

---

## **VII. KISIM - PART VII**

---

**ETİK HUKUKSAL BOYUT VE VERİ GÜVENLİĞİ**

**ETHICAL, LEGAL DIMENSION AND DATA SECURITY**

---



# 37. BÖLÜM / CHAPTER 37

## TIP BİLİŞİMİ ETİĞİ

### ETHICS OF MEDICAL INFORMATICS

Nüket ÖRNEK BÜKEN\*, Çağrı ZEYBEK ÜNSAL\*\*

\*Prof. Dr., Hacettepe Üniversitesi, Tıp Fakültesi, Tıp Tarihi ve Etik, Ankara, Türkiye  
E-mail: buken@hacettepe.edu.tr

\*\*Araş. Gör., Hacettepe Üniversitesi, Tıp Fakültesi, Tıp Tarihi ve Etik, Ankara, Türkiye  
E-mail: zeybek.cagri@gmail.com

DOI: 10.26650/B/ET07.2021.003.37

#### ÖZ

Tıp Bilişimi, tıbbi uygulama ve bilgi ve iletişim teknolojilerini içerir. Ancak, bu teknolojilerin uygulanması sırasında genellikle istenmeyen çeşitli sorunlar ortaya çıkabilmektedir. Bunlar arasında özellikle etik ve yasal endişeler daha karmaşık ve çeşitlidir. İleri teknoloji, hastalıkların tedavisi ve rehabilitasyonunda bilgi ve iletişim teknolojilerinin kullanımını artırmıştır. Dolayısıyla bu girişimlerin etik yönü ve uygulamaya yönelik etik ikilemler önem kazanmıştır. Bir yandan hastaların tıbbi ve kişisel bilgilerinin gizliliğini korumak ve veri güvenliğini artırmak konusundaki profesyonel etik sorumluluk, diğer taraftan hekimlerin tıbbi vakalarını izlemeye ve sağlık hizmetlerinin kalitesini iyileştirmeye duyulan gereksinim nedeniyle ihtiyaç duydukları bilgi ve iletişim teknolojisindeki gelişmeler. Kişisel veriler ve kişisel bilgiler, bireyin özel hayatını korumak için farklı ülkelerin çeşitli yasalar, düzenlemeler ve politikalar oluşturduğu, insan haklarının ve mahremiyet hakkının entegre bir parçası olarak kabul edilmektedir. Teknoloji hızla geliştikçe fırsatlar da artmış ve doğası gereği sınırları daraltmaya başlamıştır. Bazı araştırmacılar, dijital ortamın doğası gereği, gizliliğin olması gerektiği gibi korunamayacağını savunmaktadırlar. Bu teze karşı diğerleri de, gizliliğin ihlaline yönelik güçlü mekanizmalar kurmanın, mahremiyetin ihlaline yönelik tehditleri azaltabileceğini savunmaktadırlar. Bu kapsamda her ülke kişisel verilerin korunmasına yönelik politikalar ve yasal belgeler geliştirmeye çalışmaktadır. Gizliliğin korunmasında teknik önlemlerin alınması, iletişim kanallarının güvenliğinin sağlanması, verilerin anonimleştirilmesi, kodlama veya dijital imza kullanılması alınacak önlemlerden bazılarıdır. Özellikle tıbbi kayıtların elektronik ortama dönüşümü, bu verilere yetkisiz erişilmesine karşı yeni koruma kalkanlarının geliştirilmesi gereğini doğurmaktadır. Veri güvenliğinin sağlanmasında; verilerin kalitesini koruyacak sistemlerin geliştirilmesi, verilerin toplama amaçları dışında kullanılmaması, verilere ilgilinin rızası olmadan ulaşılamaması, verilerin veri toplama amacına uygun sürede saklanması gibi ilkeler bulunmaktadır. Tıbbi verilerin korunmasında yasal düzenlemelerin yanında bireyi de etkinleştiren mekanizmalar yararlı olmaktadır. Bu sistemde verilerin kullanımı onaya tabidir, verilere erişimin çeşitli seviyelerde gerçekleşmesi kontrol altındadır, kullanıcıların kimlikleri denetim altındadır, şifreleme metotları kullanılmaktadır. Bu alanda çalışan profesyoneller etik sorumluluklarının farkına varmadıkça, hiçbir düzenleyici sistem uygun şekilde çalışamaz. Fazladan yapılacak düzenlemelerin bir tehlikesi de profesyonellerin kendi sorumlulukları yerine, düzenlemelerle uyumlu olmaya dikkat sarf etmeleri yüzünden, ahlaki sorumluluk duygusunun göz ardı edilebilecek olmasıdır. Yani dış denetim elbette

önemli ve gereklidir ancak daha önemlisi iç denetim mekanizmalarının varlığıdır. Herhangi bir dış yapı/kurum tarafından denetlenmeden de, içten gelen doğruyu yapma konusundaki motivasyonun varlığıdır.

**Anahtar Kelimeler:** Tıbbi bilişim, bilgi ve iletişim teknolojisi, etik, yapay zeka, bilgilendirilmiş onam, mahremiyetin korunması, gizlilik, sağlık bilgilerinin etik kullanımı, nesnelerin interneti

## ABSTRACT

Medical informatics involves medical practice and information and communications technology. However, various issues hamper the implementation of these technologies. Among these challenges, ethical and legal concerns are some of the more complex and diverse ones. The objective of this study is to conduct an analysis of scientific literature to identify the ethical and legal challenges of medical informatics. Advanced technology has increased the use of information and communications technology in the treatment and rehabilitation of diseases. Therefore, the ethical aspect of these attempts has evolved as a challenge. To ensure the confidentiality of patients' information and increase data security, there is a need to monitor the cases of physicians' inefficiency and improve the quality of health care services, which all highlight the necessity of ethical issues in information and communications technology. Personal data and personal information have been considered as an integrated part of human rights and the right to privacy, where different countries formulate various laws, regulations, and policies to protect an individual's private life. With the faster growth of technology, the opportunities have increased and started to narrow the limits by its nature. Some argue that privacy cannot be protected as it should be since the nature of digital environment. However, others argue that establishing strong mechanisms can reduce the threats to privacy violations. In this regard, each country tries to develop policies and legal documents for the protection of personal data.

**Keywords:** Medical informatics, information and communications technology, ethics, artificial intelligence, informed consent, privacy protection, confidentiality, ethical use of health information, internet of things

## Giriş

Bir teknik disiplin olarak tıp ve bilişim alanının tıp içindeki uzantısı olan tıp bilişimi, bilgi ve iletişim teknolojilerinin en çok kullanıldığı ve bilimsel bilgi üretiminin de en yoğun olduğu alanlardır. Bu alandaki ilerlemeler teknoloji ile hız kazanırken, artan teknoloji kullanımı da biyoetiğin alanını genişletmiştir. Bilimsel ilerleme şimdi o denli hızlı, ortaya koyduğu sonuçlar öylesine çabuk benimsenmektedir ki, bunun üzerimizdeki etkisini yeterince değerlendirememiz, bu yüzden de bizi götürdüğü yeri yeterince anlayamama tehlikesiyle karşı karşıyayız. Bilimin uygulanmasıyla elde edilen teknik olanakların insanlığın yararına dönük kullanılması sırasında insanı bilimsel ve teknik bir uygulamanın nesnesi, ürünü haline sokma eğiliminin tehlikelerinin altını çizmenin önemli olduğu bir bilgi/iletişim teknolojisi çağından geçiyoruz.

Diğer taraftan, bir tıp tarihçesinin belirttiği gibi; “Tıp tarihinin incelenmesinin bize öğrettiği en önemli şey, bilimsel açıdan kontrol edilmeyen klasik hükümlerin, oldukça sık yanılgıya neden olan pusulalar olduğudur. Erken dönemde başlatılıp sürdürülen teknoloji uygulamaları, toplumsal değerler açısından irdelenmediğinde, tıbbi yaklaşım pusulasız ya da dümensiz bir gemiye dönüşebilmektedir”.

Bilimsel bir disiplin ve sanat olan tıba teknolojinin girmesi ve gelişmesi, birçok “yeni” durum yaratmıştır. Bu yeni durumların özelliği, çoğunlukla daha önceleri insanın yapabileceği sınırları dışında olan birçok şeyin “olanaklı” hale gelmiş olmasıdır. Bu sürecin insanın ahlaksal sorumluluk alanını genişlettiği ve kısmen de değiştirdiği açıktır. Özgür karar ve seçim için hiçbir açık kapının bulunmadığı, bazı şeylerin bize bağlı olmadığı durumlarda “ahlaksal/etik sorumluluk” pek yoktur. Ancak, bilimsel ve teknolojik ilerlemeler sayesinde bunlar insan denetimine verildiklerinde, ahlakla ilgili hale gelirler, etik değerlendirme konusu olurlar (Büken, 1997).

Etik “tümüyle olanaklı olan” ve “izin verilen” arasında bir fark olduğunu, bunun sonucunda bazı olanakların bazı ahlaksal nedenlerden dolayı gerçekleştirilmemesi gerektiğini varsayar. Tıp kurumu her bulduğu yeniliği uygulama alanına geçirebilseydi, bütün insan toplumlarında çözümü güç, değer sorunları ortaya çıkacaktı. Bu tür sonuçları önleyebilmek için tıp biliminin ortaya koyduğu yenilikleri, insanın değeri yönünden bir değerlendirmeden geçirerek, insanın onurunu ve gönencini merkeze koyarak, insanlık adına en uygun olanı uygulamaya koymasına gerekmektedir (Büken, 2019).

Bugün yaygın olarak görülen tutum bilimsel ve teknolojik ilerlemelerin olanaklı kıldığı tüm yeniliklerin bir an önce yaşama geçirilmesi, gerçekleştirilmesi yönündedir. Bu durum kısmen yeniliğin çekiciliğinden, yeni şeyler görme ve deneme isteğinden kısmen de yeni ve bilinmeyen yöntemler konusunda bir düzenlemenin olmamasından kaynaklanmaktadır. Bu “yeni” alanda yerleşmiş normların olmaması, “tam eylem özgürlüğü”ne kapı açabilmektedir. Bu durum da bilim ve teknolojiyi istenmeyen, tehlikeli olabilecek, kimi zaman etik dışı bir yöne doğru sürükleyebilmektedir.

Tıptaki yeniliklerin tartışmasız kabulü çoğu zaman kaynakların ve emeğin boşa harcanmasına, bazı durumlarda ise canlının zarar görmesine yol açabilmektedir. Dünyada kanıta dayalı tıbbi yaklaşıma duyulan gereksinim gün geçtikçe artmakla birlikte, tıbbi teknolojilerin eleştirel açıdan değerlendirilmesinin önündeki engeller de artmaktadır. Bu engellerin başında tıp tarihinde de yüzyıllar boyu etkin olan “otoriteye boyun eğme, olanı değil otoritenin işaret ettiğini görme” tutumu gelmektedir. “Otorite tarafından yanıtılma olgusu” diyebileceğimiz bu olgunun önüne geçebilmek için yeni bir teknolojiyle ilgili kararlar, bu yeniliği destekleyenlerin prestijine göre değil, bilimsel ve etik verilerin ağırlığına dayanılarak alınmalıdır (Büken, 1997).

Günümüz tıbbi artık daha çok kişiselleştirilmiş (*personalized medicine*), öngörülebilir, önleyici, hassas (*precision medicine*) ve bu alandaki bütün aktörlerin katılımını öngören bir

anlaşıştadır. Günümüzde biyotıp teknolojileri, yalnızca tanı-tedavi sürecini değil, biyotıp araştırmalarının niteliğini ve bu süreçte sınırları belirleyecek olan etikolegal düzenlemeleri değiştirmekte, dönüştürmektedir; gen *editing* teknolojileri, tüm genom sekanslama, genetik testler ve tesadüfi bulgular, tüketiciye verilen doğrudan genetik hizmetler (*direct-to-consumer testing*), insan embriyosunda genom biçimlendirme, süper insan, yapay zekâ, özerk makineler, büyük veri (*big data*), robot teknolojileri etiği, embriyonun bilimsel araştırmalardaki kullanımı, yapay üreme teknolojilerinde babalık ve anneliğin yeni boyutunun tartışılmaya başlanması, bu teknolojilerin kötüye kullanılmasının öjeniye neden olabilmesi ya da insanın doğal kapasitesinin iyileştirilmesinin yol açacağı sorunlar vb.

Sağlık alanında hızlı bir şekilde kullanılmaya başlanan bu yeni ve gelişen teknolojiler toplumu karmaşık, belirsiz ve öngörülemeyen bir sürece dahil etmektedir. Bunun sebeplerinden biri bu teknolojilerin risk ve yan etkilerinin öğrenilmesinin, ancak tecrübe yolu ile mümkün olabilmesidir. Öte yandan, henüz güvenilirliği bilinmeyen teknolojilerin geliştirilmesi ve kullanılması ile ortaya çıkan biyoetik sorunlar da pek çoktur; gizlilik, mahremiyet, ayrımcılık, özerkliğe saygı, risklerin önlenmesi, bu teknolojilere eşit ve adil erişimin nasıl sağlanacağı vb.

