünülmesi uygundur. Kanuna göre ilgili kişi bu hakkını kullanırken veri sorumlusuna başvuracak, veri sorumlusu ise verilerin paylaşıldığı üçüncü kişilere bu isteği iletecektir. Kanun bu yükümlülüğü veri sorumlusuna yüklemiştir.

Burada oluşabilecek problemlerden bir tanesi de veri sorumlusunun bu talebi ileteceği üçüncü kişilerin başka bir veri sorumlusu olmaması veya bu kişilerin tamamına ulaşılamayacak olmasıdır. Bu gibi durumlarda kanun yetersiz kalmaktadır. Bu yetersizlik AB hukukunda tartışmalara neden olmuştur.[150]

[149] https://www.wired.com/2009/12/netflix-privacy-lawsuit/ E.T:19.05.2023
[150] Çekin, s.130-134

Avrupa Adalet Divanının Google –İspanya kararındaki değerlendirmesi önemlidir. Bu karara konu olan olayda bir İspanyol daha önce aleyhine gerçekleşmiş bir haciz olayına dair yerel basında yayınlanan bir haberin kaldırılmasını talep etmiştir. Bu talebini hem yerel gazeteye iletmiş hem de arama motoru google'dan bu sayfaya olan tüm yönlendirmelerin iptalini istemiştir. Avrupa Adalet Divanı, kişisel veriler barındıran internet sitelerinin, arama motorları tarafından arama sonuçlarında sunulmasının, Temel Haklar ve Özgürlükler Şartı md.7-8 i ihlal edebileceğini, bu şekilde bilgi edinilmesinin özel hayatın gizliliği ilkesine aykırılık doğuracağı ve profilleme oluşturma ihtimalinin doğacağını belirtmiştir. Bu sebeple mahkeme yönerge md. 12/b ve md 14 f.1/b kapsamında ilgili kişinin, arama motoru işleticisinden, kendisi ile ilgili sonuçları, üçüncü kişilerin arama sonuç listesinden kaldırılması talebini uygun bulmuştur.[151] Yargıtay da bu kararla uyumlu olarak unutulma hakkını açıkça kabul etmiş, bunun özel hayatın gizliliği hakkının bir parçası olduğuna hükmetmiştir.[152]

Analog ortamlarda verilerin silinmesi veya imha edilmesi, veri sorumlusunun müdahalesiyle kolaylıkla gerçekleştirilebilirken, dijital ortamda bu konuyla ilgili bazı zorluklar ortaya çıkmaktadır. Verilerin taşıyıcısı tek başına veriyi silse veya imha etse bile yeterli olmayabilir. Çünkü veriler, mevcut durumda birçok web sitesinde arşivlenebilir ve arama motorları tarafından kaydedilebilir. Bu durum, veri sorumlusunun veriyi silse veya üçüncü şahıslara bu talebi iletip gerçekleştirilmesini beklemesiyle çözülemeyen bir durum oluşturur. İşte bu yüzden AB mevzuatı, veri silme hakkının yanı sıra "*unutulma hakkı*"ndan da bahsetmektedir.

Bu durum, dijital teknolojilerin hızla geliştiği günümüzde, verilerin silinme ve düzeltilme hakkının daha etkin bir şekilde kullanılmasını sağlamak amacıyla düzenlenmiştir ve bu sorunun çözümü için doğru bir yaklaşımdır. Söz konu düzenlemeye göre, "Veri sorumlusu, kişisel verileri kamuya açıkladığı ve kişisel verileri silmek zorunda olduğu durumlarda, mevcut teknoloji ve uygulama maliyetini dikkate alarak, veri sahibinin talep ettiği kişisel verileri işleyen veri sorumlularını,

[151] Google-İspanya Kararı https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf E.T:19.05.2023
[152] Yargıtay Hukuk Genel Kurulu, E:2014/4-56 k.2015/1679 T.17.6.2015 kazancı.com

ilgili kişisel verilere bağlantılar veya bu verilerin tüm kopyalarının silinmesi gibi teknik tedbirler de dahil olmak üzere, bilgilendirmek için makul önlemler alır. İlk taslakta, veri sorumlusu üçüncü tarafların eylemlerinden dolayı sorumlu tutulurken, tüzüğün son halinde sadece üçüncü tarafların bilgilendirilmesiyle yetinilmiştir.[153]

Günümüzde, iletişim teknolojisinin hızlı gelişimi nedeniyle üçüncü kişilere ulaşmak genellikle zor bir durum haline gelmiştir. Bu durumda, bu kişilerin nasıl bilgilendirileceği konusu belirsizlikler içermektedir. Bu sebeple, tüzükte "mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak" çözüm yolları oluşturulmaya çalışılmıştır.

AB'nin unutulma hakkını düzenleme çerçevesindeki temel amacı, dijital dünyada silme ve düzeltme hakkının güncellenmesi ve sınırlarının belirlenmesidir. Bu düzenleme, özellikle çocukluk döneminde verilen rızaların yetişkinlik döneminde kişinin istemediği sonuçlara yol açmasını engellemeyi hedeflemektedir. Bu nedenle, GDPR özellikle çocuklukta verilen rızaların kişinin risk değerlendirmesi yapma yeteneğinin yetersiz olduğunu vurgulamış ve unutulma hakkının kullanılabileceğini belirtmiştir.[154]

Unutulma hakkının uygulanma alanının belirlenmesi, yani coğrafi sınırların tespiti, bu konuda en çok tartışılan konular arasında yer almaktadır. Özellikle Fransa'nın veri koruma otoritesi (CNIL) ile Google arasındaki anlaşmazlık büyük önem taşımaktadır. CNIL, unutulma hakkı çerçevesinde bazı bağlantıların google.fr ve google.de'den kaldırılmasını talep etmiş, ancak bu bağlantıların google.com'da hâlâ bulunmasından dolayı idari para cezası öngörmüştür. Google ise bu cezayı temyize götürerek unutulma hakkının uygulanma alanı konusunda bir tartışma başlatmıştır.

Fransa, bu anlaşmazlığı Avrupa Birliği Adalet Divanı'na taşımıştır. Google, savunmasında unutulma hakkı ile ifade özgürlüğü arasında bir denge kurulması gerektiğini ve küresel bir uygulama alanının mümkün olmadığını ileri sürmüştür.

[153] Çekin, s.133
[154] European Commission, Factsheet on the "Right to be Forgotten" ruling (C131/12)

Bunun sebebi, ifade özgürlüğünü kısıtlayan ülkelerin coğrafi sınırlardan yararlanarak bu hakkı aşırı derecede etkileyebilecek olmasıdır. CNIL ise kişilerin IP adresini değiştirerek bu içeriğe erişim sağlayabileceklerini belirtmiş ve bu nedenle sadece yerel alanda engellemenin unutulma hakkına hizmet etmeyeceğini ifade etmiştir.

Temel olarak, CNIL'in böyle bir küresel etkiye sahip bir karar alması, diğer devletlerin egemenlik alanını tehdit eden bir davranış olarak değerlendirilebilir. Ayrıca, unutulma hakkını tanımayan ve ifade özgürlüğünü önceliğine alan ülkelerde bu tür bir uygulamanın benimsenmesinin mümkün olmadığı da savunulmaktadır. Ülkeler arasındaki politika farklılıkları, tek bir kararın küresel bir etki yaratmasını beklemeyi güçleştirmektedir. Fransa'nın perspektifinden bakıldığında, unutulma hakkının anlam kazanabilmesi için ilgili bağlantının kişilerin ulaşamayacağı şekilde kaldırılması gerekmektedir. Bununla birlikte, sadece yerel alandaki bağlantıyı kaldırmak, kişinin bu bilgiye erişimini engellememektedir. CNIL'ın iddiasına karşılık yapılan yorumlarda, bağlantının amacının bilgiye hiçbir şekilde erişilememesini değil, sadece erişimi zorlaştırmayı hedeflediği belirtilmektedir.

Bu uyuşmazlığa bir çözüm olarak Google, coğrafi engelleme yöntemini kullanmayı teklif etmiştir. Yani, Avrupa sınırları içinde değil, aramayı yapan kişinin coğrafi konumunu tespit ederek o bölgeden yapılan aramaları engellemek önerilmiştir. Coğrafi engelleme yöntemi, unutulma hakkının amacıyla uyumlu olduğu düşünülse de, internet kullanımının temel amacına ters olduğu şeklinde eleştirilere de maruz kalmaktadır. Tam olarak Fransa'nın istediği sonuç olmasa da, yerel alanda bağlantı kaldırılmasından daha etkili bir çözüm olacağı kesindir.[155]

Bu uyuşmazlığın çözümü için Google, 21 Ocak 2016 tarihinde coğrafi engelleme yöntemini kullanma önerisinde bulundu. Buna göre, Avrupa sınırları içinde bağlantıları kaldırmak yerine, arama yapan kişinin coğrafi konumunu belirleyerek o bölgeden yapılan aramaları engellemeyi önerdi. Coğrafi engelleme yöntemi, unutulma

[155] CNIL.fr, Right To Be Delisted: The CNIL Restricted Committee Imposes A €100,000 Fine On Google | CNIL", https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google, E.T:19.05.2023

hakkının amacıyla uyumlu kabul edilse de, internet kullanımının temel amacına aykırı olduğu şeklinde eleştirilere maruz kaldı. Fransa'nın tam olarak istediği sonuç olmasa da, yerel alanda bağlantıların kaldırılmasından daha etkili bir çözüm olacağı açıktır. Bununla birlikte, günümüzde Türkiye, İran, Çin ve Kuzey Kore gibi ülkelerde sınırlı ve özerk internet uygulamaları bulunmakta olup, belirli içeriklerin veya sitelerin güvenlik duvarlarıyla engellenmesi gibi kısıtlamalar söz konusudur. Bu tür uygulamalar, bilginin ve internetin evrenselliği gibi özelliklere ters düşmektedir. Ayrıca, farklı içerikler için birçok ülkenin bu tür kısıtlamaları uygulamaya başladığını düşünmek, endişe verici bir durumdur.[156]

Bu bağlamda, Daphne Keller'ın makalesi ölçülülük prensibine vurgu yaparak benzer bir görüşü paylaşmaktadır. Yazıda, 95/46 sayılı Direktif'in 12. ve 14. maddeleri incelenmekte ve unutulma hakkının, olaya özel olarak makul bir şekilde belirlenmesi gereken esnek bir kapsama sahip olduğu ifade edilmektedir. ABAD'ın C-131/12 sayılı Kararı'nda, unutulma hakkının teknik kapsamını belirlemek için kullanılan prensiplerin coğrafi kapsamı belirlemek için de uygulanabileceği savunulmaktadır.[157]

Mahremiyet kavramı, pek çok hak ve özgürlüğü etkileyen, korunması gereken önemli bir kavramdır. Bazı durumlarda çatışan haklar karşımıza çıkabilir. Böyle durumlarda çatışan haklar arasında bir dengenin oluşturulması ölçütümüz olmalıdır. Haklar dengesi ve ölçülülük birlikte düşünüldüğünde, bireyin gizliliğinin korunması karşısında uluslararası hukuk prensipleri, devlet egemenliği, ifade özgürlüğünün korunması, internetin doğal yapısının korunması gibi birçok hakkın zarar görmemesi sağlanmalıdır. Unutulma hakkının temelinde bilgiye ulaşılmasının engellenmesi değil, zorlaştırılması yatmaktadır. Bu nedenle, CNIL'ın savunduğunun aksi de mümkündür. küresel erişimin engellenmesi ve bağlantının kaldırılması kabul edilemez bir yöntem olmayacaktır. Unutulma hakkına yöneltilen birçok eleştiri mevcuttur. Hakkın net bir tanımının olmaması bunlardan ilkidir. Bunun nedeni tanımlamanın geniş tutulması olabilir. Tanımın daraltılması birçok kişi tarafından önerilse de Viviane Reding bu

[156] Nalbantoğlu S. Right to be Forgotten As a Fundamental Right, TAAD, Yıl:9, Sayı:34 2018, s.583-607

[157] https://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong ET:23.04.2023

düzenlemelerin gelecek teknolojilere uyumunun sağlanması içi tanımlamanın geniş tutulması gerektiğini belirtmiştir.[158]