Günümüzün teknotıp ve biyotıp dünyasında anahtar konular; moleküler biyoloji, gen teknolojisi, gen düzenleme ve biyoteknoloji, nanoteknoloji, nöroteknoloji, bilgi ve iletişim teknolojileri alanında odaklanmıştır. 20. yüzyılın son teknolojik devrimlerinden biri olan bilgi ve iletişim teknolojisi kısa sürede insanlığın geleceğini etkileyecek en önemli olgulardan biri haline gelerek 21. yüzyıla taşınmıştır. Ancak bilgi ve iletişimin geleceği yalnızca teknolojiye değil, toplumların “değerler sistemi”ne ve evrensel biyoetik değerlere de son derece bağlıdır. Bu teknolojinin sosyokültürel ve evrensel biyoetik değerler bağlamından kopartılması oldukça tehlikeli sonuçlar doğurabilir. Bilimsel ve teknolojik gelişmelerden beklenen, daha sağlıklı, mutlu, daha güzel bir yaşam, ancak bu gelişmelerin biyoetik kaygı ve duyarlılığı taşımasıyla mümkün olabilir.

Biyoetik çevrelerde de tartışmalar bu parelede devam etmektedir. “Bilimde uyulması gereken tek kural, yapılması gerekenin yapılmasıdır” diyerek etik kaygıların bilimsel araştırmaların önünde engel oluşturmayacağını savunanlar olduğu gibi, insan yaşamını ve insan değerini merkeze koymayan ve insanı “amaca araç olarak kullanan” her uygulamanın, etik açıdan değerlendirilmesi gerektiğini savunanlar ve bu girişimlerin ardındaki niyetin araştırılması gerekliliği üzerinde duranlar da vardır.

20. yüzyılın ikinci yarısından itibaren Avrupa ülkeleri ile birlikte pek çok ülkede biyoetik konularına verilen önem artmış, biyoetiğin alanına giren konularda, kılavuzlar, ulusal ve uluslararası yasal düzenlemeler oluşturulmuş, etik komiteler kurulmuş; ülkelerde biyoetik

sorunların ele alınışındaki farklılıklara rağmen ortak bir fikir birliğine varılmasını hedefleyen çalışmalar yapılmaya başlanmıştır (Quintana, 1993). Bu şekilde, biyoetiğin, akademinin ve toplumun ilgi alanına girmesi ile evrensel sorunlara evrensel çözümler üretilmesi gerektiği düşüncesi gelişmiştir.

Biyoetiğin evrenselleşmesi ile birlikte, biyoetik ve insan hakları arasındaki ilişki üzerine olan ilgi de artmış, biyoetik ve insan haklarının gelişimlerinin birlikte mümkün olduğunu savunan görüşler olmuştur. Literatürde, biyoetiğin temel ilkelerinin gelişiminde uluslararası insan hakları hukukunun dikkate alınması gerekliliği belirtilmiş, çalışmaların büyük çoğunluğu normatif ve kurumsal anlamda insan hakları yaklaşımının, biyoetik sorunların çözümünde etkin kullanılıp kullanılmayacağı üzerine yoğunlaşmıştır.

Çağımızda yüksek teknoloji tıbbının hüküm sürdüğü biyotıp alanında, etkililik ve teknik yenilikler, yalnızca bilim insanlarının değil, hastaların ve toplumun da ilgisini üzerine toplamaktadır. Biyolojik materyallerin saklanmasıdaki teknik olanakların gelişimi yanında, biyolojik verilerin dijital ortamda işlenmesi ve bilgisayar teknolojilerindeki yenilikler de örneklere ait verilerin toplanmasını, izlenmesini ve üzerinde her türlü analizin yapılmasını kolaylaştırmaktadır. Yani hem biyolojik materyalin kendisi hem de bu materyalden elde edilen verilerin kullanımı önem kazanmaktadır (Büken, 2019).

### **Hasta Mahremiyeti Açısından Veri Güvenliğinin Sağlanması**

Bilgisayar teknolojileri ve dijital bilginin hayatımızın hemen her alanına girmiş olduğu günümüzde, mahremiyetin ve güvenliğin sağlanması son derece önem kazanmaktadır. Sağlık kuruluşları/laboratuvarları arasındaki ya da biyobankalar gibi tıbbi veri sağlayıcısı organizasyonlar arasındaki veri akışları, sağlık hizmetlerinin kalitesini ve araştırma olanaklarını artırırken hasta mahremiyetinin ihlal edilmesi riskini de arttırmaktadır (Büken, 2019). İletişim teknolojilerinin biyotıp alanında kullanımının hızla yaygınlaşması pek çok açıdan kolaylıklar sağlarken, bu verilerin depolanması ve transferi konularında güvenlik ihtiyacını da gündeme getirmektedir. Gizliliğin korunmasında teknik önlemlerin alınması, iletişim kanallarının güvenliğinin sağlanması, verilerin anonimleştirilmesi, kodlama veya dijital imza kullanılması alınacak önlemlerden bazılarıdır. Özellikle tıbbi kayıtların elektronik ortama dönüşümü, bu verilere yetkisiz erişilmesine karşı yeni koruma kalkanlarının geliştirilmesi gereğini doğurmaktadır.

Veri güvenliğinin sağlanmasında; verilerin kalitesini koruyacak sistemlerin geliştirilmesi, verilerin toplanma amaçları dışında kullanılmaması, verilere ilgilinin rızası olmadan ulaşılamaması, verilerin veri toplama amacına uygun sürede saklanması gibi ilkeler bulunmaktadır. Tıbbi verilerin korunmasında yasal düzenlemelerin yanında bireyi de etkinleştiren mekaniz-

malar yararlı olmaktadır. Bu sistemde verilerin kullanımı onaya tabidir, verilere erişimin çeşitli seviyelerde gerçekleşmesi kontrol altındadır, kullanıcıların kimlikleri denetim altındadır, şifreleme metotları kullanılmaktadır (Büken, 2016 I; Büken, 2016 II).

Bugün tıp uygulamaları sırasında özel yaşamın, mahremiyetin ya da özelliğın korunması hakkı, kaynağını anayasalardan almaktadır. Tıp hizmetlerinden yararlanan kişilerin, kişisel nitelikteki bilgilerinin “mahremiyeti” korunmalıdır. Tutulan kayıtlar ve eldeki bilgiler, hastanın rızası olmaksızın üçüncü kişilere aktarılamaz. Kimi ülkelerde bu onamın yazılı olması istenmektedir. Bu bilgilerin adsız olarak, örneğın istatistiksel izlem, bilimsel araştırma gibi amaçlarla kullanılması ise düzenlemelere tabidir. Her bireyin özel yaşamının dokunulmazlığı hakkına saygı gösterilmeli ve bu hak korunmalıdır; bireyin düşünce, duygu ve kişisel yaşamının sırlarını, başkalarıyla ne ölçüde paylaşacağına kendisinin karar vermesi hakkına saygı gösterilmelidir. Günümüzde, tıp kayıtlarının bilgisayarda korunması, özel sigorta kuruluşlarının yaygınlaşması ve ağırlık kazanması, sağlık kuruluşlarının bilimsel, yönetsel, ekonomik yönden yoğun bir denetim altında bulundurulması gibi durumlar nedeniyle, hasta kayıtlarının mahremiyetinin korunması konusunda, yeterince titizlik gösterilemeyeceğı kaygısı yaygınlaşmaktadır. Bir sigorta ağına ya da bir işe girerken, yapılan tıbbi değerlendirmeler sırasında elde edilen bilgilerin korunması, en az bu taramaların kendisi kadar tartışma konusu olmaktadır.

Tıp uygulamaları sırasında, hekimin tedavisini üstlendiğı hastaya ait kişisel bilgileri saklı tutma zorunluluğı, hiç kuşkusuz insan araştırmaları için de geçerli olan bir ilkedir ve araştırmaya katılan hekimlerin gönüllü katılımcının mahremiyetine değer vermeleri ve bunun sorumluluğunu üstlenmeleri gerekmektedir. Araştırmaların sürdürülmesinde ve sonuçların yayımlanmasında gönüllülerin mahremiyetinin (özel yaşam gizliliğı) korunması, kişisel kimlik bilgilerinin açıklanmamasını gerektirmektedir. Bu konuda önlem olarak, örneğın kayıtların gizliliğı esas alınarak veriye ulaşım sınırlandırılabilir ya da kişilere bir tanıtım numarası verilebilir.

Kişisel verilerin korunmasıyla ilgili Avrupa Birliğı çerçeve yönetmeliklerinde ve özellikle biyomedikal araştırmalar açısından Oviedo Sözleşmesi (The Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine, 1997) kapsamında çeşitli maddeler bulunmaktadır. Özellikle genetik örnek ve bilgilerin saklandığı biyobankalarda bu verilerin ayrımcılığa yol açmaması, kişilerin işveren ve sigortalar gibi üçüncü şahıslar nezdinde haklarının korunması açısından önemlidir.

### **Avrupa Konseyi, UNESCO ve Birleşmiş Milletler Teşkilatının Çabaları**

Avrupa Konseyi ve UNESCO, biyomedikal alandaki uygulamalar ve araştırmalar ile ilgili insan hakları ilkelerinin oluşturulması konusunda, süreç içerisinde oldukça çaba göstermiş ve uluslararası bir fikir birliğine varmak için mekanizmalar geliştirmiştir. Bilimsel araştırmalar



ve tıbbi teknolojilerin kullanılması konularında ülkeler arasındaki farklı uygulamalar, ülkelerin ulusal yasalarındaki düzenlemelerin uluslararası düzeyde uyumlaştırılması gereksinimini doğurmuştur. Bu bağlamda Avrupa Konseyi'nin büyük çabaları olmuştur. Söz konusu uyumlaştırmanın gerçekleştirilmesi için Avrupa Konseyi Biyoetik Yürütme Komitesi (CAHBI-CD-BI) kurulmuştur. Bu komite, 1985 yılından bu yana belgeler hazırlamaktadır. Avrupa Konseyi Bakanlar Komitesi tarafından onaylanan ve bağlayıcılığı olmayan bu metinler, ülkelerin parlamentolarına tavsiye olarak sunulmaktadır.

Öte yandan UNESCO, biyomedikal teknolojilerin ve sağlık konularının evrensel yapıya sahip olmaları nedeniyle biyotıp alanında minimum ortak standartların oluşturulmasında öncü olmuş; bilim, etik ve insan haklarının ortak paydada kesişiminde büyük rol oynamıştır.

Birleşmiş Milletler (BM), sürdürülebilir kalkınma hedeflerini (*SDG* 's) belirlemeden önce hazırladığı ve 2000 yılında 189 ülke tarafından imzalanan Milenyum Deklarasyonundan kaynak olarak, Binyıl Kalkınma Hedeflerini/Milenyum Kalkınma Hedeflerini (*MDGs*) oluşturmuştur. Milenyum Kalkınma Hedeflerinde her bireyin onuruna saygı hakkı, özgürlük, eşitlik, açlık ve şiddeti ortadan kaldırmak, dayanışma ve hoşgörüyü desteklemek bulunmaktadır. Sekiz hedef olarak belirlenen Milenyum Kalkınma Hedeflerinin amacı, dünyanın en fakir ülkelerindeki sosyal ve ekonomik durumları iyileştirerek, bu ülkelerin gelişmelerine destek olmaktır. En az yirmi üç uluslararası kuruluş ve 192 BM üyesi ülke, yoksullukla mücadele, çocuk ölüm oranlarının azaltılması, AIDS gibi hastalıklar ile mücadele etmek ve global bir ortaklık oluşturmak gibi hedefler üzerinde 2015 yılında uzlaşmışlardır.

Milenyum Kalkınma Hedeflerini tamamlamak üzere oluşturulan Sürdürülebilir Kalkınma Hedefleri (*SDGs*) ise on yedi hedeften oluşmakta olup, 2030 yılında gerçekleştirilmek üzere belirlenmiştir. Birleşmiş Milletler, sürdürülebilir kalkınma programı ile 2015 ve 2030 yılları arasında her yerdeki açlık ve yoksulluğu bitirmek, ülkelerdeki ve ülkeler arasındaki eşitsizliklerle mücadele etmek, barış içinde adaletli bir toplum inşa etmek, insan haklarını korumak, kadınların ve kız çocuklarının güçlendirilmesi ile cinsiyete dayalı eşitliği desteklemeyi hedeflemektedir. Bu hedeflerin yanı sıra, evreni ve evrenin doğal kaynaklarını korumayı da sürdürülebilir kalkınma hedefleri olarak belirlemiştir.

Birleşmiş Milletler, herkes tarafından teknolojiye erişebilmenin tüm ülkeler açısından sağlanması ve “geride kimsenin bırakılmaması” prensibinden hareketle, sürdürülebilir kalkınma hedeflerinin gerçekleştirilmesi için çeşitli çalışmalar yürütmektedir. Birleşmiş Milletlerin, az gelişmiş ülkelerin teknolojik gelişmelerden de bu teknolojilerin üretildiği ülkeler ile aynı oranda yararlanabilmesi için bir Birleşmiş Milletler kuruluşu olan ‘Teknoloji Bankası’

oluşturulmuştur. Söz konusu teknoloji bankası, diğer Birleşmiş Milletler Kuruluşları ile iş birliği içinde Guinea, Haiti, Sudan, Timor-Leste and Uganda'nın bilim, teknoloji ve inovasyon konusunda teknoloji gereksinimlerini değerlendirecektir. Türkiye ve Birleşmiş Milletler arasında, Eylül 2017'de, bilim, teknoloji ve inovasyon alanlarında kapasite geliştirmek amacı ile anlaşma imzalanmıştır (UN Chronicles, 2018).

BM 1992 Çevre ve Gelişim Hakkında Rio Deklarasyonu'nda belirlenen ilkelere göre; devletler kalkınma hakkını, şimdiki ve gelecek nesillerin, kalkınmaya yönelik ve çevresel ihtiyaçlarını, eşitlikçi/hakça bir şekilde karşılamaya yönelik olarak kullanmalıdır. Ayrıca devletler, bilimsel ve teknolojik bilgileri paylaşarak ve teknolojilerin geliştirilmesi, adaptasyonu, yayılması ve transferine, yeni ve yenilikçi teknolojileri dahil etmek yoluyla, sürdürülebilir kalkınma için içsel kapasite inşasını güçlendirmek amacıyla, işbirliğine gitmelidirler (Birleşmiş Milletler Rio Deklarasyonu, İlke 9, 1992). Söz konusu Deklarasyonda, bütün devletlerin ve insanların, yaşam standartlarındaki farklılıkları azaltmak, dünyadaki insanların çoğunluğunun ihtiyaçlarını daha iyi karşılamak amacıyla, sürdürülebilir kalkınma için iş birliğine gitmeleri gerektiğini de düzenlemiştir. Aynı şekilde kaçınılmaz bir gereklilik olarak, fakirliği ortadan kaldırmak için iş birliği yapmaları gerekliliği de ifade edilmiştir.

Kalkınma konusundaki 'fırsat eşitliği prensibi', BM Antlaşması ve İnsan Hakları Evrensel Bildirgesi'nin temel ilkelerindedir. İnsan haklarını koruyan ulusal yasal düzenlemelerin yanı sıra, sürdürülebilir kalkınma için, ekonomisi güçlü olan ülkelerin bu teknolojileri üretmeyen ülkeler ile iş birliği yapmasını sağlayan ve teşvik eden bir üst yapının da oluşturulması gerekmektedir. Öte yandan, Avrupa Konseyi de Birleşmiş Milletlerin Sürdürülebilir Kalkınma Hedeflerine katkı sağlamayı amaçlamıştır. Evrensel değerler olan insan hakları, hukukun üstünlüğü ve demokrasinin sağlanması amacı ile kurulan Avrupa Konseyi'nin faaliyetlerinin, 2030 sürdürülebilir kalkınma gündemi ile ilişkili olduğu ve belirlenen hedeflerin gerçekleştirilebilmesi için BM'nin programına katkı sunacağı belirtilmiştir.

Sağlık bakım hizmetine herkes tarafından eşit şekilde erişimi güvence altına almayı düzenleyen İnsan Hakları ve Biyotıp Sözleşmesi'nin 3. maddesi ve herkes için sağlıklı yaşamlar oluşturmak ve refahı arttırmak başlığını taşıyan sürdürülebilir kalkınma hedefi birbirine paraleldir. Bu düzenleme kapsamında, yetersiz ve sınırlı kaynaklar, toplumdaki sosyoekonomik farklılıklar ve ekonomik krize karşı alınacak uygun önlemlerin herkesin kaliteli sağlık hizmetine eşit bir şekilde ulaşabilmesine katkı sağlayacağı dile getirilmektedir (Council of Europe contribution to the UN 2030 Agenda for Sustainable Development, 2018).

UNESCO Bildirgeleri ve Avrupa Konseyi İnsan Hakları ve Biyotıp Sözleşmesi (Oviedo Biyotıp Sözleşmesi) karşılaştırıldığında, üç ortak özelliklerinin bulunduğu görülmektedir.

Bunlar;

- İnsan onurunun üstün ilke olarak kabul edilmesi,
- İnsan haklarının çerçeve olarak çizilmesi,
- Bir dizi geniş etik ilkeler grubunun benimsenmesidir.

Öte yandan kültürün, inanç sistemlerinin, toplumların sosyal yapılarının farklı olmasının evrensel biyoetik ilkeler oluşturmaya izin vermediğini savunan görüşler, uluslararası düzeyde evrensel kabul edilen değerlerin, Batının liberal demokrasisinin bireyselci değerleri olması nedeni ile, evrensel olarak uygulanamayacağından söz etmektedirler. Evrensellik ve görecelik arasındaki bu tartışma biyoetiğin evrensel olarak uygulanmasını ve normatif değerler üretmesini güçleştirmektedir.

Ancak diğer taraftan çok iyi bilinmektedir ki bilim artık tek başına değil, ülkeler arasında iş birliği halinde ortak çalışmalarla yürütülmektedir. Bu açıdan bakıldığında, bilim ve teknolojinin uygulanmasının sonucu olarak ortaya çıkan etik ikilemlere karşı geliştirilecek yasal, etik ve politik çözüm mekanizmalarının da evrensel olması gerekmektedir.

Bu bağlamda, hukuki standartların birbirleriyle harmonize edilerek, uygun mekanizmaların geliştirilmesi, etik ve hukuk kurallarının etkin uygulanmasının sağlanması açısından önem kazanmaktadır. Bunun için ortak biyohukuk (*bio-law*) normları oluşturma çabası da evrensel bir çabadır. Bugün bu çaba üzerinden yeni bir alanın ortaya çıkmasına tanıklık ettiğimiz öne sürülmektedir. Söz konusu çabalar sonucunda ortaya çıkan bu yeni disiplin uluslararası biyotıp hukuku veya uluslararası biyohukuk olarak adlandırılmaktadır. Bu hukuk dalı uluslararası insan hakları hukukunun bir uzantısı olarak değerlendirilmektedir (Andorno R., 2013). Uluslararası insan hakları hukuku, kişilerin ve grupların uluslararası düzeyde korunan haklarının ihlal edilmesine karşın, onların korunması ile ilgilenen bir hukuk dalıdır.

Ioanna Kuçuradi'ye göre, insan hakları insan aklı tarafından üretilen bir fikirdir. Kuçuradi, insan haklarını, 'bütün insanların eşit olduğu ve her kişinin sırf insan olması nedeni ile sahip olduğu haklar' olarak ifade etmiştir (Kuçuradi, 2016). İnsan hakları, insanın bir tür yapısal olanaklarının gerçekleştirilmesini olanaklı kılan bir şekilde muamele görmeyi isteme hakkı olarak da tanımlanmaktadır. Kuçuradi, bu hakların her birinin etik ilkeler olduğunu öne sürmektedir. İnsan hakları, insanlardan insanın değerini koruyan davranışlarda bulunmayı istemektedir. İnsanın değeri, benzerleri arasındaki özel yeri ve ona özel yer edindiren özel-

liklerini sürekli olarak gerçekleştirebilmeyi sağlayan nesnel şartlar olarak açıklanmaktadır. İnsan hakları ile birlikte insan onuru da insanın yapısına ilişkindir. Kuçuradi insan onurunu ise insanın insan olduğunun bilincinde olmasını ve değerinin farkına varmasını sağlayan bilgi olarak ifade etmiştir.

İnsan Hakları Evrensel Bildirgesi, Medeni ve Siyasal Haklar Uluslararası Sözleşmesi, Ekonomik, Sosyal ve Kültürel Haklar Uluslararası Sözleşmesi, Çocuk Hakları Sözleşmesi, İnsan Hakları ve Temel Özgürlüklerin Korunmasına Dair Sözleşme, Avrupa Sosyal Şartı gibi pek çok uluslararası belge, bireyi ve toplumu insan hakları alanında koruma altına almaktadır. Kişisel Verilerin Otomatik İşlenmesi ile İlgili Bireylerin Korunması Sözleşmesi gibi Avrupa Konseyi tarafından hazırlanan belgeler de insan haklarını koruma altına alan daha spesifik örnekler olarak değerlendirilebilir.

Gelecek on yıllarda hukuk disiplinin biyoetik disiplini ile kesişim kümesi oluşturması sonucu, olası uluslararası biyohukuk çalışma alanının ilkelerinin de aşağıdaki şekilde olacağı öne sürülmektedir;

- İnsan onuruna saygının en üstün ilke olarak kabul edilmesi,
- İnsanın, bilim ve toplumun menfaatinin önünde öncelikli olması,
- Biyomedikal faaliyetlerin öncelikle hastalara ve araştırmaya katılanlara zarar vermemesi ve eğer mümkün ise klinik uygulamada, hastanın durumunu tedavi etme ya da hastalığı önleme ve tanı koymaya katkıda bulunması gerekliliği,
- Hastaların ve araştırmaya katılanların özerkliğine saygı gösterilmesi ve bunun doğrudan sonucu olarak, herhangi bir biyomedikal girişim için aydınlatılmış onam alınması gerekliliği,
- Özellikle, uygun sağlık bakımı ve temel ilaçlara, sağlık hizmetine adil erişimin sağlanması,
- İnsan onuru ve insan haklarına saygıyı merkeze koyarak yürütmek şartıyla bilimsel araştırma yapma özgürlüğü,
- Tanımlanabilir kişilere ilişkin sağlık verisinin gizliliğinin korunması,
- Bir kimsenin özellikle genetiği ile ilgili sağlık bilgisini bilme ve bilmeme hakkı,
- Örselenebilir/savunmasız kişilerin özel olarak korunması,
- Genetik bilgi dahil, sağlık bilgisine dayanarak ayrımcılık yapmamak ve damgalamamak,
- İnsan bedeni ve parçalarının ticarileştirilmemesi,

- İnsanlığın kimliği ve bütünlüğünün korunması, özellikle, üreme amaçlı insan klonlama ve insan *germ-line* müdahalelerinin yasaklanması,
- Biyomedikal faaliyetlerden ortaya çıkan etik, hukuki ve sosyal konuları değerlendirmek üzere uygun aşamada, bağımsız, multidisipliner ve çoğulcu etik komitelerin oluşturulması,
- Özellikle gelişmiş ve gelişmekte olan ülkeler arasındaki uluslararası araştırmalarda, adaletin sağlanması.

Biyoloji ve tıp alanındaki gelişmeler, toplumu, insanlığı ilgilendiren yeni ve karmaşık etik sorunlara yol açmaktadır. Bu bağlamda, kullanılan teknolojilerin, ortaya çıkan yeni buluşların, araştırmaların insan hakları ve insan onuruna saygılı bir şekilde yapılması, yasalarla güvence altına alınması gerektiği konusu açıktır. Ancak, insan haklarının belirsizliği sağlık konusuna özgü olmayabilir ve aslında, söz konusu olan sınırlı kaynakların dağıtılması olduğunda ortaya çıkan bir sorunun çözümünde insan haklarının temel bir zorluk ile karşılaştığı söylenebilir (Cochrane, 2012).

Bununla birlikte, biyomedikal uygulamalar ve araştırmaların ortaya çıkardığı sorunların büyük kısmının sadece insan onuru yaklaşımı ile kesin çözüme ulaştırılamayacağı görüşü de bulunmaktadır. Tüm bu nedenlerle, insanın temel hak ve özgürlüklerini etkin şekilde korumanın, insan onurunu koruma yaklaşımının yanı sıra, aydınlatılmış onam, bedensel bütünlüğü koruma, ayrımcılık yapmama, mahremiyet gibi insan haklarını da içerdiği ölçüde mümkün olabileceği dile getirilmektedir.

## **Bilgi ve İletişim Teknolojileri**

Bilgi ve iletişim teknolojilerinin 1960'larda ortaya çıkması ve teknolojik gelişmelerin sağladığı imkanlar ile birlikte bilginin yayılımı da hızlanmıştır. Teknolojik gelişmelere bağlı olarak kişinin özel hayatı ve kişisel verilerinin korunması oldukça güçleşmiştir. Bu açıdan, teknolojik yeniliklerin gizliliği ortadan kaldıran bir tehdit unsuru olduğunu savunan görüşler olduğu gibi, gizliliğin korunmasının önceliği olduğunu dolayısıyla gizliliğin korunması için alternatif tüm yolların değerlendirilmesi gerektiğini, güçlü mekanizmalarla bu tehdidin zayıflatılabileceğini savunan görüşler de bulunmaktadır (Zeybek Ünsal & Örnek Büken, 2018).