Tanımdaki eksikliklerle ilgili ortaya çıkan bir diğer tartışma, bir fotoğraftaki kişilerden birinin unutulma hakkını talep edip edemeyeceği ve bu durumun diğer kişiler açısından nasıl değerlendirileceği, itiraz haklarının olup olmadığı konusunda yoğunlaşmaktadır. Fotoğraftaki herkesin veri sahibi olarak kabul edildiğinde, mevcut tanımlama ile hangi veri sahibinin haklarının öncelikli olduğuna dair bir değerlendirme yapmanın zor olduğu düşünülmektedir.[159]

Veri sorumlusu tanımının genişletilmesine yönelik bir eleştiri de meevcuttur. Burada unutulma hakkına ilgili değerlendirme yapılırken haklar dengesine dikkat edilmesi gerekir. İngiliz Lordlar kamarasında yapılan bir düzenlemede, haklar dengesi değerlendirmesini arama motorlarının yapmasını öngörülmektedir. Bu düzenlemeye göre Google'a karar verme yükümlülüğü verilmiştir. Buna göre Google ifade hürriyeti benzeri hakların sınırlanması ile ilgili olarak bir karar verebilecektir. Veri sorumlusuna özellikle GDPR kapsamında ağır cezalar verilebilme ihtimali doğuran bu durum, veri sorumlularının cezalardan kaçınabilmek adına silinmemesi gereken verileri de silme tarafında olabileceğini düşündürmektedir. Bununla birlikte bu konuda ekonomik menfaati bulunan arama motorlarının bu değerlendirmede objektif olmayacakları konusunda haklı endişeler mevcuttur. Ayrıca veri sorumlusuna bu denli ağır yük yüklemek zaman ve iş kaybına neden olabilecek ve ölçülülük ilkesine aykırılık oluşturabilecektir.[160]

Teknolojinin ve internetin böylesine geliştiği ve yaygınlaştığı bir dönemde, unutulma hakkının kişiye sağlanmasının mümkün olup olmadığı büyük bir merak konusudur. Bu hak, hızla ilerleyen internetin özel hayata verdiği zararları en aza indirgeyerek kişiye

[158] Jeffrey R. Symposium Issue, The Right To Be Forgotten, 64 Stan.L.Rev.Online 88, s.92, E.T. 19.05.2023

[159] Emily AS. Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation, 39 Brook. J. Int'l L,2014, s. 501-502

[160] Elmalıca H. Bilişim çağının ortaya çıkardığı temel bir insan hakkı olarak unutulma hakkı. Ankara Üniversitesi Hukuk Fakültesi Dergisi 65 ,2016, s. 1603-1636

imajını ve verilerini kontrol etme imkanı sağlamayı hedeflemektedir. Bu hassasiyetin gerçekleştirilmesi amacıyla herkesin aklına ilk gelen soru, bir içeriğin internete bir kez yüklendikten sonra kaldırılabilme olasılığıdır. Unutulma hakkı kapsamında, içeriğin kendisi asıl kaynaktan silinmemektedir. Bunun yerine, arama motorları tarafından içeriğe yönlendiren bağlantıların kaldırılması sağlanmaktadır. Bu şekilde değerlendirildiğinde, içerik hala asıl kaynak üzerinde varlığını sürdürmektedir. İçerik asıl kaynaktan kaldırılmış bile olsa, diğer internet siteleri aracılığıyla kopyalanan verilerle içeriğin internet ortamında hala bulunması mümkündür. Arama motorları, her kopya içeriği tek tek tespit edip bağlantıyı kesme yükümlülüğü altında olmadığından, kopya içerikler içeren sitelere arama motorları aracılığıyla erişim sağlanması mümkündür. Bu durumda, dijitalleşmenin göz önünde bulundurulduğu bir ortamda bir içeriğin tamamen ve sonsuza kadar internetten kaldırılmasının mümkün olmadığı unutulmamalıdır.[161]

1.7.1. Yargıtay Hukuk Genel Kurulu'nun Unutulma Hakkına İlişkin Kararı

Bu olayda davacı, cinsel saldırıya uğradığı olayın Yargıtay kararında[162] yer almasıyla kişilik haklarının ihlal edildiği gerekçesiyle tazminat davası açmıştır. Yerel mahkeme, davacının talebinin kısmen kabul ederek manevi tazminat ödenmesine hükmetmiştir. Ancak, Yargıtay davacının isminin bilimsel bir kitapta açık bir şekilde kullanılmasının kişilik haklarına saldırı teşkil etmeyeceğini belirterek kararı bozmuştur. Davacının isminin yayınlanmasının bilimsel bir çalışmanın bir parçası olduğunu ve bu durumun kişilik haklarına zarar vermediğini ifade etmiştir. Yeniden yapılan yargılama sonucunda yerel mahkeme, önceki kararında direnerek davacının talebini reddetmiştir. Bunun üzerine dava Hukuk Genel Kurulu'na taşınmıştır. Hukuk Genel Kurulu, unutulma hakkı ve kişisel verilerin korunması ile bilim ve sanat hürriyeti arasında adil bir denge kurulması gerektiğini vurgulayarak davacının talebini kabul etmiştir.

[161] Elmalıca, s.1621-1622
[162] Yargıtay Hukuk Genel Kurulu'nun 17.06.2015, 2014/4-56 E, 2015/1679 K. sayılı kararı. E.T.19.05.2023

Hukuk Genel Kurulu, davacının unutulma hakkı ve kişisel verilerinin korunması hakkının ihlal edildiğini ve manevi tazminat talebinin haklı olduğunu belirtmiştir. Kararda, kişisel verilerin kamunun kolayca ulaşabileceği yerlerde tutulan her türlü veri için unutulma hakkının geçerli olduğu vurgulanmıştır. Bu açıdan bakıldığında, davacının cinsel saldırıya uğradığı olayın isminin açık bir şekilde yayınlanmasıyla unutulma hakkı ve özel hayatın gizliliği ihlal edilmiştir. Hukuk Genel Kurulu'nun bu kararı, unutulma hakkı ve özel hayatın gizliliği konularında önemli bir içtihat niteliği taşımaktadır. Karar, kişisel verilerin korunması ve bilim-sanat özgürlüğü arasında adil bir denge kurulması gerektiğini vurgulayarak, benzer uyuşmazlıklar için referans teşkil edebilecek bir yol gösterici niteliğindedir. Hukuk Genel Kurulu'nun bu kararı, unutulma hakkının Türk hukukunda somut bir temele oturduğu ilk metin olması açısından önemlidir. Karar, unutulma hakkıyla ilgili geniş açıklamalar içermesi nedeniyle, ileride yapılacak kanuni düzenlemelerin ve uygulama sorunlarının çözümüne ışık tutabilecek niteliktedir. Ancak, kararın unutulma hakkını temel alması, Türk hukukunda kanuni bir dayanağının olmamasıyla eleştirilebilir. Anayasa'nın 20. maddesinin 3. fıkrasının son cümlesi, kişisel verilerin korunması hakkının -ve dolayısıyla unutulma hakkının- yalnızca kanunla düzenlenebileceğini belirtmektedir. Türkiye'deki kişisel verilerle ilgili mevzuatta unutulma hakkına dair bir düzenleme bulunmamasına rağmen, bu kavramın yargı içtihatlarıyla hukuki bir zeminde yer alması, kanunilik ilkesinin ihlal edilmesine neden olabilecek sakıncaları beraberinde getirmektedir.[163]

Kişisel verilerin korunması hakkının tarihsel süreçteki gelişimi ve amaçlananın bireyin kişisel verilerinin korunması olduğu düşünüldüğünde, unutulma hakkının ayrı bir hak olarak neden gereklilik arz ettiği sorusu akla gelebilir. Bireyin kişisel verilerine yönelik silme hakkı, yaşamını özgürce sürdürebilmesi için her zaman yeterli olmayabilir. Günümüz teknolojisiyle birlikte her türlü kişisel verinin sınırsız bir şekilde kaydedilmesi ve hızlı bir şekilde geniş kitlelere ulaşabilmesi, verilerin tamamen silinmesini zorlaştırmaktadır. Bu durum, bireyin üçüncü kişilerin

[163] Elmalıca, s.1628-1629

gözetiminden kurtulma ve özgür bir yaşam sürme isteğiyle birlikte unutulma hakkının gerekliliğini ortaya çıkarmaktadır.[164]

Potansiyel çok ciddi bir soruna işaret eden unutulma hakkı, dijital dünyadaki kişilere ait izlerinin silinmesiyle ilgilenir. Diğer bir deyişle bu hak, kişilerin geçmişinin kendi talebiyle silinip silinemeyeceği sorusunun bir sonucu olarak ortaya çıkmıştır.[165]

Unutulma hakkı, kişilerin dijital dünyadan istedikleri verilerini çıkarabilme hakkını ifade eder. Bu verilere resimleri, adres bilgileri, isimleri vb kişisel verileri dahil edilebilir. Bu tür kişisel veriler rahatsız edici içerikler şeklinde olabilir ve ilgili kişi bu içeriklerin yayılmasını isteyebilir. Temelde unutulma hakkı, kişinin kendine ait kişisel verileri üzerinde tayin hakkı kapsamında değerlendirilir. Bu bağlamda düşünüldüğünde , unutulma hakkı kişilere bazı olanaklar sunar. Böylelikle kişiler geçmiş ve geleceklerini, hür iradeleriyle yönetebilme imkanı bulurlar. Dijital dünyada verilerin yayılma ve paylaşılma hızı düşünüldüğünde, bu hakkın uygulanabilmesi imkansız gibi görünebilir. Bu hakkın karşısında fikir belirtenlerin ortak değerlendirmesi "eğer unutulmak istiyorsanız baştan hatırlanmayacaksınız" şeklindedir.[166]

Unutulma hakkı, kişilerin belirli bir zaman dilimindeki verileri üzerinde hak sahibi olması durumuna dayanır.[167]

Unutulma hakkı, pozitif ve negatif olmak üzere iki temel hakkı içermektedir. Pozitif hakkı, bireyin kendi geçmişi üzerinde kontrol sahibi olmasını ifade ederken, negatif hakkı ise unutulmak, hatırlanmamak isteme durumunu içerir. Bu şekilde unutulma

---

[164] Özdemir H. Haberleşmenin Gizliliği ve Kişisel Verile, *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, Y:2009, C:XIII, S:1-2, s.285.

[165]Gülener S. Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", *Türkiye Barolar Birliği Dergisi*, Y:2012, S:102, s.221.

[166] Kulevska S. The Future of Your Past: A Right to be Forgotten Online?, June 24, 2013 http://www.chillingeffects.org/international/weather. cgi?WeatherID=769 E.T: 19.05.2023

[167] Çınar A. Unutulma Hakkının Ortaya Çıkış Serüveni Ve Kapsamının Değerlendirilmesi, TAAD, Yıl 13 Sayı 49 Ocak 2022, s.551-584

hakkı, bir kişinin kapsamlı ve geniş bir şekilde kendi hakkındaki bilgileri silme hakkı olarak da görülebilir. Bu hak, bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlama yetkisine sahip olmanın yanı sıra geçmişteki cezalarına ilişkin bilgilerin veya olumsuz yorumlara yol açabilecek bilgi ve fotoğrafların kaldırılmasını talep etme hakkını da içermektedir.[168]

Bireyin unutulma hakkı talebi üzerine, veri sorumlusunun, veriyi silme veya yok etme yükümlülüğü de vardır. Ancak, bu verilerin kullanımı ve işlenmesi , ifade özgürlüğü kapsamında değerlendirilebilir, hukuki bir zorunluluk bulunabilir veya kamu yararı söz konusu olabilir. Bu durumlarda, veriyi sorumlusunun talebi reddetme hakkı vardır. Yani, unutulma hakkı talebi veri sorumlusu tarafından değerlendirilir ve belirli durumlarda talep reddedilebilir.[169]

1.7.2. Unutulma Hakkı ve Haberleşme ve İfade Özgürlüğü ilişkisi

Unutulma hakkı, bazı durumlarda haberleşme özgürlüğü ile çatışabilir. Kişiler kendilerine ait veri üzerinde hak sahibi olduklarını söylerken, diğer kişiler ise haberleşme özgürlüğü çerçevesinde bilgi alma hakları olduğunu söyleyebilir. Oluşabilecek çatışma durumu ölçülülük ilkesi çerçevesinde çözülmelidir. Buradaki çatışma daha çok iletişim özgürlüğü temelindedir.

Haberleşme bireylerin ya da insan topluluklarının ilişki süreçlerinde bilginin üretilmesi, paylaşılması, geliştirilmesi sürecinde kullandıkları bir araçtır.[170]

[168]Fleischer P. The right to be forgotten, or how to edit your history. http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html E.T:19.05.2023
[169]Ahi Ş. Unutulma Hakkı (The right to be forgotten). https://ahi.av.tr/unutulma-hakki-the-right-to-be-forgotten/ E.T:19.05.2023

[170] Gedik Ö. Türk Yargı Kararları Çerçevesinde Kitle İletişim Özgürlüğü, Seçkin Yayınları, Ankara 2008, s.39.

Haberleşme her ne kadar insan ilişkilerinde çok önemli bir kavram olsa da günümüz teknolojisi düşünüldüğünde bir araç olarak haberleşme cihazlarının özel hayatın gizliliği açısından ciddi ihlaller oluşturma riski olduğu açıktır. Bu durum insanlar arasında ciddi endişelerin oluşmasına neden olmuş ve bununla ilişkili özellikle kişisel verilerin korunması hususunda ulusal ve uluslararası kuruluşlar önlem almaya başlamışlardır.[171]

Diğer taraftan AİHM'in "Google" sitesine erişimle ilgili verdiği Ahmet Yıldırım/ Türkiye kararı önem arz etmektedir. Bu kararda internetin kişilerin ifade ve bilgi edinme özgürlüğü açısından önemine değinilmiştir. Ayrıca internetin günümüzde haber alma ve verme özgürlüğünün çok önemli bir parçası olduğu belirtilmiştir.[172]

Haberleşme ve ifade özgürlüğü ile unutulma hakkı arasında adil bir dengenin kurulması gerektiği kuşkusuzdur. Diğer bir ifadeyle, toplum için önem taşıyan bir bilgi dışında, bireyin rızasına aykırı olarak kişisel verilerinin internet ortamında yer alması haberleşme ifade özgürlüğü çerçevesinde kabul edilemez. Bu durumun kişinin rızası dışında sürmesi, bireyin hayatını özgür ve serbest biçimde sürdürememesine neden olur.

Avrupa Komisyonu tarafından Ocak 2012'de teklif edilen Direktif md.17 unutulma hakkını düzenler. Bu düzenlemede, bireylere, kişisel verileriyle ilgili her türlü bağlantı, kopya ve örneğin silinmesini talep etme hakkı verilmiştir. İlk fıkrada, kullanıcının verilerinin ne zaman silinmesi gerektiği belirtilmektedir. Eğer veriler, toplanma amacına uygun şekilde uzun bir süre boyunca kullanılmamışsa ve kullanıcı verilerin saklanmasına rıza göstermiyorsa, veri sorumlusu kullanıcının verilerini hemen silmek ve daha fazla yayılmasını engellemekle sorumludur. Ancak ifade özgürlüğü, kamu yararı, tarihsel, istatistiksel ve bilimsel amaçlar ile üye devletlerin hukuk sistemlerinin gerektirdiği durumlar gibi şartların varlığı durumunda, veri sorumlusu veriyi tutma ve saklama hakkına sahip olabilir. Bu şekilde, unutulma

[171] Tortop Nur. Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu, *Amme İdaresi Dergisi,* Y:2000, C:33, S:3, s.2.

[172] http://hudoc.echr.coe.int/sites/tur/Pages/search.aspx#{"fulltext":["Yıldırım"],"documentcollectionid2" E.T: 19.05.2023

hakkının kullanımıyla ifade özgürlüğü ve diğer kamu yararları arasında dengenin sağlanması hedeflenmektedir. [173]

Amerika bu konuda Kıta Avrupası düzenlemelerinden farklı düşünmektedir. ABD'de unutulma hakkı kavramı ile ifade özgürlüğünün kısıtlanacağı ve internetin sansürleneceği düşünülmektedir. Bazı eleştirmenler, unutulma hakkının internet üzerinde sansür mekanizmalarını tetikleyebileceğini ve ifade özgürlüğünü sınırlayabileceğini iddia etmektedir. Bu eleştiriler, unutulma hakkının uygulanmasının, kamuoyu tartışmaları ve bilgiye erişim gibi temel özgürlükleri olumsuz etkileyebileceği endişesini yansıtmaktadır.[174]Amerikan hukuku ifade ve basın özgürlüğü kavramlarını temel alarak değerlendirme yaparken, kıta Avrupası hukuku temele insan onuru, özel yaşamın gizliliği çerçevesinde değerlendirir.[175]

Bununla birlikte bir kitle iletişim aracı olarak internet önemli bir takım sorunların oluşması için potansiyel barındırmaktadır. İnternet üzerinde günümüzde kişilerle ilgili büyük miktarda veri toplanmaktadır. Bu verilerin kişilerin yaşamı üzerinde önemli etkileri olabilmektedir. Toplanan ve işlenen bu veriler kişilerin iş başvurularında, kredi değerlendirmelerinde değerlendirilmektedir. Mevcut bu durum ihlalerin oluşması riskini oldukça arttırmaktadır. Dolayısıyla birey hakkında birçok önemli karar bu verilere dayanılarak verildiğinden bu verilerin doğruluğunun, güvenilirliğinin sağlanması oldukça önemlidir.[176]

Kişisel sağlık verileri özelinde düşünüldüğünde unutulma hakkının bazı durumlarda gerekli olduğu görülür. Kişinin kendisince ya da üçüncü kişiler aracılığıyla internet üzerinden paylaşılan bir sağlık verisi, zamanla sosyal hayatını, iş hayatını etkileyecek bir durum oluşturabilir. Bu bağlamda KVKK ve GDPR maddelerini

[173] Soysal T. Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi. Uyuşmazlık Mahkemesi Dergisi 0, 2019, s. 339-422

[174] Karakaş, ME. "Dijital Geçmişin İnternet Erişiminden Kaldırılması "Unutulma Hakkı" ve Türk Hukukunda Görünümü", Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 2, 2020, 262-289

[175] Bennett SC. The Right to Be Forgotten: Reconciling EU and US Perspectives, Berkeley Journal of International Law, Volume 30, Isse 1, Article 4, s.173.

[176] Peschke L. The Web Never Forgets!: Aspects Of The Rıght To Be Forgotten. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 19, 2015, s. 151-160

karşılaştırdığımızda, GDPR bu hakkı detaylı bir şekilde düzenlerken, KVKK'da bu düzenlemenin olmadığı fakat uygulamada Yargıtay içtihadi ile bu açığı kapatmaya çalıştığı görülmektedir. Bu hakkın kanun hükmü ile koruma altına alınması gerekmektedir. Bu durum kişisel verilerinin korunması hakkı ve özel hayatın gizliliği hakkı ile de sıkı ilişki içerisindedir.

1.8. Arama Motorları ve Google

Günümüzde sıklıkla kullanılan arama motorları üzerinden unutulma hakkını değerlendirecek olursak; Bu motorlar, büyük veri kümelerinden bilginin elde edilmesi için pratik uygulamalardır. Google ve Yahoo gibi arama motorları, tarama yapmak suretiyle bu veriyi incelemekte ve hızlı biçimde yanıtlar vermektedir.[177]

Google, kullanıcıların arama ve internet kullanımıyla ilgili verileri toplamakta ve bu verileri kullanarak kişisel profiller oluşturma eğilimindedir. Bu durum, kişisel verilerin gizliliği ve korunması konusunda eleştirilere neden olmuştur. Özellikle Google'ın uzun süre verileri tutması ve kullanması, unutulma hakkıyla ilgili tartışmalara yol açmıştır. AB ülkelerindeki otorite kuruluşlarının unutulma hakkına yaklaşımlarına bakıldığında, genellikle kullanıcıların lehine kararlar verildiği görülmektedir. Bu kuruluşlar, Google'ın kişisel verileri uzun süre tutmasına karşı çıkmış ve bireylerin bu verilerin silinmesi hakkını desteklemiştir. Google, kişisel verileri toplama ve işleme amacının daha iyi hizmet sunmak olduğunu savunmaktadır. Ancak, bu açıklamalar bazı veri koruma otoriteleri tarafından yeterli bulunmamış ve Google'ın gizlilik politikalarının uygunluğu sorgulanmıştır. Daha önce bahsi geçen kararda CNIL, Google'ın gizlilik politikasının 95/46/AT sayılı Direktif'e uygun olmadığını belirtmiştir. Benzer şekilde, İspanya Kişisel Verilerin Korunması Otoritesi, Google aramasından kaynaklanan referansların silinmesi taleplerini kabul etmiştir. Bu da, kullanıcıların Google'dan bu tür referansların silinmesini talep etme hakkına sahip

[177]Peschke, s.151-160

olduklarını göstermektedir. Sonuç olarak, Google gibi büyük şirketlerin kişisel verilerin korunması konusundaki uygulamaları ve politikaları tartışmalara neden olmuştur. AB ülkeleri ve diğer kuruluşlar, unutulma hakkı ve kişisel verilerin korunması konusunda bireylerin lehine kararlar verme eğilimindedirler. Bu tartışmalar, kullanıcıların veri gizliliğini koruma ve şirketlerin daha şeffaf ve uyumlu politikalar izleme konusundaki bilincini artırmaktadır.[178]

Büyük sosyal paylaşım ağları, özellikle Facebook ve Google gibi platformlar, kullanıcılara geniş bir iletişim ve içerik paylaşım imkanı sunmaktadır. Bu platformlar sayesinde kullanıcılar, haberleri takip edebilir, arkadaşlarıyla iletişim kurabilir, fotoğraf ve videolar paylaşabilir, ilgi alanlarına göre içerikleri keşfedebilir ve daha birçok aktivite gerçekleştirebilirler. Ancak, bu hizmetlerin sunulmasının bir bedeli olduğu unutulmamalıdır. Sosyal medya platformları, kullanıcı verilerini toplar ve bu verileri çeşitli şekillerde kullanarak reklam hedeflemesi, kullanıcı davranışlarının analizi, içerik önerileri ve diğer ticari faaliyetlerde bulunurlar. Bu durum, kullanıcıların özel hayatlarının gizliliği ve veri güvenliği konusunda endişelerin ortaya çıkmasına neden olmuştur. Sonuç olarak, büyük sosyal paylaşım ağları bireylere özgürlük ve iletişim imkanı sunarken, kullanıcıların kişisel verilerinin nasıl işlendiği ve gizliliklerinin ne kadar korunduğu konularında dikkatli olmaları önemlidir.[179]

Google gibi büyük bir şirketin veri tabanı yapısı göz önüne alındığında, düzeltme veya silme hakkının tam anlamıyla uygulanmasının zor olduğu belirtilmektedir. Google, büyük miktarda veriyi depolama, aktarma ve yedekleme konusunda güçlü bir altyapıya sahiptir, bu nedenle verilerin tamamen silinmesi veya düzeltilmesi zor olabilir. Ancak, Avrupa Adalet Divanı kararı sonrasında Google, taleplerin toplanması için harekete geçmiş ve binlerce başvuru alındığı bildirilmiştir. 2014 Mayıs ayında başlayan bu uygulama kapsamında 145 bin talep alınmış ve bu taleplerle ilgili 498.737 URL adresinin silinmesi istenmiştir. Bu, kullanıcıların unutulma hakkını kullanmak için

[178] Zeybek ÜÇ. Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", Hacettepe Hukuk Fak. Dergisi, 3(1) 2013, s.99.

[179] Kulevska S. The Future of Your Past: A Right to be Forgotten Online?. https://lumendatabase.org/blog_entries/522 E.T:20.05.2023

Google'a başvurduğunu ve şirketin bu talepleri değerlendirdiğini göstermektedir. Google gibi büyük şirketlerin, kullanıcıların veri koruma haklarını uygulamak için teknik ve organizasyonel düzenlemeler yapması gerekmektedir. Veri tabanı yapıları ve işleyişleri göz önüne alınarak, taleplerin değerlendirilmesi ve verilerin silinmesi veya düzeltilmesi için uygun süreçlerin oluşturulması önemlidir. Bu şekilde, kullanıcıların haklarının korunması ve veri tabanlarının daha şeffaf ve kullanıcı odaklı bir şekilde yönetilmesi sağlanabilir.[180]

Unutulma hakkına yönelik yasal düzenlemeler Avrupa'da başlamıştır ve destekleyen kararlar mevcutsa da Türkiye'de henüz tam olarak kabul edilmemiştir. Google gibi arama motorlarının kişisel verileri kolayca ortaya çıkardığı ve AB Adalet Divanı'nın "Google Kararı"yla kişisel verilerin silinmesi gerekliliğini vurgulanmıştır.[181]

[180] https://www.ulusal.com.tr/haber/8441749/binlerce-avrupali-unutulmak-istiyor E.T:20.05.2023
[181]Akgül A. Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı'nın Google Kararı, TBB Dergisi 2016 (116) 2015, yıl:7 sayı:116, s.35

DOKUZUNCU BÖLÜM
KİŞİSEL VERİLERİN AKTARILMASI

1. KİŞİSEL VERİLERİN ÜÇÜNCÜ KİŞİLERE AKTARILMASI

Kişisel verilerin üçüncü kişilere aktarılmasında diğer işleme durumlarında olduğu gibi açık rıza ve hukuka uygunluk nedenleri aranacaktır. Burada verilerin aktarıldığı kişinin de, eğer veri işleme faaliyetinde bulunursa, veri sorumlusu sorumluluğu taşıyacağı açıktır.