Günümüzün yeni paradigması, veriye dayalı araştırmadır. Çok fazla sayıda kişinin verileri elektronik ortamda toplanıp depolanmaktadır. Bu veriler sağlık bakım hizmetlerinin geliştirilmesi ve araştırma olanaklarının artırılması için önemli bir potansiyele sahiptir. Günümüzde sağlığın iyileştirilmesi ve hastalıkların nedenlerini ortaya çıkarmak için araştırmalar artık bu büyük veri setlerine dayalı olarak yapılmaktadır. Literatürde “*Big Data*” olarak ifade edilen

büyük verinin temelde üç özelliğinin (3V) bulunduğu kabul edilmektedir; bu özellikler verinin çok büyük hacimli (*volume*) olması, çok çeşitli (*variety*) olması ve teknolojinin ilerlemesine paralel oranda hızlı (*velocity*) bir şekilde işlenmesi imkânına sahip olması olarak belirlenmiştir. Bazı araştırmacılar bu özelliklere ek olarak büyük verinin değerli olma (*value*) ve doğru olma (*veracity*) özelliğine de sahip olduğunu savunmaktadır (Zeybek Ünsal & Örnek Büken, 2018)

Sağlık özelinde büyük verinin tanımı ise AB Avrupa Komisyonu'nun 2016 tarihli raporunda yapılmıştır. İlgili raporda sağlıkta büyük veri; "Rutin veya otomatik şekilde elektronik olarak elde edilen ve saklanan büyük veri setleridir. Farklı amaçlar için yeniden kullanılabilir. Bu veriler sağlığı geliştirme ve sağlık sistemi performansını iyileştirmek amacıyla mevcut veri tabanlarıyla bağlantı kurar ve söz konusu verilerle birleşir. Büyük veri terimi belirli bir çalışma için toplanan verileri ifade etmemektedir." şeklinde tanımlanmıştır. Avrupa Konseyi, 23 Ocak 2017 tarihli rehberinde kişi ve grupların karar vermesine yönelik yeni ve öngördürücü bilgilerin ortaya çıkarılması amacıyla verileri analiz etmek için kullanılan yazılımların da büyük veri olarak anlaşılması gerektiğini belirtmiştir. Sağlıkta büyük veri hali hazırda farklı kaynaklardan toplanmış olup kullanıma hazır durumdadır; tele-tıp, akıllı telefon uygulamaları, tıbbi görüntüleme, biyolojik materyal/radyografik tetkikler, patolojik materyal/arşiv, elektronik sağlık kayıtları ve bu kayıtlara ilişkin notlar, sekanslama teknolojileri ile elde edilen DNA'lar, sosyal medya, sigorta talepleri araştırmaların veri kaynakları arasında sayılmaktadır (Zeybek Ünsal & Örnek Büken, 2018).

Bilgi ve iletişim teknolojisi (*ICT*), dijital bilgiye erişen, bu bilgiyi alan, saklayan, değiştiren ve ileten herhangi bir ürün ya da programı kapsayan geniş bir kavramdır. Sağlıkta *ICT* uygulamaları, sağlık bilgi teknolojileri (*HIT*) olarak da bilinmektedir. Sağlık bilgi teknolojileri, kullanıcıların farklı amaçlar için sağlık bilgisi toplamasına, paylaşmasına ve kullanmasına yardımcı olan farklı ürünler, teknolojiler ve hizmetlerdir (Shaw, Hines, & Kielly-Carroll, 2017)

Sağlık hizmetindeki nesnelerin interneti, bulut bilişim ve büyük veri teknolojilerinin birbirlerinin etkisini arttıracak şekilde entegre olması, bilgi ve iletişim teknolojileri temelli sağlık uygulamaları (e-sağlık, u-sağlık, tele-sağlık gibi) 'akıllı sağlık' kavramının ortaya çıkmasına neden olmuştur. (Kang, Park, Hwan Cho, & Lee, 2018).

Önümüzdeki 10-15 yıl içinde önemli etkileri olacağı düşünülen gelişen bilgi ve iletişim teknolojileri; duygusal programlama, çevresel zekâ, yapay zekâ, biyoelektronikler, bulut bilişim, geleceğin interneti (nesnelerin interneti), insan-makine arasında bağımlı yaşama, nöroelektronik, kuantum bilişim, robotik, sanal/arttırılmış gerçeklik olarak listelenmiştir. (Stahl, Timmermans, & Flick, 2017).

Rathanue Enstitüsü tarafından hazırlanan raporda bilgi teknolojileri üçüncü bir perspektif olarak ele alınmış; bilgi teknolojilerinin her yerde karşımıza çıktığı, kişisel ve sosyal yaşamın bütünüyle bir parçası olduğu belirtilmiştir (van Est et al., 2014). Bilgi teknolojilerinin davranışsal ve bilişsel bilimlerle birleştirilmesi, insan ve makine arasında daha iyi etkileşim sağlanması için olanaklar sunmaktadır. Bu yeni sistemlerin tanımlayıcı özelliği kullanıcılarla ve çevreye tepki verebilme yeteneğinin olmasıdır. Her tür araç ya da çevreye yerleştirilmiş küçük ve ucuz sensör teknolojisi kişilerin sürekli olarak davranış ve fizyolojilerini ölçmeye izin vermektedir. Bilgisayarın gücü ve yaygın internet ağ bağlantılarındaki gelişmeler sonucunda, cihazlarda ya da bulutta bulunan veriler analiz edilebilmekte ve başka uygulamalar ile paylaşılabilir (van Est et al., 2014).

Firmalar, insanların mental sağlığını ve çalışma ortamındaki refahını iyileştirmek için, çalışanların stres düzeylerini izlemek amacıyla giyilebilir teknolojiler üretmektedir. Kullanıcı bir bileklik takmakta, bu bileklik, kullanıcının stres düzeyini azaltmak için kalp atışı, hareketleri, vücut ısısı gibi sinyalleri ölçmektedir. Bu sinyaller daha sonra kullanıcının işle ilgili aktiviteleri hakkındaki bilgilerle birlikte, akıllı telefonu ve bilgisayarına gönderilmektedir. Giyilebilir teknolojinin amacı, kişileri istenmeyen strese sokan durumlarda vücudunun nasıl tepkiler verdiğini ölçerek, stresi ortaya çıkaran faktörler hakkında bilgi elde etmek ve kişiye bu durumlar ile baş etmesi için geri bildirimde ve tavsiyelerde bulunmaktır. Bu verilen geri bildirimler ile kişinin daha sağlıklı yaşaması veya iyi yaşam tarzlarını desteklemesi hedeflenmektedir. Bilgi teknolojilerinin bu uygulamaları, e-koçluk (*e-coaches*) olarak da adlandırılmaktadır.

Ancak bu teknolojiler, mahremiyet, toplandığı amaç dışındaki amaçlarla veri toplanması, elde edilen verinin kime ait olduğu, çalışanların işle ilgili olmayan davranışlarının da işveren tarafından kontrol edilebilmesi gibi sorunları da beraberinde getirmektedir. Tüketici ürünleri içine yerleştirilen sensörler aracılığı ile kalp atışı, duygular, uyku paternleri gibi büyük miktarlarda biyolojik veriler toplanabilmektedir. Bu bağlamda, sensörlerin kullanıldığı bir toplumda bedensel ve ruhsal bütünlüğün nasıl sağlanacağı, sosyal verilerde olduğu gibi, biyolojik verilerin de büyük firmalara karşılıksız verilir verilmeyeceği soruları gündeme gelmiştir.

Bununla birlikte, Rathaneu Enstitüsü'nün raporunda uzmanların duygu tanıma teknolojileri, yüz tanıma uygulamaları ve bu teknolojilerin Facebook profilleri ile bağlantısını kurmak için yoğun şekilde çalıştıkları belirtilmiştir. Gelecekte, bu üç özelliğin Google Glass'ta kullanılabilmesinin, her kullanıcının kim olduğumuzu, ne yaptığımızı, kimlerin arkadaşlarımız olduğunu ve nasıl hissettiğimizi görebileceği sonucunu doğuracağı ifade edilmiştir (van Est et al., 2014).

Nanoteknoloji ile de daha küçük ve daha etkili bilgisayar çipleri ve batarya teknolojilerinin gelişmesi sonucunda da insan bedenini kablosuz izleyebilme imkanı sunan araçlar giderek artacaktır. Kişilerin sağlığını izleyebilmeyi sağlayan kablosuz ağlar üzerinden büyük miktarlarda veri alışverişinin artması, kişilerden uygun onam alınmadan sağlık verisinin toplanması, analiz edilmesi ve kullanılabilmesine neden olmaktadır. Bu durum, gittikçe rafine edilmiş verilere dayanarak kişilerin değerlendirilmesi, tanınması ve sınıflandırılması olasılıklarının ortaya çıkması sonucunu doğurabilecektir (van Est et al., 2014).

Tüm bu gelişmeler düşünüldüğünde, sosyal medyanın, kameraların ve diğer sensörlerin olduğu ve verilerin toplanıp analiz edilebildiği bir ortamda mahremiyetin korunmasının nasıl sürdürülebileceği sorusu etik ve hukuki açıdan cevap aranılan sorulardır. Bu bağlamda ölçülmeyi, analiz edilmeyi ve yaşamımıza koçluk edilmesini reddetme hakkımız olup olmadığı, manipüle edilmeyi nasıl önleyebileceğimiz soruları da gündemdedir.

## Gelişen Bilgi ve İletişim Teknolojileri

### Yapay zeka

Yapay zekâ (YZ); bilgisayarimsal (*computational*) modeller kullanarak, gerekçelendirme, öğrenme, adapte olma gibi insanın bilişsel yetilerinin taklit edilmesi olarak tanımlanmaktadır. Öğrenme algoritmalarının hesaplanmasını hızlandırmak için çok yüksek etkinlikte bilgisayar grafik kart işlemcilerinin keşfedilmesi, bu kartların programlama gücünün artması ve büyük miktarlardaki verilere erişimin gelişmesine bağlı olarak 2010 yılından bu yana yapay zekada hızlı bir ilerleme olmuştur. Günümüzde yapay zeka, hastalıkların tanısında, kronik durumların yönetilmesinde, sağlık hizmetlerinin ulaştırılmasında ve ilaç keşiflerinde kullanılmaktadır.

Yapay zekâ; insan duygu, düşünce ve gerekçelendirmesini taklit eden makineleri ifade eden geniş yapay zeka; belirli işleri insanlar kadar ya da insanlardan daha iyi yapan teknolojileri ifade eden dar yapay zeka olarak sınıflandırılmaktadır (Jones et.al., 2018).

Son yıllardaki en başarılı yapay zeka türlerinden biri makine öğrenmesidir. Makine öğrenmesi, ampirik veriden elde edilen paternleri ya da karmaşık ilişkileri öğrenebilen ve doğru kararlar verebilen bilgisayar algoritmaları çalışmasıdır. Makine öğrenmesi problemleri, öğretici ile öğrenme ya da öğretici olmadan öğrenme olarak ayrılabilir. Yüz tanıma gibi, öğreticinin olduğu makine öğrenme algoritmasında, makineye çeşitli yüz örnekleri veya yüz dışındaki örnekler gösterilmektedir. Algoritma, gösterilen bu fotoğraflar üzerinden fotoğrafın yüz olup olmadığını tahmin etmeyi öğrenmektedir. Öğretici olmadan öğrenmede, gösterilen görüntülerin yüz ya da yüz olmadığı belirtilmemektedir (Jones et.al., 2018). Makine, bir işi tamamlamak için verilen belirli talimatları kodlamak yerine, büyük miktarlardaki veri ve al-



goritmalar kullanılarak eğitilmekte ve bu şekilde o görevi nasıl yerine getireceğini öğrenme becerisi geliştirmektedir. Bilinen algoritmaların aksine, makineye iyi cevabın ne olduğunu söyleyen veridir ve makine açıkça bir programlama olmadan öğrenmektedir.

Yapay zekanın özellikle sağlık alanında yaygın olarak kullanılmaya başlandığı ve çeşitli tıbbi durumların tanısını koyarken, insanlar kadar etkin olduğu ve hatta bazı durumlarda insandan daha etkili olduğu gösterilmiştir. Örneğin yapılan çalışmalar, intihar eğiliminin tahmin edilmesinde yapay zekanın insanlardan daha iyi olduğunu göstermiştir (Loh, 2018). Öte yandan, Houston Metodist Araştırma Enstitüsü, meme kanseri riskini doğru ve hızlı şekilde tahmin ederek hekimlere yardım etmesi için, bir yapay zeka yazılımı geliştirmiştir. Söz konusu yazılım, mammogramları analiz etmiş, hasta takip çizelgesini sağlık çalışanından 30 kat daha hızlı ve % 99 doğruluk oranına sahip tanı koyucu bilgiye dönüştürmüştür (Methodist, 2016).

IBM firmasının süper bilgisayarı olarak bilinen Watson da, beyin kanseri olan hastaların tümörlerinden elde edilen genetik bilgiyi taramak için kullanılmıştır. Watson, haftalarca ya da aylarca süren bu işlemi sadece dakikalara indirmiştir. Her hastanın sahip olduğu mutasyona ilişkin veriler daha sonra kişiye özel hazırlanmış klinik tedavi planı ile eşleştirilmektedir.

Bugün bilim insanları buluşlar yapabilen yapay zekâ da geliştirebilmektedir. Örneğin, IBM Watson, kanser için yeni ilaçlar bulmak amacı ile kullanılmakta, bu yapay zekanın kanser için bir gün tedavi geliştirebileceği umudu olduğu belirtilmektedir (Robinson, 2018).

Yapay zekadan farklı olarak, şu anda bilgisayarın işleme şekli mantıksal bir yaklaşım benimsemektedir. Bilgisayar, Google araması ile eşleşmek için milyonlarca web sayfası taramakta ya da bir satranç hareketini tahmin etmek veya bir satranç adımı önermek için binlerce satranç oyununu analiz etmektedir. Ancak insan zihnini taklit etmek için, bu işlemlerin dış dünya ile etkileşime geçerek tecrübe ve anlamlandırılmaya dayandırılarak yapılması gerektiği de belirtilmektedir.

Yapay zeka sağlık alanının yanı sıra, farklı alanlarda da kullanılmaya başlanmıştır. Örneğin, Japonya'daki bir sigorta şirketi, 34 çalışanını yapay zeka ile değiştirmiş, böylece verimliliğin %30 artacağına ve iki yıldan daha kısa sürede yaptığı yatırımın karşılığını alacağına inanmıştır. Washington Post gazetesi de 2017 yılında 850 yazının yayımlanması için yapay zeka muhabiri kullanmıştır (Loh, 2018). Avukatların yaptıkları işler dahi bu yeniliğin dışında kalmamış, 2017 yılının sonunda, bir yapay zeka İnsan Hakları Mahkemesi'nin vereceği kararı %79 doğruluk oranı ile tahmin etmiştir.

Yapay zeka pek çok akıllı telefon ve yazılımda çeşitli şekillerde bulunsa da, klinikteki kullanımı henüz sınırlıdır. Ancak bu alandaki çalışmalar hızla ilerlemeye devam etmektedir. Örneğin, nöral ağlar (bilgisayimsal model) kullanılarak paralize olmuş ve konuşamayan

hastaların ne söylemek istediklerini gösteren, beyinlerindeki sinyalleri doğrudan konuşmaya dönüştürebilen, beyin-bilgisayar arayüz çalışmaları yapılmıştır. Böylece, bir kaza ya da kriz sonucunda konuşma yetisini kaybetmiş olan kişiler, gözlerini kullanarak ya da başka küçük hareketler yaparak imleci ya da ekrandaki harfleri hareket ettirerek iletişim kurmak yerine, konuşmaları doğrudan yeniden oluşturulabilecektir. Bu teknoloji ile kişi, kendi konuşma tonunu ve ses tonundaki değişimini kendisi kontrol edebilecektir (Servick, 2019).

Sağlık alanında yapay zeka kullanımının uygulamada hızlı bir değişime neden olacağı, bu değişimin hasta hekim iletişim modelini dönüştüreceği ve bu doğrultuda nasıl bir sürecin işleyeceği tartışılan konular arasındadır.

Yapay zeka ile ilgili son dönemde yapılmış çalışmaları derleyen bir makaledeki örneklerle bakıldığında, tıbbın pek çok alanında yapay zekanın kullanıldığı görülmektedir. Örneğin oftalmolojide, diyabet hastalarından alınan fundus fotoğraflarını taramak için yapay zeka tabanlı derecelendirme (*grading*) algoritması kullanılmış, değerlendirmesi ve tedavisi için oftalmolojiste gönderilmesi gereken durumların yüksek güvenilirlik (%94) ve %98 hassasiyet ve belirlilik ile tespit edilmesi amaçlanmıştır (Loh, 2018).

Bir başka çalışmada, birden fazla hastanede yürütülen klinik araştırmada, derin öğrenme ve nöral ağ bağlantıları (*neural networks*) kullanan yapay zeka ajanlarının oftalmolojistler kadar iyi bir şekilde konjenital katarakt için doğru tanı koyabildikleri ve tedavi sunabildikleri gösterilmiştir (Loh, 2018). Deri kanseri ile ilgili olarak, araştırmacılar, 129450 klinik fotoğrafın olduğu veri setlerini kullanarak bir nöral ağı eğitmiş, yapay zekanın dermatologlar ile seviyesi karşılaştırıldığında aynı yeterlikte deri kanserlerini sınıflandırabildiği görülmüştür. Yapay zekanın, kardiyovasküler risk tahminini de önemli ölçüde doğru yaptığından söz edilmektedir. Makine öğrenmesi, 350.000 hastadan fazla kişinin rutin klinik verisini kullanarak, var olan algoritma ile karşılaştırıldığında 355 hastanın daha kardiyovasküler hastalık geliştirdiğini doğru şekilde tahmin etmiştir. Klinik nörobilim de yapay zekadan yararlanmaktadır. Yüksek risk grubuna giren 24 aylık çocuklarda otizm tanısı koymak için, 6 ila 12 aylık kişilerin beyninin MR görüntülerini kullanan derin öğrenme (*deep learning*) algoritması, bu kişilere %81 pozitif doğruluk oranı ile otizm tanısı konulabileceğini tahmin etmiştir (Loh, 2018).

Yapay zekanın yapabildiği şeyler arasında, radyoloji ve patoloji testlerinden alınan görüntüler üzerindeki paternleri tanıyabilmek de bulunmaktadır. Bu bağlamda, yapay zekanın açık biyobelirteçleri (*biomarker*) olmayan mental bozuklukları tahmin etmede hekimlerden daha iyi olup olmayacağı sorusu merak edilmektedir. Vanderbilt Üniversitesi Tıp Merkezi'ndeki araştırmacıların tasarladığı makine öğrenmesi, algoritmalarını hastaların elektronik sağlık ka-

yıtlarında uygulayarak, 2 yıl içinde bir kimsenin intihar girişiminde bulunup bulunmayacağını %80-%90 oranında, gelecek hafta intihar edip etmeyeceğini %92 oranında doğru tahmin etmiştir. Facebook da sosyal medya madenciliği ile elde ettiği verilere dayanarak kişinin intihar eğilimi olup olmadığını tahmin etmek için yapay zeka algoritmasını ne şekilde kullanacağını araştıran birkaç şirketten biridir (Loh, 2018).

Son yapılan çalışma ile yapay zeka tabanlı Face 2, akıllı telefon uygulaması kullanılarak, kişilerin yüzlerinin fotoğraflarının analiz edilmesi ile çocuklardaki nadir hastalıkların teşhisinin mümkün olabileceğini söylemektedir (Dolgin, 2019).

Tedavi açısından bakıldığında bir yapay zekanın hekimin yerini alıp alamayacağı sorusu merak edilmektedir. Bu konuda önemli gelişmelerden biri Çin’de yaşanmış, dünyada ilk kez hiçbir insan müdahalesi olmadan otonom implant ameliyatı robot diş hekimi tarafından başarı ile gerçekleştirilmiştir. Buna ek olarak, 2016 yılında akıllı cerrahi bir robot tek başına bir domuzun ince bağırsağını dikmiş ve operasyonda aynı görev kendilerine verilen insan cerrahlardan daha iyi dikiş attığı belirtilmiştir (Loh, 2018).

Yapay zeka, sağlık ve sosyal bakım hizmetlerindeki kaynakların dağıtımı ve planlanmasında kullanıma potansiyeli de taşımaktadır. Örneğin, İngiltere’de, Harrow Konseyi tarafından IBM Watson Bakım Yönetim Sistemi (IBM Watson Care Manager system)’nin maliyet etkinliğinin artırılması için pilot uygulama yapılmıştır. Söz konusu uygulama ile kişilerin kendi ihtiyaçları ve kendilerine ayrılan bakım bütçesine göre, bakım sağlayan kişilerle eşleşmesi sağlanmaktadır Yapay zeka aynı zamanda hastaların deneyimlerini iyileştirmek amacı ile de kullanılmaktadır. Bu amaç doğrultusunda İngiltere, Liverpool’da bulunan Alder Hey Çocuk Hastanesi, IBM Watson ile birlikte bilişsel hastane oluşturmaya çalışmaktadır. Bu hastanede, hastalarla iletişimi kolaylaştıran bir uygulama bulunacak, vizitelerden önce hastanın anksiyetesi tespit edilebilecektir. Böylece, klinisyenlere hastalarına uygun tedavi verme konusunda bilgi vererek onlara yardımcı olacaktır (Nuffield Council on Bioethics, 2018).

Yapay zeka, büyük ve karmaşık veri setlerindeki paternleri daha hızlı ve doğru şekilde tespit etmek ve analiz etmek için de kullanılmaktadır. Örneğin, İngiltere’de Kanser Araştırmaları Enstitüsü’nün canSAR veri tabanı, bilimsel araştırmalardan elde edilen bilgiler ile hastalardan aldığı genetik ve klinik veriyi birleştirmekte, kanser ilaçları için yeni hedeflerle ilgili tahminlerde bulunmak amacıyla yapay zeka kullanılmaktadır. Klinik araştırmalara katılması uygun olan hastaları belirlemeye yardımcı olması nedeni ile, sağlık hizmetinde kullanılan yapay zeka sistemlerinin tıbbi araştırmalar için de değerli olabileceği düşünülmektedir. Yapay zekanın hastalıkların tanı koymada yardımcı olma potansiyeli de bulunmakta, bu amaçla İngiltere’de

bazı hastanelerde denenmektedir. Kişisel sağlık değerlendirmesi sunan ve evde bakım tavsiyesinde bulunan yapay zeka uygulamaları piyasada yerini almıştır. Örneğin, Ada Sağlık Arkadaşı uygulaması konuşma robotu (*chat-bot*) yönetmek için yapay zeka kullanmaktadır. Bu uygulama kullanıcının semptom bilgileri ile diğer bilgilerini birleştirmekte ve olası tanıların neler olabileceğini söylemektedir (Nuffield Council on Bioethics, 2018).

Nuffield Biyoetik Konseyi'nin yapay zeka ile ilgili çalışmasında, klinikte yapay zekanın kullanılması olasılığının olduğu alanlar, medikal görüntüleme, ekokardiyografi, nörolojik durumların taranması, ameliyatlar olarak belirtilmiştir. Çalışmada, medikal görüntüleme ile belirli süredir sistematik olarak veri toplandığı ve saklandığı bu nedenle yapay zeka sistemlerinin eğitilmesinde kullanılmak için hazır oldukları dile getirilmiştir. Yapay zeka, pnömoni, meme ve cilt kanserleri ile göz hastalıkları gibi durumları tespit etmede umut vericidir. Parkinson hastalığı gibi nörolojik durumların semptomlarını izlemek, bunları tespit etmek ve psikotik episodları tahmin etmek için konuşma paternlerini analiz eden yapay zeka araçları da geliştirilmektedir. Yapay zeka tarafından kontrol edilen robotik araçlar da, yaraları kapatmak için düğüm atmada, laparoskopik cerrahide belirli işleri yapmak için araştırmalarda kullanılmıştır (Nuffield Council on Bioethics, 2018).

Bununla birlikte, İngiltere'de tüberküloz hastalarında yapılan bir araştırmada, hastanın verilen ilaç ve tedaviye gösterdiği uyumu gözlemek ve desteklemek için yapay zeka uygulamaları kullanılmış, araştırmanın sonuçları umut verici olmuştur. Yapay zeka (*artificial intelligence; AI*) ile ilgili olarak, şirket düzeyinde veri kontrolörlerini belirli veri uygulamalarında desteklemek için etik komiteler oluşturulmasını öneren bir yaklaşım bulunmaktadır. Çoğu şirket artık kritik projeleri konusunda danışmanlık almak için şirket içinde ve dışında komiteler oluşturmuşlardır. Bu yaklaşıma göre, komiteler, yapay zeka ile ilgili temel hakların uygulanması gibi sosyal konuları inceleyebileceği gibi, etik konularda uzman bir komite gibi de hareket edebilir. Öte yandan, diğer danışma kurullarında olduğu gibi, yapay zeka etik komitelerinin oluşturulması da bağımsızlık, komitenin içişleri ve dış işlerindeki durumu ve çıkar çatışmalarını en iyi engelleyen uygulamaların neler olabileceği yönünde soruları da beraberinde getirmektedir (Council of Europe, 2019).

## **Sağlıkla İlgili Nesnelerin İnterneti**

Nesnelerin interneti (*Internet of Things, IoT*), veri alıp gönderen, internete bağlı çok sayıda nesne ve cihazları tanımlamak için kullanılan bir kavramdır (UNCTAD UNCoTaD, 2016). Bu kavram ilk olarak Kevin Ashton tarafından 1999 yılında ortaya atılmış, Radyo frekansla tanımlama (*radio frequency identification, RFID*) teknolojisi ile eşsiz olarak tanımlanabilen birbirine bağlı nesneler için kullanılmıştır.

Gelişen bir teknoloji olan nesnelerin interneti ile artık internet sadece dünya çapında bir ağ üzerinden insanların bilgisayar kullanarak birbirleriyle iletişim kurduğu bir yer değil; makinelerin, cihazların veya araçların elektronik olarak kendi çevreleri ile iletişim kurduğu bir platformdur. Nesnelerin interneti, herhangi bir insan etkileşimi olmadan nesnelere veri transferi olarak da tanımlanmaktadır (Imison, Castle-Clarke, Watson, & Edwards, 2016)

RFID, nano, kablosuz sensörler ve akıllı teknolojiler, 2005 yılında yapılan Dünya Bilgi Toplumu Zirvesi'nde nesnelerin interneti (*Internet of things, IoT*) kapsamında dört önemli teknoloji olarak ifade edilmiştir (Tzafestas, 2018).