Kişisel verilerin yurtdışına aktarılması açısından ilk gereklilik açık rızanın olmasıdır. Burada açık rıza alınmadan önceki bilgilendirme kısmı önemlidir ve bu bilgilendirme verinin hangi amaçla işleneceğinin ve hangi ülkelere aktarılacağı bilgisini içermelidir. Kişisel verilerin aktarılması noktasında hukuka uygunluk sebeplerinin varlığı(md. 5-6) yeterli değildir. Aynı zamanda verilerin aktarılacağı ülkelerde yeterli korumanın olması şartı aranmaktadır. Her ne kadar Kurul "Yeterli korumaya sahip ülkelerin belirlenmesinde esas alınacak kriterler" ile ilgili karar yayınlamış olsa da henüz güvenli ülkeler listesi yayınlanmamıştır.

Kurul'un bir ülkeyi güvenli ülke sınıfına alırken değerlendireceği kıstaslar KVKK md.9 da düzenlenmiştir. Bu değerlendirmede;

> "*Türkiye'nin taraf olduğu uluslararası sözleşmeler, Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumu, Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini, Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüd edilen önlemleri, değerlendirmek ve ihtiyaç duyulması halinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir*"[182]

[182] Çekin, s.116

Yeterli korumanın bulunmadığı ülkelerde veri aktarımı yapılacaksa, hem Türkiye'deki hem de karşı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri gerekmektedir. Bu durumda açık rıza aranmaksızın aktarım yapılabilecektir. Fakat burada yazılı taahhüt olsa bile kurulun onayı gerekecektir.(md.9)

AB hukukunda farklı bir yaklaşım olarak komisyon kararı olarak önceden hazırlanan ve komisyon kararı olarak yayınlanan düzenlemelerde herhangi bir değişiklik yapılmadıkça kurulun onayına gerek olmadan aktarılabilecektir.

2. KİŞİSEL VERİLERİN YURTDIŞINA AKTARIMI

Kişiler verilerin yurtdışına aktarılması, genel olarak veri aktarımının ülke sınırları ötesine iletilmesi anlamında kullanılır. KVKK md.3 f/1-e bendi kapsamında kişisel verilerin işlenmesi başlığı altında tanımlanan işlemlerdendir.

Kişisel verilerin yurtdışına aktarılması, hem kişilik hak ihlallerinin oluşmasına sebebiyet verebilmesi hem de ulusal güvenlik endişeleri açısından, tüm ülkelerin üzerinde dikkatle durdukları bir alandır.[183] Aktarım sonrasındaki veri üzerindeki hakimiyet kaybı ciddi bir risk oluşturmaktadır. Verinin iletildiği ülkenin hukuki rejiminin farklı olması, hakların talebi için gerekli olan masraflar açısından, para birimlerinin farklı olması ve uluslararası ölçekteki işlemlere has bürokratik zaman kayıpları diğer olumsuzluklardır.

Kişisel verilerin korunması amacıyla kişisel veri aktarımının tamamen kısıtlanması ya da çok zorlaştırılması, özellikle uluslararası çalışan şirketlerin ticari olarak ciddi zararlara uğramasına yol açabilir. Burada veri sorumlusunun menfaatleri ile iligili kişinin kişisel verileri üzerindeki hakimiyet yetkisinin dengelenmesi sağlanmalıdır.[184]

[183] Akçalı GB. Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 25, 2019, s.850-872

[184] Arslan Ç. Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması, *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 9, Sayı: 1, Ocak 2010, Sayfa: 447-487

Bu durum, verinin yurtdışına çıkarılmasıyla ortaya çıkabilecek hak ihlallerini önleyebilmek aynı zamanda kişisel verilerin korunması kurulunun ülke sınırları içerisindeki yetkileri dahilinde verileri tutabilmesi ve kontrollü aktarılmaya izin vermesi açısından önemlidir.

Verilerin yurtdışına aktarılması konusunda ülkeler arasında mevzuatsal farklılıklar bulunmaktadır. Kimi ülkeler tüm veriyi sıkı bir şekilde ülke içerisinde tutmaya çalışırken, bazı ülkeler bu verinin belirli koşullar ve ikili anlaşmalar çerçevesinde aktarılmasına izin vermektedir. Özellikle ticari ilişkilerin korunması bağlamında AB ülkeleri nezdinde uygulanan mevzuatın uyumlu hale getirilmesine yönelik çalışmalar dikkat çekmektedir. Verilerin ülkeler örneğinde belirli bölgelerde saklanması, kısmen ya da tamamen sınırlandırılmasına yönelik yapılan düzenlemelere veri lokalizasyonu(Data lokalizasyonu) denilmektedir. Bu durum her ülke özelinde farklı gerekçelerle yapılabilmektedir.(siber güvenlik, kamu düzeni vs.)[185]

Kişisel Verileri Koruma Kurumunun 26.10.2020 tarihli 'Yurtdışına Veri Aktarımı Kamuoyu Duyurusu' ile Bankacılık kanunu md.73 uyarınca yurtdışına veri aktarımlarının KVKK md.9 f.1 çerçevesinde açık rıza ile yapılacağı belirtilmiştir.

Türk hukukunda yurtdışına veri aktarımı konusunda bazı katı sınırlandırmalar mevcuttur. Bazı durumlarda ise koşullu sınırlandırmalar mevcuttur. Özellikle verisi aktarılacak kişinin açık rızasının alınması önemlidir.[186]

KVKK bağlamında yurtdışına veri aktarımı kavramı tanımlanmamıştır. Sadece koşulların neler olduğu belirtilmekle yetinilmiştir. Bu durum yurt dışına veri aktarımı

[185] Svantesson D. Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers,* No. 301, OECD Publishing,2020, Paris, https://doi.org/10.1787/7fbaed62-en

[186] Asikoglu İ, Uzun FB. Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri (Problems Caused by Basing Cross-Border Data Transfers to Explicit Consent and Solution Suggestions) (August 31, 2020). Prof. Dr. Türkan Rado'nun Anısına Armağan, 2020, Available at SSRN: https://ssrn.com/abstract=3683903 E.T:19.05.2023

kavramının hangi kişiler arası veri aktarımını kapsadığı probleminin net bir cevabı olmamasına neden olabilmektedir.

Veri aktarımının ülke sınırını aşması durumu KVKK m.9 çerçevesinde değerlendirilmektedir. Verilerin tutulduğu sunucuların yurtdışında olması durumu da aynı şekilde değerlendirilmektedir. Kurulun 2019/157 sayılı 31.05.2019 tarihli kararında gmail e-posta hizmetine bağlı sunucuların farklı ülkelerde farklı veri merkezlerinde tutulması durumu da kişisel verileri yurtdışına aktarılması çerçevesinde KVKK m.9 kapsamına girmektedir.[187]

Bulut hizmetlerinin kullanımı da kişisel verilerin yurtdışına aktarılması bakımından özellik arz etmektedir. Depolama, kullanım, uygulama gibi bir takım hizmetleri ortak bir havuzda sağlayan bu uygulamalarda, kişisel verilerin bulunduğu yer ile saklandığı yerin birbirinden faklı olması söz konusudur.[188]

Kişisel verileri koruma Kurumu bulut hizmet sunumu sağlayan ve sunucuları yurtdışında bulunan şirketlerin yurtdışı veri aktarımı yaptığını kabul etmektedir. Hatta bu şirketlerin verilere erişim yetkisi olmasa bile bu durum geçerlidir. Bu nedenle bu durumlarda bu şirketlerin veri merkezlerinin ve sunucularının nerede bulunduğu konusunda KVKK'daki yükümlülüklere uyulması önem arz etmektedir.[189]

2.1. Yeterli Korumanın Bulunması ve Uygun Koruyucu Önlemlerin Alınması Durumunda Kişisel Verilerin Yurtdışına Aktarılması

KVKK m.9 f/2-a kapsamında kişisel verilerin aktarılacağı yerlerde yeterli koruma seviyesinin sağlanmasına ilişkin yetkili makam kararının bulunması halinde yurtdışına veri aktarımı sağlanabilir. GDPR m.45 f/1 kapsamında ise üçüncü ülkelere ya da

[187] Çelik I. Kişisel Verilerin Yurt Dışına Aktarılması. Oniki Levha Yayınları, 1. Baskı, İstanbul, 2022, s.70
[188] Dülger, s.334
[189] Kişisel verilerin koruma kurumu, doğru bilinen yanlışlar-2 s.34 https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2 E.T:19.05.2023

uluslararası kuruluşlara veri aktarımı gerçekleştirilebilir. Eğer geçerli bir yeterlilik kararı yoksa ilgili mevzuat içerisinde istenen uygun koruyucu önlemlerin alınması sonrası veri aktarımı yapılabilir.

KVKK kapsamında yeterli koruma taahhüdü ve bağlayıcı şirket kurallarına istinaden yurt dışına veri aktarımı yapılabilirken, GDPR bakımından ise 'Kamu idareleri ve organları arasındaki düzenlemeler, standart sözleşme maddeleri, bağlayıcı şirket kuralları, onaylı davranış kuralları, onaylı belgelendirme mekanizmaları veya adhoc niteliğindeki özel sözleşme maddeleri' kapsamında birtakım koruyucu önlemler alınabilmektedir.

GDPR md.44'de KVKK'dan farklı olarak veri aktarımının ancak bir veri işleyen tarafından gerçekleştirilebileceği düzenlenmiştir. Ancak bu şekilde bir veri işleyen, uluslararası bir kuruluşa ya da 3. ülkelerde bulunan bir veri sorumlusuna aktarımda bulunduğu zaman uluslararası kuruluşlara veri aktarılmış sayılacaktır.[190]

KVKK bağlamında md.5 ve md.6 da belirtilen işleme şartları gerçekleştiğinde, verilerin aktarılacağı ülkelerde yeterli korumanın bulunması durumunda, ilgili kişiden açık rıza alınmasına gerek olmaksızın yurt dışına veri aktarımı gerçekleşebilir. Bu şekilde koşulları sağlandığında veri aktarımı çok hızlı bir şekilde gerçekleştirilebilir. KVKK md.9 a göre kurul, yeterli korumanın bulunduğu ülkeleri belirler ve ilan eder. Bu değerlendirmede bazı kriterler düzenlenmiştir. Buna göre; Türkiye'nin taraf olduğu ülkeler, veri aktarımı yapılacak ülkeler ile karşılıklılık durumu, aktarılacak kişisel verinin niteliği, amacı ve süresi, aktarımı yapılacak olan ülkenin bu konudaki mevzuatı, aktarım yapılacak ülkedeki veri sorumlusunun önlem konusundaki taahhütleri, gereklilik halinde ilgili kurum ve kuruluştan alınan görüş vb. durumlar dikkate alınarak düzenleme yapılır.

Kişisel verileri koruma kurulu henüz bu ülkelerin listesini açıklamamıştır. Bu listenin açıklanması, kişisel verilerin yurt dışına aktarılması hususunda, hızlı uygulanabilir,

[190] European Data Protection Board Guidelines, https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en E.T:19.05.2023

daha maliyetsiz bir yolu kullanıma açacaktır. Listenin açıklanmasındaki gecikmenin olası bir nedeni de yeterli korumanın bulunması konusunda aranan 'karşılıklılık' ilkesidir. Diplomatik ilişkileri ilgilendiren bu durumun, kurulun yeterli korumanın bulunduğu ülkeleri belirlerken zorluk çıkarabileceği anlaşılabilir bir durumdur.[191] Yeterli korumanın bulunduğu ülkeler listesinin belirlenmesi durumunda da bu listenin süresiz olarak geçerli olması durumu söz konusu olmayacaktır. Çünkü değerlendirmede göz önüne alınacak kriterler dinamik bir yapı içerdiğinden değişime açıktır. Bu nedenle kurul bu durumu göz önünde bulunduracak, gerektiğinde tadil edecek, askıya alabilecek ve ilga edebilecektir.

KVKK md.9 çerçevesinde veri aktarımı yapılacak olan ülkenin bu konudaki mevzuatı ve uygulamasının yeterli korumanın sağlanması hususunda değerlendirilmesi belirtilmiştir. Bu değerlendirmede; kişisel verilerin korunmasının anayasal bir hak olarak kabul edilmiş olmasını, kişisel verilerin korunması kanununun bulunmasını ve buna ek olarak ikincil düzenlemelerin yapılmış olmasını, aynı zamanda bu düzenlemelerin Türk mevzuatına uygun olmasını ve uygulamaya yönelik rehberlerin bulunmasını dikkate alacaktır. Aktarım yapılacak ülkenin mevzuatı değerlendirilirken KVKK ile uyumu, işleme faaliyetinin şeffaflık ilkesi çerçevesinde yapılıp yapılmadığı ve buna yönelik hukuki teminatın olup olmadığı, güvenliği sağlamaya yönelik idari ve teknik tedbirlerin alınması hususu değerlendirilmelidir.

KVKK ve mevzuatımızdaki ikincil düzenlemelerin hazırlanmasında yararlanılan ve uzun süredir uygulamada bulunan ve yerleşmiş olan AB mevzuatına istinaden AB'ye üye olan devletler için yeterlilik kararının verilebileceğine yönelik görüş bulunmaktadır.

Her ne kadar KVKK md.9 da bağımsız veri koruma otoritesinin bulunması kriterinden bahsedilmese de kurum tarafından bağımsız veri koruma otoritesinin bulunması, oluşturulacak otoritenin yapısı, hangi görev ve yetkilere sahip olacağı, denetim yetkisi

[191] Çelik, s.84

ve kararlarına karşı başvuru olanağı gibi bir takım unsurlar açısından değerlendirilmesi gereği belirtilmiştir.[192]

Yeterli korumanın varlığı açısından KVKK'daki koşullar sağlanmadığı durumlarda, karşılıklı olarak veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve kurulun iznini almaları şartıyla, ilgili yer alması gereken asgari unsurlar kurum tarafından belirtilmiş ve web sayfasında her iki tarafa aktarım için ayrı taahhütname şablonları oluşturulmuştur.[193]

KVKK'dan farklı olarak GDPR'da Avrupa komisyonu tarafından onaylanan standart sözleşme maddeleri kullanılacak olursa, denetim makamının iznine ihtiyaç duyulmamaktadır. Buna benzer şekilde KVKK uygulamalarının düzenlenmesinin özellikle de kurum onayının belirli bir süre ile sınırlanmadığı düşünüldüğünde, süreci hızlandırabilecektir.[194]

Kişisel Verileri Koruma Kurumu 10 Nisan 2020 tarihinde "*Bağlayıcı Şirket kuralları Hakkında Duyuru*" yayınlamıştır. Bu durum yurtdışına veri aktarımının başka bir yoludur. Bu duyuruda "*Yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için verilerin yurtdışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri politikaları*" olarak tanımlanan bu kuralların taahhütname yoluna kıyasla çok uluslu grup şirketleri için daha kolay bir çözüm olduğu belirtilmiştir. GDPR md.47 de "binding corporate rules" olarak düzenlenen bu durum KVKK'da ayrıca düzenlenmemiştir. Yukarıda adı geçen duyuruda bağlayıcı şirket kuralları başvurularının KVKK md.9 f/2-b uyarınca kurulun izinini gerektirmesi, taahhütnamelerin özel bir türü olarak kabul edildiğini göstermektedir. Duyuru ile birlikte Veri sorumluları için bağlayıcı şirket kurallarında bulunması gereken temel hususlara ilişkin yardımcı doküman ve başvuru formu da yayınlanmıştır. Buna göre; "*Şirketler topluluğuna bağlı Türkiye'de faaliyet gösteren veri sorumlusundan, grup üyesi olarak yurtdışında bir veya daha fazla ülkede faaliyet*

[192] Kişisel verileri koruma kurumu, esas alınacak kriterler
[193] Kişisel verileri koruma kurumu taahhütnameler https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler E.T:19.05.2023
[194] Çelik, s.93

gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan ve veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularına" aktarım yaparken bağlayıcı şirket kuralları(BŞK) kullanılabilir.

BŞK'ya dayalı olarak başvuru usulünde başvuru taslağının hazırlanması ve kurulun onayının alınması gereklidir. Bu kapsamda "Çok uluslu grup şirketinin Türkiye'deki yerleşik merkezi olan grup üyesi' veya "*Türkiye'de yerleşik merkezin bulunmaması halinde grup şirketi adına başvuru yapmak üzere yetkilendirilen Türkiye'de yerleşik bir grup üyesi*" tarafından başvuru yapılmalıdır.

Başvuru sonrası kurul 1 yıl içerisinde kararını verecektir. Bu süre ihtiyaç halinde 6 aylık süreler şekline uzatılabilecektir. Burada kesinliğin olmaması uygulamanın etkinliğini azaltmaktadır. BŞK'nın kurul tarafından onayından sonra geçerliliği konusunda belirli bir süre tanınmamışsa da kurallara uyulmaması durumunda askıya alınması veya feshedilmesi söz konusu olabilecektir. Bir ihlal söz konusu olursa, oluşan zarar grubun Türkiye'de yerleşik merkezi ya da yetki verilmiş olan Türkiye'de yerleşimi bulunan grup üyesi tarafından giderilmelidir. Bunu düzenleyen BŞK metnine göre;

- *Sorumluluğu üstenen grup üyesi BŞK ya aykırı davranışların sonlandırılmasına çalışacaktır.*
- *Oluşan maddi ve manevi zararı tazmin edecektir.*
- *Yargılama yetkisinin Türk mahkemelerinde ve yetkili makamlarda olduğunu kabul edecektir.*
- *Sorumluluğu üstlenen grup üyesinin, oluşan zararın yurtdışında yerleşik grup üyesi tarafından*

gerçekleştirilmediğinin ispat yükünün kendinde olduğunu kabul edecektir.

ONUNCU BÖLÜM
KİŞİSEL VERİ KORUMA KANUNU VE ULUSLARARASI VERİ KORUMA KANUNU KARŞILAŞTIRILMASI

1. KVKK VE GDPR UYGULAMA ALANI KARŞILAŞTIRMASI

KVKK Md. 2 de belirtildiği üzere, kişisel veri kavramı, sadece gerçek kişiler için kabul edilmektedir. Veri sorumlusu ve veri işleyen bakımından değerlendirildiğinde ise bu kişiler, gerçek ve tüzel kişiler olabilir.

Konu bakımından uygulama alanı ise Md.2 de "tamamen ve kısmen otomatik olan sistemlerle' ya da 'herhangi bir veri sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler" denilmek suretiyle açıklanmıştır. Otomatik sistemlerden kasıt, bilişim sistemleri üzerinden, insan müdahalesi olmadan yapılan veri işleme faaliyetleridir.[195]

KVKK md.28 f/2 de bu hükümlerin uygulamasını sınırlandıran bazı hükümler vardır. Buna göre tamamen ilgili kişiye ait veya aynı konutta yaşayan aile fertlerine ait faaliyetler kapsamında bir veri işleme söz konusuysa bu verilerin 3. Kişilerle paylaşılmaması ve diğer yükümlülüklere uyulması kaydıyla KVKK hükümleri uygulanmayacaktır.[196]

Yer açısından uygulamada KVKK da açıklık yoktur. Bu nedenle kural olarak ülkemiz hukukunun geçerli olduğu yerlerde uygulanacaktır. Kişisel Verileri Koruma Kurulu'nun 23.06.2020 tarihli ve 2020/471 sayılı kurul kararı yorumlama ve işleyişi değerlendirme açısından önemlidir. Buna göre Türkiye'de temsilciliği bulunan ve veri işleme faaliyeti gerçekleştiren işletmeye KVKK hükümlerinin uygulanmaması,

[195] KVKK temel kavramlar s.20 https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun%27da-Yer-Alan-Temel-Kavramlar E.T19.05.2023
[196] Çelik, s.22

mevzuatın amacına ters düşmektedir Anayasa kapsamında kişisel verilerin korunması temel hak ve hürriyetlerdendir. Bu nedenle uygulama alanı belirlenirken en üst düzeyde ve kapsamda belirlenmesi gerektiği belirtilmiştir.[197]

KVKK, Türk Hukukunun uygulandığı her yerde uygulanabilir. AB'ye üye ülke vatandaşlarının verilerini işleyen tüm işletmeler GDPR kapsamındadır AB sınırları içerisinde yaşayan kişilere ait verileri işleyen şirketler de GDPR'a bağlıdır.

2. SAĞLIK ALANINDA YAPAY ZEKA KULLANIMI VE KİŞİSEL SAĞLIK VERİSİ İŞLEME

Kişisel sağlık verilerinin anonimleştirilmesinin amacı, bu verilerin bireylerin kimliklerinin tespit edilemeyecek şekilde gizli tutulmasını sağlamaktır. Anonimleştirme işlemi ile; veriler, bireyleri doğrudan veya dolaylı olarak tanımlayamayacak hale getirilir, gizlilik ve güvenlik sağlanır. Bu şekilde, kişisel sağlık verilerinin işlenmesi sırasında gizlilik ihlalleri, veri sızıntıları veya kötü niyetli kullanımların önlenmesine yardımcı olur.

KVKK anonimleştirme konusunda esnek bir yaklaşım sergiler. KVKK, kişisel verilerin belirli veya belirlenebilir gerçek kişilerle ilişkilendirilemeyecek hale getirilmesini kabul eder. Bu durumda, verilerin yeniden tanımlanma riski olsa bile, anonimleştirme işlemi yeterli kabul edilebilir. KVKK, anonimleştirme için geriye dönüşü olmayan bir durumu zorunlu tutmaz.

GDPR ise anonimleştirme konusunda daha katı bir yaklaşım benimser. GDPR, anonimleştirmenin, kişisel verilerin tamamen tanımlanamaz hale getirilmesini gerektirdiğini belirtir. Anonimleştirilmiş verilerin yeniden bağlantı kurulamaması ve bireylerin geriye dönük olarak tanımlanamaması gerekmektedir.

[197] Çelik, s.23.

Her iki düzenleme de kişisel verilerin korunmasına odaklanır ve anonimleştirme yöntemlerinin kullanılmasını teşvik eder. Ancak KVKK, anonimleştirme konusunda daha esnek bir yaklaşım sergilerken, GDPR daha katı bir yaklaşım benimser ve anonimleştirme için daha yüksek bir eşik koymaktadır. Bu farklılıklar, kişisel sağlık verilerinin anonimleştirilmesi konusunda farklı uygulamaların ve standartların oluşmasına neden olabilir.

Sonuç olarak, kişisel sağlık verilerinin kullanıldığı tüm alanlarda KVKK, GDPR ile kıyaslandığında özellikle verinin kimliksizleştirme işleminden sonra, yeniden kişisel veri oluşturulabilmesi açısından daha açık alanlar barındırır. Bu konunun KVKK içerisinde daha da detaylandırılması ve kişisel sağlık verileri gibi özel nitelikli veri alanlarında daha sıkı kontroller alınması, veri güvenliğini arttırabilir.

3. KİŞİSEL SAĞLIK VERİSİNİN YURT İÇİ VE YURTDIŞI AKTARIMI

KVKK ve GDPR düzenlemeleri, kişisel sağlık verilerinin yurtdışına aktarımı konusunda bazı farklılıklara sahiptir.

GDPR, kişisel sağlık verilerinin yurtdışına aktarımı için farklı hukuki dayanaklar sunar. Bunlar arasında AK tarafından onaylanmış bir üçüncü ülke bulunması, standart sözleşme şartlarının kullanılması, Bağlayıcı şirket Kuralları uygulanması ve veri sahibinin açık rızası sayılabilir. KVKK ise veri transferi için ilgili kişinin açık rızasını gerektirir.