Sağlıkla ilgili nesnelerin interneti olarak adlandırılan teknolojiler, sağlığın yönetilmesi, hastalıkların önlenmesi, hastaların fonksiyonlarının izlenmesi (eş zamanlı tele izleme), tedavilerin test edilmesi, kişinin sağlık durumunun eş zamanlı olarak takibi, sağlık araştırmaları için veri toplama gibi konularda artan önemli bir role sahiptir. Noninvaziv eş zamanlı hasta takibi sağlayan *IoT* teknoloji örnekleri firmalar tarafından üretilmeye başlanmış, Amerika'da pek çok akıllı sağlık cihazı *FDA* tarafından onaylanmıştır. Bu örnekler arasında, Medtronic tarafından üretilen Mobil Hasta Yönetim Sistemi bulunmaktadır; bu sistem ile ölümcül olmayan kardiyak aritmilerin tespiti için takibi gereken hastaların fizyolojik verisi ölçülmekte, kaydedilmekte, saklanmakta ve periyodik olarak transfer edilmektedir. Bu sistem, giyilebilir sensör kullanmakta, hastanın elindeki alıcı verici (*transceiver*) ile güvenli bir sunucuya bilgiler gönderilmektedir. Buna ek olarak, implante edilebilen kardiyovasküler görüntüleme cihazı da *FDA* tarafından onaylanmıştır. Bu cihaz ile hastanın kalp ritimleri sürekli olarak takip edilebilmekte, toplanan veriler bluetooth aracılığı ile akıllı telefon uygulamalarına gönderilmektedir. Cihaz, hastanın göğsünün derisinin hemen altına fazla invaziv olmayan bir şekilde ayakta yerleştirilebilmektedir. İsviçre'deki Sensimed firması ise, hastalarda glokom hastalığının gelişimini izlemek için hekimlere yardım eden bir kontakt lens geliştirmiştir. İçine mikrosensör yerleştirilen yumuşak tek kullanımlık silikon bir lens ile bir gün için gözle ilgili spontan/kendiliğinden olan boyut değişimi sürekli olarak kaydedilmektedir (Kang, Park, Hwan Cho, & Lee, 2018).

Tüketiciye sunulan sağlık uygulamalarının yüzbinlerin üzerinde olduğu 2015 yılında yayımlanan bir çalışmada belirtilmiştir. Mobil internet dalgası 2000'li yıllarda iki milyar kullanıcıya birbirine bağlamış ve bu sayı hızlı bir artış göstermiştir. Nesnelerin interneti 50 milyar nesneyi 2020 yılı itibari ile internet ile birbirine bağlayacak bir potansiyele sahiptir (Tzafestas, 2018).

Tıp ve bilgi teknolojilerinin etkileşiminin, sağlık bakım sunumunu dönüştüreceği; *IoT* ile ilgili teknolojilerin %40'ının 2020 yılı itibariyle sağlıkla ilgili olacağı ve 117 milyar dolarlık

bir pazar oluşturacağı öngörülmektedir. Dönüşen bu sistemin içinde, örneğin diabet hastalarının bir kimlik kartı olacak, bu kart ile hastanın elektronik sağlık kayıtlarının, bulgularının, tıbbi öykülerinin, reçete edilen ilaçların ve laboratuvar sonuçlarının saklandığı güvenli bir buluta bağlanılacaktır. Hekimler ve hemşireler bu kayıtlara tablet ya da masaüstü bilgisayarlarından kolayca erişebileceklerdir (Dimitrov, 2016).

Hassas tıp, genom bilimleri ile başlamış olup, analiz ve yorum için çok boyutlu veri sunan omik platformları (omics platforms) ile gelişmeye devam etmektedir. Bu bağlamda, Intel ile Oregon Sağlık ve Bilim Enstitüsü, 2015 yılında ortak bir proje başlatarak yüksek performanslı analiz platformu olan Kanser Bulut Ortaklığını kurmuştur. Bu platformda, kanser araştırmaları için kullanılacak olan özel tıp verileri toplanmakta ve güvenli bir şekilde saklanmaktadır. Platform kanser ile başlatılmış olsa da Intel, Parkinson gibi hastalıkların tedavisi üzerine çalışan enstitüler ya da diğer enstitülerin federe bulut ağını da paylaşımına açmak istemektedir (Dimitrov, 2016).

Nesnelerin interneti üzerinden, kişinin kalp atışı, solunumu, kan oksijen saturasyonu, vücut ısısı, kan şekeri, vücut ağırlığı gibi parametreler elde edilmekte, bunlarla birlikte kişinin modu, hareket ve uyku durumuna ilişkin veriler de toplanabilmektedir. Bu elde edilen veriler sonucunda, tanı ve tedaviler geliştirilerek hastalıklar önlenmektedir. Örneğin, hareket kontrolörü olarak oyunlarda kullanılan 'The Myo', ortopedide, kemik ya da kırıkta kırıldıktan sonra egzersize ihtiyacı olan hastalarda kullanılmaktadır. Myo'nun yardımı ile hastalar kendi süreçlerini gözleyebilmekte, hekimler de hastanın hareket açılarını ölçebilmektedir. Bir başka örnek, FDA tarafından onaylanmış olan Zio Yama (*patch*)'dır. Bu yama ile kalp atış hızı ve EKG ölçülmektedir. İlaç firmaları da geleneksel ilaç merkezli yaklaşımdan uzaklaşarak IoT'den yararlanmaya başlamıştır (Dimitrov, 2016). Örneğin Glaxo firması, elektrosötikler, sinirlerin mikrostimulasyonu ile çalışan biyoelektrik ilaçlara yatırım yapacağını duyurmuştur. Johnson&Johnson firması da Google ile bir takım oluşturarak, robotik cerrahi geliştirmektedir. Aynı zamanda kan basınç monitörleri gibi giyilebilir cihazlar konusunda Philips ile iş birliği yapmaktadır. Novartis de yine Google ile birlikte, akıllı lensler, kan glikoz seviyesini ölçen giyilebilir cihazlar gibi sensörler üzerine çalışmaktadır.

Nesnelerin internetinin bir örneği olan giyilebilir teknolojiler; kliniğin dışında kişilerin sağlık durumunu sürekli izlemeye ve sağlık durumlarını öngörmeye olanak sağlayan, kişinin doğrudan taktığı ya da gevşek olarak bedenine iliştirilmiş araçlardır. Giyilebilir teknolojilerin kaynağında, üretilen veriler bulunmakta, çeşitli taraflar bu verileri birleştirmeye ve veri akışını kontrol etmeye çalışmaktadır (Dimitrov, 2016). Sention bu örneklerden birini oluşturmakta, hastaların evlerinde taktıkları sensörler aracılığı ile toplanılan bilgi yapay zeka kullanılarak analiz edilmektedir. Bu aracın verdiği sinyallerle hastanın kötüleştiği anlaşılmakta ve erken

müdahale yapmak amaçlanmaktadır. Böylece hastaların hastaneye gitmesi de önlenmek istenmektedir. Bu teknolojiler ile risk altındaki hastaların hastane ortamından uzakta, evlerinde sürekli olarak gözlenmeleri mümkün olmakta, acil bir durum geliştiğinde kendisi ile ilgilenen sağlık profesyoneline durumu bildirilebilmektedir. Hastanede uzun süre kalması istenen kronik hastalıklara sahip kişilerin ise, durumlarının evde gözlenmesi hastaneye gitme oranlarını ve maliyetini azaltmaktadır.

Ancak söz konusu teknolojilerin sağlık alanına entegre edilebilmesinin sınırlılıkları ve zorlukları bulunmaktadır. İnternet ağı üzerinde birbirine bağlanan her nesne ve her insanın verilerinin her an nesnelerin internetinin bir parçası olmasının ortaya çıkardığı zorluklar arasında; internet bağlantısının kopması durumunda ne olacağının belirsizliği, *IoT* cihazlarının, ağ yönlendiricilerinin ve bulut bağlantılarının onarımından kimin sorumlu olacağı ya da güvenilir olup olmayacakları, *IoT* hizmetinin bulut bölümü heklense (*hacking*) de evdeki ağ bağlantısına erişimi engellemenin mümkün olup olmadığı soruları gündemdedir. Bununla birlikte, hizmet sağlayıcısının önemli yaşamı destekleyen *IoT*'lerde bir arıza ile karşılaşması ve cihazın çalışmaması, cihazın kullanıcının onamı olmadan ya da istenmeyen şekilde hareket etmesi durumları ile de karşılaşılabilir. Aynı zamanda, *IoT* cihazları ile toplanan verinin kime ait olacağı, *IoT*'nin veri toplaması gereken durumlar olup olmadığı, kullanıcı artık *IoT* kullanmak istemediğinde onamından vazgeçip vazgeçemeyeceği da temel sorulardır. Bunun yanı sıra dijital ayırım (*digital divide*) olarak ifade edilen ve akıllı cihazları kullanamayan ya da bu cihazların nasıl kullanıldığına dair bilgisi olmayan kişilere sağlık hizmeti sunumunda ne tür farklar ortaya çıkacağı sorusu da yanıt beklemektedir (Tzafestas, 2018).

## **Bilgi İletişim Teknolojileri ile Gelişen Tıp ve Ortaya Çıkan Etik Tartışmalar**

Biyoteknolojiler, nanoteknolojiler ve nöroteknolojilerinin, bilgi ve iletişim teknolojileri ile etkileşimi kişisel veri tanımını güçleştirmekte, verinin yönetimi ve transferi ile ilgili karmaşık problemleri de beraberinde getirmektedir. Bu bağlamda, yapay zeka, beyin görüntüleme teknolojileri, giyilebilir sensörler gibi cihazların ortaya çıkardığı mahremiyet sorununa ilişkin, mahremiyet ile ilgili hukuki düzenlemelerin kapsamının bu teknolojiler bağlamında genişletilmesinin etkin hukuki koruma sağlamak açısından önemli olduğu düşünülmektedir.

Bilgi iletişim teknolojileri ile veri koruma arasındaki ilişkiyi gösteren en yakın örnekler bulut bilişim, nesnelerin interneti ve büyük veri analitiği başlığı altında sayılmıştır. Bulut hizmetlerinin karmaşıklığı, bazı ülkelerin bu teknolojiye özel yasalar hazırlamasına neden olmuş, örneğin Kore Cumhuriyeti'nde bulut bilişime özel yasa teklifi sunulmuştur (UNCTAD, 2019).



Gelişen bilgi ve iletişim teknolojilerinde öne çıkan bir kavram olan mahremiyet, 19. yüzyılın sonlarından bu yana gittikçe hukuki bir kavram haline gelmiş temel bir insan hakkıdır. Mahremiyetin sorunlarının ortaya çıktığı öne çıkan örneklerden bazıları, *RFID*, Facebook gibi sosyal ağlar ve kurulan büyük biyobankalardır. Mahremiyet kavramı farklı şekillerde tanımlanmakta, farklı kişiler tarafından mahremiyete farklı anlamlar yüklenmektedir. Avrupa Komisyonu, Avrupa Birliği'nin yedinci çerçeve programı kapsamında 2010 yılında Mahremiyet ve Gelişen Bilim ve Teknolojiler (PRESCIENT) adı ile başlattığı mahremiyetin yeniden kavramsallaştırılmasını amaçlayan projesinde, gizliliği temel unsur olarak ele almış, gelişen teknolojilerin nasıl bir etkiye sahip olduğunu değerlendirmek için uygun yöntemler geliştirmeyi hedeflemiştir (Friedewald, Wright, Gutwirth, & Mordini, 2010).

Mahremiyet, kişinin biyolojik materyal gibi kendi bedeni ile ilgili bilgilere ve kişisel bilgilerine erişimi kontrol etme hakkını içermektedir. Mahremiyet hakkı, kişinin genetik kodları, biyometrik verileri gibi beden fonksiyonları ve özelliklerini gizli tutma hakkı olarak da tanımlanmaktadır. Mahremiyetin bir başka türü olan haberleşme gizliliğinin amacı ise, e-posta yolu dahil haberleşmeyi, haberleşmeyi dinlemek için böcek ve yönlentmeli mikrofon kullanmayı, telefon ya da kablosuz iletişimi engellemeyi, kişinin kendisi dışında e-postasına dışarıdan erişimi ya da e-posta mesajlarının kaydedilmesini önlemektir. Gelişen teknolojilerin birbirine yaklaşması göz önüne alındığında, bir eylem ile birden fazla mahremiyet türleri ihlal edilebilmekte, bu nedenle sadece kişisel verilerin ya da elektronik haberleşme özgürlüğünün engellenmesini koruyan mevzuat oluşturmak yeterli görülmemektedir. Aynı zamanda, yeni ve gelişmekte olan teknolojilerin süprizlerle dolu olmasının bir sonucu da farklı teknoloji uygulamalarının farklı mahremiyet türlerini ihlal etmesi şeklinde kendini göstermesidir. Bir başka ifadeyle, mahremiyete ilişkin yeni ve öngörülemez problemlerin ortaya çıkması her yeni teknolojinin olası bir sonucudur. Örneğin, yeni nesil sekanslama teknolojileri ile kişinin hassas veri olarak nitelendirilen kişisel bilgileri elde edilmektedir. DNA sekansları; kişinin cinsiyeti, cinsel yönelimi, etnisitesi, fiziksel ve zihinsel sağlığı ile belirli davranış eğilimlerini gösterebilmektedir. Tüm genom DNA sekanslama tekniğinin, kişinin istediği şekilde, takip edilmeden ve izlenmeden yer değiştirme ve seyahat özgürlüğünü kapsayan konum gizliliğini ihlal etme riski de bulunmaktadır. Kişinin DNA profili ile belirli bir konumdaki DNA örnekleri karşılaştırılarak, bir kişinin nerede bulunduğu tespit edilebilmektedir (Friedewald, Wright, Gutwirth, & Mordini, 2010).