GDPR, üçüncü ülkelere (AB dışındaki ülkeler) kişisel sağlık verilerinin aktarılmasını kısıtlar ve ilave koruma önlemleri talep eder. Bu önlemler, üçüncü ülkenin veri koruma düzenlemelerinin uygunluğunu değerlendirmeyi, sözleşme şartlarının kullanımını veya yetkilendirilmiş bir düzenleyici kurumun varlığını içerebilir. KVKK ise, veri aktarımı konusunda ‘Yeterli korumanın sağlandığı ülkeler’ kavramını oluşturmuştur. Fakat bu ülkelerin listesi henüz belirlenmemiştir.

GDPR, veri aktarımı için kuruluş içi kuralları (BCR) kullanmayı önerir. BCR, bir veri kontrolörünün veya veri işleyicinin yurtdışındaki grup şirketleri arasında veri aktarımı için benimsenen iç kuralları ifade eder. KVKK ise, bu konuda belirli bir düzenleme içermemektedir.

GDPR, üçüncü ülkelere kişisel sağlık verilerinin aktarımında, veri koruması düzeyini sağlamak amacıyla yetkilendirilmiş kuruluşlar tarafından sertifikaların kullanılmasını önerir. KVKK ise, bu konuda belirli bir düzenleme içermemektedir.

4. KİŞİSEL SAĞLIK VERİSİNDE UNUTULMA HAKKI

Unutulma hakkı hem GDPR hem de KVKK'nın önemli bir unsuru olarak karşımıza çıkar. Unutulma hakkı temelde kişisel verilerin silinmesi veya yok edilmesini talep etme hakkını ifade eder. Verisi işlenen kişi, belirli durumlarda, bu verileri işleyen veri sorumlusuna başvurarak bu hakkını kullanabilir. Unutulma hakkı, kişinin daha önce vermiş olduğu rızasını geri çekmesi durumunda devreye girebilir.

GDPR, unutulma hakkının belirli koşullarda uygulanacağını kabul eder. Örneğin, veri işleyenin kişisel verileri işlemesi için gerekli olan amaç artık ortadan kalktıysa, hukuki bir zorunluluk da bulunmuyorsa veya kişinin rızası yoksa, bu verilerin silinmesi gerekmektedir. Bu durumda veri sorumlusu, kişisel verileri silme talebini yerine getirmekle yükümlüdür.

Ancak unutulma hakkı, bazı istisnalar ve sınırlamalarla da karşılaşabilir. Örneğin, ifade özgürlüğü ve bilgi edinme hakkı gibi temel haklar, kamu sağlığı, hukuki savunma gibi nedenlerle unutulma hakkı kapsamında istisnalar uygulanabilir.

GDPR, unutulma hakkının etkin bir şekilde uygulanmasını sağlamak için veri sorumlularının gerekli önlemleri almasını ve süreçleri düzenlemesini talep eder. Veri sorumlusu, kişisel verilerin silinmesini, yayılmasını veya kamuoyuna duyurulmasını gerektiren durumlarla ilgili bir politika veya prosedür geliştirmeli ve bu talepleri etkin bir şekilde yönetmelidir.

GDPR, bu hakkı “unutulma hakkı” olarak tanımlar ve kişinin rızası geri çekildiğinde veya veri işlemenin amacı ortadan kalktığında uygulanabilir. KVKK ise unutulma hakkını “silme veya yok etme” hakkı olarak tanımlar.

GDPR’da unutulma hakkının denetimi ve uygulanması için AB ülkelerinde bağımsız veri koruma otoriteleri bulunur. KVKK’da ise Kişisel Verileri Koruma Kurumu bulunur. Örneğin, ifade özgürlüğü, araştırma ve istatistik gibi amaçlarla işlenen verilerde unutulma hakkı sınırlanabilir. Ayrıca, KVKK’da belirtilen diğer hukuki nedenler veya kanuni yükümlülükler de unutulma hakkının uygulanmasını etkileyebilir. Kurum unutulma hakkının denetiminden ve uygulanmasından sorumludur.

Sonuç olarak GDPR ve KVKK unutulma hakkını kişisel sağlık verileri üzerinden de değerlendirir ve bireylere kişisel verilerinin belirli koşullar altında silinmesini talep etme hakkı tanır. Bu hakkın uygulanması, KVKK tarafından yetkilendirilen kişisel verileri koruma otoritesi olan Kişisel Verileri Koruma Kurumu (KVKK) tarafından denetlenebilir ve gerektiğinde cezai yaptırımlar uygulanabilir.

GDPR’da unutulma hakkının denetimi ve uygulanması için AB ülkelerinde bağımsız veri koruma otoriteleri bulunur. KVKK’da ise Kişisel Verileri Koruma Kurumu, unutulma hakkının denetiminden ve uygulanmasından sorumludur.

SONUÇ

Dijitalleşen dünya ile birlikte sağlık sisteminin de hızlı bir şekilde dijitalleştiğini görmekteyiz. Bu durum tetkik ve tedavi süreçlerinin değişmesi, bürokrasinin yavaş işleyen bazı alanlarının hızlanması, kullanılan kağıt sarfiyatının azalması, verilerin korunması için arşiv ve fiziki dosyalama işlemlerinin azaltılması gibi birtakım faydalar sağlamaktadır. Ancak bu durum aynı zamanda kişisel sağlık verileri gibi nitelikli verilerin üçüncü kişilere ulaşabilmesi, belki daha da tehlikelisi, kısa sürelerde çok uzak ülkelere taşınabilmesi ve bunun neticesinde hukuk sisteminin bu alanlarda etkisiz kalabilmesi ya da hak ihlali yapan kişi veya kişilere ulaşılamaması risklerini taşımaktadır. Bu nedenle bizim ülkemizde olduğu gibi bir çok ülkede de, sürekli gelişen bilişim sistemlerine ayak uydurabilmek ve hak ihlallerini azaltabilmek için günden güne yeni mevzuat düzenlemeler yapılmaktadır.

Ülkemizde 6698 sayılı Kişisel Verileri Koruma Kanunu yürürlüktedir. Bahsedilen kanun 95/46 sayılı direktif temel alınarak düzenlenmiştir. GDPR bu direktifi yürürlükten kaldıran düzenlemedir ve Avrupa Birliği ülkelerinde geçerli olan temel veri koruma düzenlemesidir. Oldukça detaylı düzenlenmiş olan bu metin, diğer bir çok ülkede olduğu gibi ülkemiz mevzuatıyla da benzerlikler içerir. Her ülkenin veri koruma düzenlemesinde bölgesel, kültürel bir takım farklılıklar mevcuttur. Birçok ülkede, gerek mevcut ticari ilişkileri korumak, ülkeler arası hizmetlerin aksatılmadan sürdürülebilmesini sağlamak, gerekse nitelikli ve hassas verilerin korunabilmesi ve bu açıdan olası hak ihlallerinin engellenmesi amacıyla tarafları koruyucu düzenlemeler yapılmaktadır.

Kişisel sağlık verileri ise daha sıkı düzenlemelerin gerekli olduğu, hak ihlallerinin daha yıkıcı sonuçlara yol açabileceği bir alandır. Bu önem nedeniyle her ülke bu verileri özel nitelikli veri/Hassas veri olarak kabul etmiş ve bu verilerle ilgili tüm işleme faaliyetlerini bir takım özel koşullara bağlamıştır. Bu verileri koruma altına alırken bir takım dengelerin korunması gerekliliği de aşikardır. Bunlardan ilki kişisel sağlık verilerinin korunması koşulunu sağlarken diğer taraftan çıkarılan düzenleyici işlemlerin yapay zeka destekli bilimsel gelişmeyi engellememesini sağlamaktır. Son

yıllarda özellikle büyük sağlık verisi üzerinden yapılan çalışmalarla sağlanan bilgiler hastalıkların tanı ve tedavisinde tarihte hiç olmadığı kadar hızlı bir ivmelenme sağlamıştır. Bilimsel gelişmenin bu kısmı özellikle çok büyük sağlık veri setlerine ihtiyaç duymaktadır. Kişileri hak ihlallerine maruz bırakmadan bu sürecin başarıyla sürdürülebilmesi için verinin kimlik tespitine olanak vermeyecek şekilde anonimleştirilmesi gerekmektedir. Bu süreç özellikle bilişim teknolojilerinin günden güne ve olağanüstü süratle arttığı günümüz koşullarında birçok zorluk barındırmaktadır. Yapay zeka teknolojileri ile, anonimleştirilmiş verinin bir takım verilerle karşılaştırılarak ve birleştirilerek yeniden kimliği belli ya da belirlenebilir veri haline getirebilmesi bazı durumlarda mümkün olabilmektedir. Bu durum verisi işlenen kişiler için bir diğer endişe kaynağıdır. Bu ve benzeri zorluklar nedeniyle oluşturulacak mevzuat düzenlemelerinin bir takım teknik içeriklere sahip olması gerekir.

Yapay zeka teknolojilerinin, kişisel sağlık verileri, özellikle büyük sağlık verisi ile kullanımı, önceden öngörülemeyecek bir takım, çıkarıma dayalı verilerin üretilmesi sebebiyle kişisel verilerin işlenme ilkeleri ile çatışma durumu yaratabilir. Fakat bu durum mutlak bir çatışma olarak değerlendirilmemeli, somut olay özelinde değerlendirilmelidir. Özellikle GDPR ve KVKK yi bu durum açısından değerlendirdiğimizde her iki hukuk sisteminin de bu tür hassas verileri bir koruma kalkanı altında tuttukları görülmektedir. Bir çok ülkenin de mevzuatını özellikle GDPR temel yapısına benzer şekilde yapmaya çalıştıkları görülmektedir. Bunun temel nedeni GDPR'ın oldukça detaylı olması ve uygulama pratiği ile sürekli geliştirilmesidir. Yapay zeka teknolojilerinin hızlı ve tahmin edilemez düzeyi bu mevzuat düzenlemelerini, hak ihlalleri bakış açısıyla sürekli değişime zorlamaktadır. Mevzuatsal düzenlemelerin gerek ülkemizde gerek GDPR ülkelerinde, gerekse de diğer birçok ülkede bu tür nitelikli verileri koruma açısından yeterli içeriğe sahip oldukları görülmektedir. Ülkemiz özelinde değerlendirirsek düzenlemelerin -elbette süreç içerisinde değişme ihtiyacı olmakla birlikte, içerik olarak mevcut aşamada yeterli olduğu, fakat esas görevin uygulamadaki etkinlik olduğu ve bu durumun da Kişisel Verileri Koruma Kurumuna büyük bir sorumluluk yüklediği görülmektedir.

Bilişim teknolojileri aracılığıyla kişisel sağlık verilerinin dünyanın herhangi bir yerine aktarılabilme konusu bir başka endişe konusudur. Böylelikle kişilerin kendi verileri üzerinde denetim yetkisini kaybetmesi, açıklandığı takdirde kişinin ayrımcılığa itilebileceği, dışlanacağı bir takım sağlık verilerinin üçüncü kişilerin eline geçme ihtimali, bazı kişileri sağlık hizmetinden yararlanmaktan bile vazgeçirebilecek olumsuz durumlara yol açabilecektir. Bu bağlamda sadece bir ülkenin bu önlemleri alması yeterli korumayı sağlayamayacak, kişisel sağlık verilerinin güvenliği sağlanamayacaktır. Buna çözüm olarak KVKK'da belirtilen yeterli korumaya sahip ülkeler kavramı henüz bu kavramın içeriği tam olarak doldurulmadığından ve yeterli korumaya sahip ülkeler listesi kurum tarafından açıklanmadığından henüz eksikliklerle doludur. Bu eksikliğini ivedi bir şekilde çözülerek, yeterli korumaya sahip ülkeler listesi açıklanmalıdır. Böylelikle istenen koşulların listesi de belirlenmiş olacağından, sürecin işleyişini daha hızlı ve verimli bir zemine oturması sağlanmış olacaktır.

Uluslararası düzeyde korumanın sağlanması, ülkelerin ortak ve makul koşulları yaratması ve veri güvenliği için gerekli düzenlemeleri, kurumları ve denetleme mekanizmalarını yetkinleştirmeleri ile mümkün olabilecektir. Tek tek ülkelerin yapacağı düzenleyici çalışmalar fayda sağlasa da esas etki bu çerçevede benzer düzenlemeler yapan devletlerin sayısı arttıkça ortaya çıkacaktır. Bu düşünceye paralel olarak detaylı bir şekilde düzenlenmiş GDPR düzenlemelerinin bir çok ülke tarafından temel alınarak, düzenlemelerin bu şekle uygun olarak yapılıyor olması bu anlamda güvenliğin sağlanması konusunda ümit vermektedir.