Kişisel verilerin korunması, mahremiyet hakkından hem daha geniş hem de daha spesifik olarak tanımlanmaktadır (Friedewald, Wright, Gutwirth, & Mordini, 2010). Bu hakkın gizliliği daha geniş tanımlanmasının nedeni olarak, kişisel verilerin korunmasının sadece maddi olarak



mahremiyeti korumayı amaçlamadığı, bunun dışında ifade özgürlüğü, din ve vicdan özgürlüğü, bilginin serbest dolaşımı ve ayrımcılık yapmama ilkesini de korumayı amaçladığı gösterilmektedir. Bunun yanı sıra, kişisel veriler her işlendiğinde uygulandığı için bu hakkın spesifik olma özelliği gösterdiği belirtilmektedir (Friedewald, Wright, Gutwirth, & Mordini, 2010).

Kişisel verilerin korunması hakkı özel hayatın gizliliği kapsamında ele alınmaktadır. Bu çerçevede, BM İnsan Hakları Evrensel Beyanamesi'nin 12. ve Medeni ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17. maddelerinde özel hayatın gizliliği düzenlenmiştir. Avrupa İnsan Hakları Sözleşmesi ve Avrupa Birliği Temel Haklar Şartı da özel hayatın gizliliği ile ilgili hükümler içermektedir. Kişilerin özel hayatının gizliliği, kişilerin kendi kaderini belirleme (*self-determination*) özgürlüğü, farklı olma hakkı, seçim yapma özgürlüğü, cinsiyeti, sağlığı ve sosyal davranışlarında özerk olması vb. ile ilgili hakları korunmaktadır (Friedewald, Wright, Gutwirth, & Mordini, 2010).

BM'nin gizliliğin korunmasına yönelik yapmış olduğu çalışmalar, bu alandaki rolünü de güçlendirmiştir. BM ilk olarak Dijital Haklar konusunda açıklamasını yayınlamış, daha sonra özel hayatın gizliliği konusunda özel bir raporör görevlendirmiştir (UNCTAD, 2016). BM Genel Kurulu, 2013 yılında aldığı bir karar ile haberleşmenin önlenmesi ve gözetlemenin insan hakları üzerinde olumsuz etkileri olmasının derin kaygıya yol açtığını açıklamıştır. Karara göre, çevrimiçi olmayan kişilerin hakları nasıl korunuyorsa, çevrimiçi olan kişilerin hakları da aynı derecede korunmalıdır. Bu kararın ardından 2014 yılında BM'nin yayınladığı detaylı raporda (A/HRC/27/37) ise, IDPC, BM ve Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin (108 Sayılı Avrupa Konseyi Sözleşmesi) yeni teknolojilerin ortaya çıkardığı sorunları karşılamakta yetersiz kaldığı belirtilmiştir (UNCTAD, 2016).

Rapora göre, OECD'nin 2013 tarihli kılavuzu orta düzeyde koruma sağlamaktadır. Buna ek olarak, AB Veri Koruma Tüzüğü'nün de koruma derecesinin orta düzeyde kaldığı ifade edilmiştir. Ancak, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 Sayılı Avrupa Konseyi Sözleşmesi), yeni bilgi ve iletişim teknolojilerinin kullanımı sonucunda ortaya çıkan sorunlara çözüm getirmek ve Sözleşmenin etkin uygulanmasını güçlendirmek amaçları doğrultusunda modernleştirilmiştir. Şeffaflık, orantınlık, hesap verebilirlik, veri azaltma, tasarım gereği gizlilik (*privacy by design*) gibi ilkeler, veri koruma mekanizmasının temel elementleri olarak kabul edilmiş, sözleşmeye entegre edilmiştir (Council of Europe, 2019).

Medeni ve Siyasal Haklar Uluslararası Sözleşmesi'ndeki hükme göre, hiç kimsenin özel, aile veya haberleşme hayatına keyfi ya da hukuka aykırı bir şekilde müdahale edilemez.

Bununla birlikte, onur ya da itibarına hukuka aykırı saldırıda da bulunulamaz. Düzenlemeye göre herkes, böyle bir müdahale ya da saldırıya karşı yasalar ile korunma hakkına sahiptir. Diğer uluslararası insan hakları metinleri de benzer hükümler içermektedir.

Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde gizliliğin farklı bir formu olan kişisel verilerin korunmasını isteme hakkı tanınmıştır. Bu maddenin oluşumu, OECD tarafından 1980 yılında hazırlanmış olan özel hayatın gizliliğinin korunması ve kişisel verilerin sınır ötesi akışı hakkındaki kılavuza, Avrupa Konseyi'nin 1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sürecinde Kişilerin Korunması Sözleşmesi ve 1995 tarihli AB Veri Koruma Direktifi ile birlikte Avrupa Birliği düzenlemelerine dayanmaktadır (Friedewald, Wright, Gutwirth, & Mordini, 2010).

Avrupa Parlamentosu temel bir hak olan verilerin korunması hakkını korumak ve üye ülkeler arasında kişisel bilgilerin serbest dolaşımını güvence altına almak amaçları ile 1995 yılında 95/46/EC sayılı Kişisel Verilerin Korunması AB Direktifi'ni kabul etmiştir. Gerçek kişilerin temel hak ve özgürlüklerinin korunması amacı ve verilerin güvenli serbest dolaşımının sağlanması için AB üye ülkelerin ulusal düzenlemeler yapması istenmiştir. AB merkezli şirketler de veri işleme ve transferi için belirlenen kurallara uygun hareket etmek durumundadır. Kullanıcılar kişisel verilerinin nasıl kullanıldığı, toplanılan ve işlenen verilerin nasıl paylaşıldığı ile ilgili bilgilendirilme hakkına sahiptir. Bununla birlikte, veri sahibinin kişisel verilerinin düzeltilmesini ya da silinmesini isteme hakları da bulunmaktadır. AB Veri Koruma Direktifi (95/46/EC), daha sonra GDPR'ın 25 Mayıs 2018 tarihinde yürürlüğe girmesi ile yürürlükten kaldırılmıştır (Curtiss, 2016).

Yeni teknolojilerle kişisel bilginin toplanması ve kullanılmasının korunmasının daha zor hale gelmesi üzerine AB, bu direktife ek düzenlemeler getirmiştir. Bu bağlamda, "Mahremiyet ve Elektronik Haberleşme Direktifi" 2002 yılında oluşturulmuş, elektronik posta (e-posta), telefon ile haberleşme, trafik verisi, arayan kişinin numarasının korunması konularına değinilmiştir. Bu direktif veri saklama direktifi ile değiştirilmiş, veri için minimum ve maksimum saklama tarifesi belirlenmiştir.

Çerez direktifi olarak da bilinen "Mahremiyet ve Elektronik Haberleşme Direktifi"ni değiştiren 2009 tarihli bu direktif ile, önceden onam alınması şartı ile (*opt-in*), bir *web* sitesinin çerez kullanımına izin verilmiştir (Curtiss, 2016). Tüm dünyada, kapsamlı, sektörel, kendi kendine denetleme (*self-regulation*) ve teknoloji tabanlı olmak üzere dört temel veri koruma modeli kullanılmaktadır. Kapsamlı veri koruma yasaları, kamu ve özel sektördeki kişisel verilerin toplanması, kullanılması ve paylaşılmasını düzenlemektedir. Sektörel modelde, kişisel

veriler, tıbbi kayıtlar ya da kredi kayıtları gibi belirli bir endüstri sektörüne özgü kişisel verileri ele alan yasalar yürürlüğe koyarak korunmaktadır. Kendi kendini denetlemeyi esas alan model ise bir şirketin, endüstrinin ya da bağımsız bir organın kendi etik kurallarını oluşturarak kişisel verileri korumasını esas alır. Teknoloji tabanlı modelde de idari önlemlerin önemlerini görece azaltan, alternatif koruma yöntemi olarak şifreleme gibi teknolojik önlemler kullanarak kişisel veriler korunmaktadır. AB'nin benimsediği yaklaşım 1995 yılından bu yana kapsamlı model olup, Genel Veri Koruma Yönetmeliği (*GDPR, General Data Protection Regulation*) ile bu yaklaşım benimsenmeye devam etmiştir (Curtiss, 2016).

Özel hayatın gizliliği kapsamında ele alınan kişisel verilerin korunması hakkı ile ilgili Avrupa İnsan Hakları Mahkemesi'nde görülen davalarda; gerçek kişilerin, hak ihlallerini, bu ihlalden doğan zararı somut bir şekilde ortaya koymaları gerektiği yaklaşımı benimsenmiştir. Ancak devlet güçlerinin ve istihbarat kurumlarının elde ettiği kişisel verilerin kişinin özel hayatını ihlal ederek doğrudan somut bir şekilde kişiyi zarara uğrattığını ispatlamak güçtür. Buna bağlı olarak, veriye dayalı teknolojiler ile kişinin özel hayatına doğrudan müdahale edildiğinin ve somut bir zarara uğradığının gösterilmesinin işin doğası gereği zor olması, Avrupa İnsan Hakları Mahkemesi'nin bu yaklaşımından uzaklaşmasına neden olmuştur (Van der Sloot, 2017). Bu tür davalarda somut ihlali ve bu ihlalden zarar meydana geldiğini ispatlamanın, kişinin hak araması önünde bir engel olduğu düşünülmüştür. Bu nedenle, Avrupa İnsan Hakları Mahkemesi artık somut ihlal veya kişisel zararın doğduğunun gösterilmesi şartını aramamaktadır (*non-interference* ilkesi). Bunun yerine güç ilişkilerine ve gücün keyfi kullanılıp kullanılmadığına, egemenlik kurmama ilkesine (*non-domination* ilkesi) odaklanmaktadır. Bu ilkeye göre kişi, ancak yaşamına dışarıdan kontrolsüz müdahale yoksa özgürdür. Yaklaşımındaki bu değişimin, Avrupa İnsan Hakları Mahkemesi'nin gelecekte klasik bir mahkeme gibi değil, Avrupa Anayasa Mahkemesi gibi görev yapmasına neden olabileceği öngörülmüştür (Van der Sloot, 2017).

Nesnelerin interneti, büyük veri, yapay zeka gibi teknolojiler ve 5G ağları ile bağlantı-sallığın artması sonucu büyük yararlar ile birlikte veri sahipleri için riskler de taşımaktadır. Özellikle veri korumaya ilişkin yönetim biçimlerindeki zorluk; potansiyel yararları göz ardı edip sınırlandırmadan, ortaya çıkan riskleri yönetmede karşımıza çıkmaktadır. Sınır ötesi veri transferi konusunda da çeşitli yaklaşımlar bulunmakta, bu konu ile ilgili bir yasa olması gerektiği uluslararası düzeyde kabul edilmektedir. Amerika Birleşik Devletleri'nde olduğu gibi, ulusal düzeyde ise bazı ülkelerde yabancı bir ülkeye kişisel verilerin transferi konusunda herhangi bir sınırlama yoktur (UNCTAD, 2016).

Literatürde, gelişen bir teknoloji olan nesnelerin interneti ile ilgili hukuki düzenlemelelerin, nesnelerin internetinin işleyişinde yer alan üç bileşeni içermesi gerektiğini öne süren bir çalışma bulunmaktadır. Buna göre hukuki düzenlemeler, internet ile birbirlerine bağlanan ci-

hazların, ağlar ve güvenliklerinin, internet ile bağlı cihazlarla ilişkili verilerin düzenlenmesini içermelidir (Tzafestas, 2018).

Konumuz bağlamında, yapay zeka ve robotların hukuku konusunda bir çalışma başlatan ilk hukuki kurum Avrupa Parlamentosu olmuştur. Parlamento, 2017 yılında robotik hakkında Medeni Yasadaki kurallar üzerine Avrupa Komisyonu'na öneriler getiren bir karar almıştır. Öneriler arasında, akıllı robotlara özgü hukuki bir statü vermek, AB'de tüm robotların zorunlu kayıt olacağı bir sistem ile akıllı robotlara sigorta yapmak bulunmaktadır. Hukuki düzenlemeler ile ilgili yeni evrimsel bir adım atılmakta, sorunlara cevap niteliğinde olan düzenlemeler yerine akıllı düzenlemelere doğru yön değiştirilmektedir.