Kişisel sağlık verilerin işlenmesi ve aktarılması konusunda son zamanlarda gittikçe artan şekilde üzerinde durulan bir diğer husus da unutulma hakkıdır. Kişilerin kendi istekleri doğrultusunda paylaştıkları ya da herhangi bir şekilde üçüncü kişilere ulaşan kişisel sağlık verileri unutulma hakkı çerçevesinde değerlendirilmelidir. Kişilerin geleceğini, yaşayışını, sosyalleşmesini, meslek hayatını etkileyebilecek bu tür nitelikli verileri, özellikle kişiler tarafından talep edildiğinde, sosyal ağlardan belli bölgelerde ya da mümkünse tüm dünyada ortadan kaldırılabilmelidir. Nitekim bu hakkı destekleyecek mahkeme kararları da mevcuttur. Bu konu, özellikle sosyal ağların

kullanımının giderek arttığı düşünüldüğünde gelecekte daha sıklıkla yüzleşmek durumunda kalabileceğimiz bir sürece evrilmektedir. Bu anlamda kişisel sağlık verilerinin işlenmesi ve aktarılması konusu ‘unutulma hakkı’ bağlamında tartışılması gereken bir konudur. Bilişim sisteminde paylaşılan verinin kopyalanma yoluyla farklı mecralarda paylaşılabilir olması, temelde unutulma hakkının %100 uygulanmasını imkansız kılmaktadır. Fakat burada uygulanması gereken konu, verisi işlenen kişi için sağlanabilecek maksimum korumanın sağlanmasıdır.

Sonuç olarak kişisel verilerin korunması kavramı bilişim teknolojileri ile iç içe geçmiştir. Kişisel sağlık verileri gibi daha hassas korumanın gerektiği bir alanda çalışan kişilerin bu alandaki veri işleme faaliyetlerinin temel düzeyde de olsa işleyişini bilmeleri elzemdir. Bilişim teknolojilerinin gelişim hızı düşünüldüğünde, mevzuatın en üst düzeyde koruyuculuğunu sağlayabilmek, ancak içinde hukukçular, sağlık çalışanları, bilişim teknoloji uzmanları öncelikli olmak üzere sürece dahil olan tüm kişilerin bulunduğu, multi disipliner çalışma grupları ile mümkün olabilecektir. Sürecin hızlı gelişimi göz önüne alındığında, bu ekiplerin de sürekli ve iş birliği içerisinde çalışması, düzenlemelerin koruyuculuğunun sağlanması açısından bir gerekliliktir.

KAYNAKÇA

Abudureyimu Y. / Oğurlu, Y. "Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Cilt 20, Sayı 41, 2021, s. 765-782.

Akçalı Gür, B. "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 25, 2019, s. 850-872.

Akgül, Aydın, "Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi", Yayımlanmamış Doktora Tezi, Kocaeli 2013.

Akıncı, Ayşe Nur, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", Kalkınma Bakanlığı Çalışma Raporu-6.

Akkurt, Sinan Sami, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, Cilt 2, Sayı 5, 2020, s. 21.

Aksoy, Hüseyin Can, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", Kişisel Verileri Koruma Dergisi, Cilt 4, Sayı 2, 2022, s. 69-87.

Aksoy, Hüseyin Can, "The Right to Personality and It's Different Manifestations as the Core of Personal Data", Ankara Law Review, Cilt 5, Sayı 2, s.235-249.

Aksoy, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010.

Allyson, Haynes Stuart, "Google Search Results: Buried If Not Forgotten", North Carolına Journal of Law & Technology, Cilt 15, Sayı 3, 2014, s. 463.

Arslan, Ç., "Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Sayı 1, Ocak 2010, s. 447-487

Aşıkoğlu, İpek / Uzun, Fatih Burak, "Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri (Problems Caused by Basing Cross-Border Data Transfers to Explicit Consent and Solution Suggestions)", Prof. Dr. Türkan Rado'nun Anısına Armağan, 2020, https://ssrn.com/abstract=3683903 (son erişim tarihi: 19.05.2023).

Aşıkoğlu, Şehriban İpek, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda", Kişisel Verileri Koruma Dergisi, Cilt 1, Sayı 2, 2019.

Atagün, Ömer Faruk, “Kişisel Veri Koruma Hukukunda Anonimleştirme”, https://www.omeratagun.com/files/Kisisel%20Veriler%20Anonimlestirme.pdf (son erişim tarihi: 10.05.2023).

Aydın, Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı’nın Google Kararı”, TBB Dergisi, Cilt 2016, Sayı 116, 2015, s. 35.

Ayözger Öngün, A. Ç., Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, 2. bs, 2019.

Bennett, Steven C, “The Right to Be Forgotten: Reconciling EU and US Perspectives”, Berkeley Journal of International Law, Cilt 30, Sayı 1, Article 4, s.173.

Büyüksağiş, E. “Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 18, 2021, s. 529-541.

Cassani, Carlotta, “Hukuka Uygunluk Nedeni Olarak Hukukta Rıza”, TBB Dergisi, Sayı 77, 2008, s. 236-248.

Civelek, D. Y. Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Ankara 2011.

Cömertler N. / Kar M. “Türkiye’de Suç Oranının Sosyo-Ekonomik Belirleyicileri: Yatay Kesit Analizi”, Ankara Üniversitesi SBF Dergisi, Cilt 62, 2007, s. 37-57.

Croft, W. Bruce / Metzler Donald / Strohman, Donald, Search Engines and Information Retrieval in Practice, Boston, USA 2010.

Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3.bs, İstanbul 2020.

Çelik, Işıl, Kişisel Verilerin Yurt Dışına Aktarılması, 1. bs, İstanbul 2022.

Çelik, Yeşim, “Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı”, TAAD, Cilt 32, 2017.

Çelikel, Serdar, “Kişisel Verilerin İşlenmesinde, Açık Rıza HukukaUygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR’la Karşılaştırmalı Olarak İncelenmesi”, Uyuşmazlık Mahkemesi Dergisi, Cilt 9, Sayı 17, Haziran 2021, s. 161-190.

Çınar, Abdurrahim, “Unutulma Hakkının Ortaya Çıkış Serüveni ve Kapsamının Değerlendirilmesi”, TAAD, Cilt 13, Sayı 49, Ocak 2022, s. 551-584.

Doğan, Derya, “Kişisel Verilerin Korunmasında Veri Madenciliği Etkisi: Online Mahremiyetin Sonunda mıyız?”, Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri, 23-25 Ocak 2013, Akdeniz Üniversitesi, Antalya, https://ab.org.tr/ab13/kitap/dogan_AB13.pdf (son erişim tarihi: 19.05.2023).

Dülger, Murat Volkan, "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Cilt 1, Sayı 2, 2015.

Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, 3. bs, İstanbul 2020.

Elmalıca, H. "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 65, 2016.

Er, Ünal, Sağlık Hukuku, 2. bs, Ankara 2019.

Favaretto, M. / De Clercq, E. / Elger, B. S. "Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review", J Big Data, Cilt 6, Sayı 12, 2019. Doi:10.1186/s40537-019-0177-4

Gedik, Ömer, Türk Yargı Kararları Çerçevesinde Kitle İletişim Özgürlüğü, Ankara 2008.

Gianclaudio, Malgieri, "Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations", Computer Law & Security Review, Cilt 35, Sayı 5, 2019,

Gülener, Serdar, "Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Türkiye Barolar Birliği Dergisi, 2012, s. 102-221.

Hatemi, H., Kişiler Hukuku, 9. bs, İstanbul 2021.

Karakaş, M.E. "Dijital Geçmişin İnternet Erişiminden Kaldırılması "Unutulma Hakkı" ve Türk Hukukunda Görünümü", Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 2, 2020, s. 262-289.

Kavza, Uğur, "Veri Madenciliğinde Mahremiyetin Sağlanması". Yayımlanmamış Yüksek Lisans Tezi.

Kılınç, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, Cilt 61, Sayı 3.

Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", TBB Dergisi, Cilt 124, 2016, s. 81-152.

Küzeci, Elif, İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı. İnsan Hakları Yıllığı, Cilt 32, 2014.

Küzeci, Elif, Kişisel Verilerin Korunması, 4 bs., İstanbul 4. Baskı.

Mendoza, Isak / Bygrave, Lee A., "The Right Not to Be Subject to Automated Decisions Based on Profiling" (Ed. Tatiani Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou). EU Internet Law: Regulation and Enforcement, 2017, https://ssrn.com/abstract=2964855 (son erişim tarihi: 10.04.2023).

Mittelstadt, B. D. / Allo, P. / Taddeo, M. / Wachter, S. / Floridi, L. "The Ethics of Algorithms: Mapping the Debate", Big Data & Society, Cilt 3, Sayı 2, 2016. Doi:10.1177/2053951716679679

Na L / Yang C/ Lo CC/ Zhao F/ Fukuoka Y/ Aswani A. "Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning", JAMA Netw Open, Cilt 1, Sayı 8, Aralık 2018, s. e186040. Doi: 10.1001/jamanetworkopen. 2018.6040

Nalbantoğlu, Seray, "Right to be Forgotten As a Fundamental Right", TAAD, Cilt 9, Sayı 34, 2018, s. 583-560.

Oğuzman, Kemal / Barlas, Nami. Medeni Hukuk, 15. bs, İstanbul 2008.

Ömür, Rahmi Can, "Kişisel Sağlık Verilerinin Korunması ve Hastanelerin Sorumluluğu", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt 15, Sayı 1, 2018.

Özdemir, Hayrunnisa, "Haberleşmenin Gizliliği ve Kişisel Veriler", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, , Cilt 13, Sayı 1-2, 2009, s. 285.

Özekes, S. "Veri Madenciliği Modelleri ve Uygulama Alanları", İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, Cilt 2, 2003, s. 65-82.

Peschke, L. "The Web Never Forgets!: Aspects Of The Right To Be Forgotten", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt 19, 2015, s. 151-160.

Retornaz, Eylem / Güçlütürk, Osman, Gelişen Teknolojiler ve Hukuk II: Yapay Zeka, İstanbul 2021.

Rodriguez, Roberto / Wilson, J, Petra / Schanz, Stephen J, The Regulation of Privacy and Data Protection in The Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to personal-Identifiable Health Databases, Washington 2001.

Sabire, Sanem, Tıp Alanında Kişisel Verilerin Korunması, 4. bs, Ankara 2020.

Shoor, Emily Adams, "Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation", 39 Brook. J. Int'l L, 2014, s. 501-502.

Sloan, H., / Warner, Richard Beyond Bias: Artificial Intelligence and Social Justice, Virginia Journal of Law and Technology, 2020, s. 1 vd.

Soysal, T. "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", Uyuşmazlık Mahkemesi Dergisi, 2019, s. 339-422.

Svantesson, D., "Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines", OECD Digital Economy Papers, Sayı 301, 2020, Doi: /10.1787/7fbaed62-En

Şimşek, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması. İstanbul 2008.

Tanör, Bülent, Türkiye'de İnsan Hakları Sorunu, 3. bs, İstanbul 1994.

Taylor, Mark John, Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge 2012.

Tortop, Nuri, "Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu", Amme İdaresi Dergisi, Cilt 33, Sayı 3, 2000, s. 2.

Uçak, M., "Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası", Kişisel Verileri Koruma Dergisi, Cilt 3, Sayı 1, 2020, s. 41-60.

Uzun, Yusuf / Uzun, Fatma Nur / Çakar, Esra, "Veri Madenciliği ve Kullanım Alanları", Uluslararası Mühendislik, Doğa ve Sosyal Bilimler Sempozyumu Isens-21 Ana Teması Enerji ve Toplum, 25-28 Kasım 2021, Batman Üniversitesi. https://www.researchgate.net/publication/356819774_veri_madencılıgı_ve_kullanım_alanları_data_mınıng_and_areas_of_use (son erişim tarihi: 19.05.2023).

Wang Y, / Kosinski M. "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images", J Pers Soc Psychol, Cilt 114, Sayı 2, Şubat 2018, s. 246-257. Doi: 10.1037/pspa0000098

Yann Le, Cun / Yoshua, Bengio / Geoffrey, Hinton, Deep Learning, 2015, s. 436.

Yantaç, Cavit /Falcıoğlu, Mete Özgür, "Yapay Zeka, İnsan ve Hukuk", Beykent Üniversitesi Hukuk Fakültesi Dergisi, 2020, s. 31.

Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Korunması, 4. bs, Ankara 2020.

Yücedağ, Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 75, Sayı 2, 2017.

Zeybek, Ünsal Çağrı, "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", Hacettepe Hukuk Fakültesi Dergisi, Cilt 3, Sayı 1, 2013, s. 99.

İnternet Kaynakları

"108 nolu sözleşme", https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, (19.05.2023).

"95/46 sayılı kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması direktifi", www.eur-lex.europa.eu, (19.05.2023).

"95/46/AT sayılı direktif md. 8/I", www.eur-lex.europa.eu, (19.05.2023).

"Amazon Scraps Secret aI Recruiting Tool that Showed Bias Against Women", Reuters, (11 Ekim 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G, (15.05.2023).

"Applied sciences and engineering: Computer science", https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe, (14.05.2023).

"Avrupa hasta haklarının geliştirilmesi bildirgesi", http://www.saglikhakki.org/amsterdam1.htm, (19.05.2023).

"Avrupa insan hakları mahkemesi, Z/Finlandiya Davası, Başvuru Numarası: 22009/93", https://dergipark.org.tr/en/download/article-file/1671838, (19.05.2023).

"Big data is better data", https://www.ted.com/talks/kenneth_cukier_big_data_is_better_data (19.05.2023).

"Binlerce Avrupalı unutulmak istiyor", Ulusal, (12 Ekim 2014), https://www.ulusal.com.tr/haber/8441749/binlerce-avrupali-unutulmak-istiyor, (20.05.2023).

"Biyoetik ve insan hakları evrensel bildirgesi", http://www.unesco.org.tr/Content_Files/Content/Sektor/Sosyal_ve_Beseri_B/evrensel_bildirgesi.pdf (19.05.2023).

"Biyoloji ve tıbbın uygulanması bakımından insan hakları ve insan haysiyetinin korunması sözleşmesi: İnsan hakları ve biyotıp sözleşmesinin onaylanmasının uygun bulunduğuna dair kanun", https://www.tbmm.gov.tr/kanunlar/k5013.html, (19.05.2023).

"Declaration of Lisbon". https://www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/, (19.05.2023).

"Declaration on the promotion of patients' rights in Europe", http://www.nurs.uoa.gr/fileadmin/nurs.uoa.gr/uploads/Nomothesia_Nosilefton/Evropaika_keimena/eu_declaration1994_1_pdf, (19.05.2023).

"European charter of patients rights", http://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/health_services_co108_en.pdf, (19.05.2023).

"European data protection board guidelines", https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en, (19.05.2023).

"European parliament report, report with recommendations to the commission on civil law rules on robotics (2015/2103(INL)", https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html, (19.05.2023).

"Google-İspanya Kararı", https://kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf, (19.05.2023).

"Hekimlik meslek etiği kuralları", https://www.ttb.org.tr/kutuphane/h_etikkural.pdf, (30.04.2023).

"Kişisel veri koruma hukukunda anonimleştirme",https://www.omeratagun.com/files/Kisisel%20Veriler%20Anonimlestirme.pdf, (19.05.2023).

"Kişisel verileri koruma kurumu, esas alınacak kriterler. Kişisel verileri koruma kurumu taahhütnameler", https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler, (19.05.2023).

"Kişisel verilerin otomatik işleme tabi tutulması karşısında bireylerin korunması sözleşmesinin onaylanmasının uygun bulunduğuna dair kanun tasarısı ve dışişleri komisyonu raporu", www.tbmm.gov.tr/sirasayi/donem24/yil01/ss700.pdf, (19.05.2023).

"KVKK temel kavramlar", https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun%27da-Yer-Alan-Temel-Kavramlar, (19.05.2023).

"Tıbbi deontoloji nizamnamesi", http://www.mevzuat.gov.tr/MevzuatMetin/2.3.41257 8.pdf, (19.05.2023).

"Tıbbi deontoloji nizamnamesi", https://www.mevzuat.gov.tr/mevzuatmetin/2.3.412578.pdf, (30.04.2023).

"U.S. congress, office of technology assessment: federal government information technology: Electronic record systems and individual privacy, Washington", https://ota.fas.org/reports/8606.pdf, (19.05.2023).

ABAD 06.11.2003 C-101/01 (http://curia.europa.eu/juris/liste.jsf?num=C-101/01, 19.05.2023).

ABAD- Breyer v. Federal Republic of Germany, (https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200442%22]}, 19.05.2023).

Ahi Hukuk, "Unutulma hakkı (The right to be forgotten)", https://ahi.av.tr/unutulma-hakki-the-right-to-be-forgotten/, (19.05.2023).

AİHS, https://www.echr.coe.int/documents/convention_tur.pdf, (19.05.2023).

Archie, Maryam / Gershon, Sophie / Katcoff, Abigail / Zeng, Aaron, "Who's Watching?" https://courses.csail.mit.edu/6.857/2018/project/Archie-Gershon-Katchoff-Zeng-Netflix.pdf (14.05.2023).

CNIL.fr, right to be delisted: The CNIL restricted committee imposes A €100,000 fine on Google, https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google, (19.05.2023).

Culnane, Chris, "Health data in an open world", https://arxiv.org/abs/1712.05627 (14.05.2023).

Danıştay, 09.10.2018 T. 2018/1490 E (http://emsal.danistay.uyap.gov.tr, 19.05.2023).

Danıştay, D15D YD 06.07.2017 E: 2016/10500 (http://emsal.danistay.uyap.gov.tr, 19.05.2023).

Data Protection, "Convention 108 and protocols", https://www.coe.int/en/web/data-protection/convention108-and-protocol, (30.4.2023).

Domo, "Data never sleeps 10.0", https://www.domo.com/data-never-sleeps, (14.05.2023).

Dülger, Murat Volkan, "Kişisel sağlık verileri yönetmeliğinin yürütmesinin durdurulmasına ilişkin Danıştay'ın 09.10.2018 tarihli kararına ilişkin değerlendirme", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792286, (19.05.2023).

ECHR, "S. And Marper v UK. Başvuru no. 30562/04 ve 30566/04, 04.12.2008", www.echr.coe.int, (19.05.2023).

European Commission, "Big data", https://digital-strategy.ec.europa.eu/en/policies/big-data, (14.05.2023).

European Commission, Factsheet on the "Right to be Forgotten" ruling (C131/12).

European Parliament, "Civil liability regime for artificial intelligence", https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654178/EPRS_STU(2020)654178_EN.pdf, (19.05.2023).

European Parliament, "Highlights", https://www.europarl.europa.eu/stoa/en/home/highlights, (14.05.2023).

Fleischer, "The right to be forgotten, or how to edit your history", http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html, (19.05.2023).

http://hudoc.echr.coe.int/sites/tur/Pages/search.aspx#{"fulltext":["Yıldırım"],"documentcollectionid2", (19.05.2023).

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (19.05.2023).

https://digitalstrategy.ec.europa.eu/en/policies/expert-group-ai, (14.05.2023).

Jeffrey Rosen, Symposium Issue, The Right To Be Forgotten, 64 Stan.L.Rev.

Keller, Daphne, "Global right to be forgotten delisting: Why cnil is wrong", https://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong, (23.04.2023).

Kişisel Veileri Koruma Kurumu, "Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler ile ilgili kişisel verileri koruma kurulunun 31/01/2018 tarihli ve 2018/10 sayılı kararı", https://kvkk.gov.tr/Icerik/4110/2018-10, (19.05.2023).

Kişisel Veileri Koruma Kurumu, "İşlenme amacının gerektirdiğinden fazla kişisel veri işlenmesi/aktarılması (veri minimizasyonu ilkesine aykırılık)", https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik, (15.05.2023).

Kişisel Veileri Koruma Kurumu, "Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru" kişisel verileri koruma kurulunun 25/03/2019 tarihli ve 2019/78 sayılı karar özeti", https://www.kvkk.gov.tr/Icerik/5434/2019-78, (16.05.2023).

Kişisel Veri, "95/46/EC kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması direktifi", https://kisiselveri.com/9546ec-turkce, (19.05.2023).

Kişisel Verilerin Koruma Kurumu, "Doğru bilinen yanlışlar-2", https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2, (19.05.2023).

Kulevska, "The future of your past: A right to be forgotten online?", https://lumendatabase.org/blog_entries/522, (20.05.2023).

Kulevska, Sanna, "The future of your past: A right to be forgotten online?", http://www.chillingeffects.org/international/weather.cgi?WeatherID=769, (19.05.2023).

Mltimedia Centre, "Panel for the future of science and technology", https://multimedia.europarl.europa.eu/en/webstreaming/panel-for-future-of-science-and-technology_20221128-1500-SPECIAL-STOA, (14.05.2023).

Nelson, Clarke W., 90th anniversary of the mayo medical records system. Elsevier, Cilt 72 Sayı 8, 1997, s. 696. www.mayoclinicproceedings.org/article/S0025-6196(11)63586-6/fulltext, (son erişim tarihi 19.05.2023).

Resmi Gazete (10.03.2018, 30356), "Aydınlatma yükümlülüğünün yerine getirilmesinde uyulacak usul ve esaslar hakkında tebliğ", http://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm, (19.05.2023).

Resmi Gazete, (01.08.1998, 23420), "Hasta hakları yönetmeliği", http://www.resmigazete.gov.tr, (19.05.2023).

Resmi Gazete, (07.04.2016, 29677), "KVKK md. 6. KVKK (2016), http://www.resmigazete.gov.tr, (19.05.2023).

Resmi Gazete, (10.03.2018, 30356), "Veri sorumlusuna başvuru usul ve esasları hakkında tebliğ", https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm, (19.05.2023).

Resmi Gazete, (13 Temmuz 2023), "Yürütme ve idare bölümü", http://www.resmigazete.gov.tr, (19.05.2023).

Resmi Gazete, (14.04.1928, 863), "Tababet ve şuabatı sanatlarının tarzı icrasına dair kanun", http://www.resmigazete.gov.tr, (19.05.2023).

Resmi Gazete, (20.10.2016, 29863), "Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelik". http://www.resmigazete.gov.tr, (19.05.2023).

Resmi Gazete, (24.11.2017, 30250), "Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelikte değişiklik yapılmasına dair yönetmelik", http://www.resmigazete.gov.tr/eskiler/2017/11/20171124-1.htm, (19.05.2023).

Resmi Gazete, (28.10.2017, 30224), "Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkında yönetmelik" http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, (19.02.2023).

Resmi Gazete, (30.12.2017, 30286), "Veri sorumluları sicili hakkında yönetmelik, http://www.resmigazete.gov.tr/eskiler/2017/12/20171230-7.htm, (19.02.2023).

Spiros, Simitis, "Revisiting sensitive data", https://rm.coe.int/0900001_6806845af, (19.05.2023).

Standford, "Artificial intelligence and life in 2030", 2016, https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, (14.05.2023).

T.C. Cumhurbaşkanlğı Mevzuat Bigi Sistemi, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4847&MevzuatTur=7&MevzuatTertip=5, (30.04.2023).

Türk Dl Kurumu, www.tdk.gov.tr, (16.05.2023).

Wired, “Netflix spilled your brokeback mountain secret, lawsuit claims”, https://www.wired.com/2009/12/netflix-privacy-lawsuit/, (19.05.2023).

World Health Organzation, https://www.who.int/about/mission/en/, (19.05.2023).

www.eur-lex.europa.eu, (19.05.2023).

Yargıtay 12. Ceza Dairesi, T: 02.12.2015 E: 2015/4006 K: 2015/18748”, (https://barandogan.av.tr/blog/mevzuat/tck-madde-136-verileri-hukuka-aykiri-olarak-verme-veya-ele-gecirme-sucu.html, 19.05.2023).

Yargıtay 4. Hukuk Dairesi 03.07.2013, 2013/6256 E, 2013/1282 K.

Yargıtay Ceza Genel Kurulu, T:17.06.2014 E: 2012/1510 K:2014/331, (www.emsal.yargitay.gov.tr, (19.05.2023).

Yargıtay Hukuk Genel Kurulu, 17.06.2015, 2014/4-56 E, 2015/1679 K.

Yargıtay Hukuk Genel Kurulu, E:2014/4-56 k.2015/1679 T.17.6.2015 (https://kazancı.com, 19.05.2023).