Avrupa Komisyonu da 24 Nisan 2018 tarihinde "Artificial Intelligence for Europe" ismi ile bir bildiri yayınlamıştır (Zanfır-Fortuna, 2018).

Komisyonun belirlediği stratejideki temel hedefler;

- Yapay zeka uygulamalarının geliştirilmesi için finansal destek sağlanması,
- Veriyi araştırmacılara erişilebilir hale getirmeye yönelik girişimde bulunmak,
- Yapay zekanın işgücündeki etkilerini analiz ederek, yapay zeka çağında iş gücü ile başa çıkabilecek şekilde üye ülkelerin iş gücü hazırlamasını desteklemek için bir çerçeve oluşturmak,
- 2018 yılında kabul edilen yapay zeka etik kılavuzunun yanı sıra, uygun bir etik ve hukuki çerçeve oluşturmak,
- Üye ülkeler ve araştırma enstitüleri ile işbirliği yapmak için altyapı oluşturmak olarak belirlenmiştir.

AB üyesi olan Fransa 29 Mart 2018 tarihinde yapay zeka (YZ) ile ilgili ulusal stratejisini açıklamıştır. Almanya, akademi, endüstri ve devlet arasında stratejik bir diyalog geliştirmek için öğrenme sistemleri konusunda bir platform oluşturarak otomatik ve bağlantılı sürüş etiği hakkında bir rapor sunmuştur. Finlandiya da benzer şekilde stratejisini açıklamıştır. Bununla birlikte, Komisyon, yapay zeka ile ilgili amaçların gerçekleştirilmesi için kişisel verilerin kullanılmasının düzenlenmesi konusunda GDPR'ın rolüne de vurgu yapmıştır. AB üye ülkeleri, AB Komisyonu yukarıda sözü edilen stratejisini açıklamadan önce, Yapay Zeka Konusunda İşbirliği Deklarasyonunu imzalamıştır (Zanfır-Fortuna, 2018).

Nuffield Biyoetik Konseyi'nin 2018 yılı Mayıs ayında paylaştığı çalışmasında yapay zekanın sağlık alanındaki kullanımının bugünkü sonuçları ile potansiyel sonuçlarının ne olacağı incelenmiştir (Bioethics NCo 2018). Gelecekte yapay zekanın insan kontrolü olmadan insan-

lara özgü pek çok eylemi yapabileceği öngörülmektedir. Ancak bu eylemleri yaparken yapay zekanın etik davranıp davranamayacağı, kimin etik değerlerine göre eğitileceği, yeni ortaya çıkan etik değerlerin yapay zekaya öğretilmesine gereksinim duyulacağı konular üzerinde durulmaktadır. Yapay zekanın insanların hatalarını ve yanlışlığını aza indirme potansiyeli olduğu düşünülse de eğitilmeleri için kullanılan veriden kaynaklanan yanlışlığı da pekiştirebileceği düşünülmektedir.

Yapay zekanın eğitilmesi için kullanılan veri setlerinin taraflı hazırlanması, verilerin sınırlı olması, yapay zekanın bu veri setlerine dayanarak eğitilmesi etik bir sorun olarak karşımıza çıkmaktadır. Makine öğrenmesi YZ algoritmalarında da büyük veri analitiğinde olduğu gibi kullanışlı/anlamli veriler üretilebilmesi için büyük miktarlarda veriye gereksinim bulunmaktadır. Bu nedenle, büyük veride olduğu gibi, veriyi en aza indirme (*data minimisation*) YZ için de bir zorluk oluşturmaktadır. Veriyi azaltmak belirli bir düzeye kadar mümkün olabilmektedir. AB Genel Veri Koruma Tüzüğü uyarınca, veri azaltma ilkesine göre, toplanan verinin daha uzun süre saklanması ve farklı amaçlar için işlenmeye devam edilmesi, veri gizliliğinin sağlanmasını destekleyen temel nedenlerin varlığı halinde söz konusu olabilmektedir. Veriler, toplanma amacı ile ilgili olduğu süre boyunca işlenmeli ve işlendikleri amaç için gerekli olduğu kadarıyla veri kullanılmalıdır.

Makine öğrenmesinin eğitime aşamasında büyük veri setlerine gereksinim olmasına rağmen, eğitim için kullanılan verinin miktarı ve yapısını eleştirel şekilde değerlendiren bir tasarım örneğinin kabul edilmesi önemli görülmektedir. Bu tasarım örneğinde, gereksiz ya da marjinal veriler azaltılarak, eğitim için kullanılan veri setinin miktarı sadece gerektiği durumda kademeli olarak artırılabilir. Eğitim algoritmalarında bu şekilde veri azaltma yönteminin çalışması için, sentetik veriler kullanılabilirliği önerilmiştir. Bu öneri doğrultusunda, kişisel veriler kümesinin bir alt kümesi oluşturulacak, bu kümedeki veriler anonimleştirilerek eğitimde kullanılacaktır (Nuffield Council on Bioethics, 2018).

Öte yandan, yapay zekanın gizlenebilecek ayrımcılığa yol açabileceği; geniş bir popülasyonu temsil etmeyen veri setleri ile eğitildikleri için adil olmayan kararlar verebilecekleri belirtilmektedir. Örneğin, Face2gene ile down sendromunun tespitinde etnik kökenlere göre doğruluk oranı değişim göstermiştir. Bu sistem, tanı koymada ikincil yardımcı kaynak olarak yapay zekadan yararlanmak isteyen hekimler tarafından kullanılmaktadır. Verilerin ticarileştirilmesi de bu tanı koyucu uygulamaya erişimi sınırlayacaktır.

Örneğin, zatürre sonrası hangi hastalarda komplikasyon gelişebileceğini tahmin etmek için yapay zeka uygulaması kullanılmış olan 2015 yılına ait bir klinik araştırmada, yapay zeka, astımı olan hastaların eve gönderilebileceğine ilişkin hekimlere yanlış bilgi vermiş, bu durum

yapay zekanın güvenilirliğinin yeniden sorgulanmasına neden olmuştur. Bununla birlikte, yapay zekanın gereksiz test ve tedaviler uygulanması talebini artırma potansiyeli taşıdığı da belirtilmektedir. Yapay zekanın öğrendikçe kendi parametrelerini ve kurallarını değiştirebiliyor olması, sistemin çıktılarının doğrulanması veya verilerin hatalarını belirlemede de güçlüğüne neden olabilecektir.

Yapay zekanın hatalı karar verme potansiyeli taşıması nedeniyle karar verme sürecinde yapay zekadan destek alınması durumunda sorumluluğun kime ait olacağı, yapay zeka sistemlerinin çıktılarının geçerli hale getirilmesindeki güçlükler, yapay zeka sistemlerinin eğitilmesinde kullanılan verinin taraflı olmasının içerdiği riskler, hassas verinin mahremiyeti ve güvenliğini sağlamada oluşabilecek sorunlar, yapay zeka teknolojisinin gelişmesi ve kullanımını sırasında toplumun güvenini sağlamak, zararlı amaçlar için yapay zeka kullanımı, yapay zekanın sağlık profesyonellerinin rolleri üzerine etkisinin ne olacağı gibi sorular/sorunlar, yapay zeka ile birlikte anılan temel etik başlıklardır.

İnsanların kararlarında hataya düşebildikleri ve yapay zekanın insan hatasını azaltan bir yöntem olması dolayısıyla yapay zekanın (YZ) yanlılığının bir sorun olarak görülmemesi gerektiği yönünde bir argümanın öne sürülemeyeceği savunulmaktadır. İnsan hatası ve yapay zekanın bu hata payını azaltması üzerinden karşılaştırmanın neden yapılamayacağı dört nedenle açıklanmıştır (Nuffield Council on Bioethics, 2018).

İlk olarak YZ çözümleri seri şekilde uygulanmak üzere tasarlanmıştır. Yanlılığı olan bir YZ, zayıf tasarlanmış kabul edilmekte, aynı ya da benzer durumlarda olan çok sayıda insanı etkilemesinin kaçınılmaz olduğu dile getirilmektedir. İnsan hatası sadece tek bir durumu etkilerken, seri üretilmesi nedeni ile YZ'deki hata çok sayıda kişiyi ilgilendirmektedir. İkinci olarak, yapay zekanın hata oranlarının insan beynininkine yakın ya da ondan daha düşük olduğu alanlar olmasına rağmen, çoğu karmaşık karar alma eylemlerini içeren süreçlerde daha yüksek hata oranları olduğu belirtilmiştir. Üçüncüsü, insan hatasının sosyokültürel boyutlarının olmasıdır. Bu da insan hatasını makine hatalarından ayıran bir unsur olarak değerlendirilmektedir. İnsan hatası, sosyal kabul edilebilirlik ve sorumluluktan kurtarma açısından, YZ hatası ile ayrılmaktadır. Bu da YZ'nin yapacağı potansiyel yanlış çözümlerin kabul edilebilirliğini zorunlu olarak etkileyecektir.

Son olarak, insan ve YZ kararlarının olumsuz etkilerinin, örneğin tamamen otonom araçlar ile insanların kullandıkları araçların ortaya çıkardığı zararlardan hareketle, zarar gören kişi sayısı gibi sayısal karşılaştırma yapılmasının da indirgemeci bir yaklaşım olduğu öne sürülmektedir. Otomatikleştirilmiş sistemlere izin verilmesinin haklı çıkarılabilmesi için en azından insanların kullandığı araçların sebep olduğu zararlardan hareketle, otoma-

tikleştirilmiş sistemlerin daha az zarara neden olacağına vaat edilmesi gerekmektedir. Bu sayısal yaklaşım sadece zararı azaltan politikaları değil, riskleri önleyici politikaların da kabul edilmesi gerektiğini ifade eden ihtiyatlılık yaklaşımı ile de örtüşmemektedir (Nuffield Council on Bioethics, 2018).

Hastalar açısından yapay zeka uygulamalarının olumlu etkileri de bulunmaktadır. Söz konusu uygulamalar hastaların sağlık durumlarını, kendi semptomlarını gözlemleyebilmelerini ve sağlık bakımlarını mümkün olan en kısa zamanda alabilmelerini sağlamaktadır. Ancak, aydınlatılmış onamın içeriği de yapay zeka uygulamaları ile birlikte genişlemektedir. Yapay zekanın karar verici olduğu durumlarda kişiye bu konuda bilgi verilmesi önem taşımakta, hangi verilerinin ne amaçla nasıl işlendiğinin kişinin anlayacağı şekilde anlatılması gerekmektedir.

Buna ek olarak, yapay zeka, riskler konusunda yaptığı hesaplamalara göre seçenekleri sınırlandırdığında veya kullanıcının en üstün yararına göre karar verdiğinde kişinin özerkliğini negatif yönde etkileyebilecektir. Aynı şekilde, yapay zekadan tanı koymada ve tedavi planı oluşturmada yararlanıldığında, sağlık çalışanının yapay zekanın ulaştığı sonuçları hastasına açıklayamadığı durumlarda da kişinin özgür ve aydınlatılmış onam vermesi engellenmiş olmaktadır. Yapay zeka destekli karar veren sağlık profesyonellerinin hastalarına karşı etik sorumluluklarının çerçevesi de bu teknoloji ile değişmektedir. Sağlık profesyonelleri yapay zekanın aldığı kararlardaki hata oranının azlığına güvenerek, kararlarının sonuçlarını ve hatalarını değerlendirme gereksinimi duymayabilirler.

Öte yandan, klinik verilerin, araştırma makalelerinin ve profesyonel kılavuzların yapay zeka kullanılarak analiz edilebilmesi, tedavi hakkında aydınlatılmış kararlar vermeyi kolaylaştırıcı bir etkiye de sahiptir.

Siber atakların ve sağlık bilgisayar sistemlerinin korunmasında ve veri güvenliğinin sağlanmasında yapay zekadan yararlanılsa da, bu sistemlerin heklenmesi ve hassas verilere erişilerek bu verilerin kötüye kullanılması ihtimali de bulunmaktadır. Bununla birlikte, kolayca tespit edilemeyecek şekilde sahte veya taraflı veriler sisteme girilmiş de olabilir. Bu nedenle, bu sistemlerin olası kötüye kullanılmaları karşısında kişilerin hassas ve özel verilerini koruyucu mekanizmaların geliştirilmesi gerekmektedir.

Yapay zeka teknolojileri ile, kişinin klavyede yazma şekli gibi motor davranışlarını analiz etmek, hareketlilik paternlerini tespit ederek kişinin sağlığı hakkında kendisinin haberi olmadan bilgi edinmek de mümkündür.

Avrupa Konseyi Biyoetik Çalışma Grubu da yeni ve kendi kendini yenileyebilen yapay zekanın, insan türü yerine geçebilme olasılığı üzerinden insan türünün varlığını sürdürmesi

konusundaki kaygılarını dile getirmiştir. Aynı zamanda, yeni ve geliştirilen teknolojilerin birbirlerine yakınlaşması ile bu teknolojilerin günlük hayata etkisi, kolektif normların psikolojisi ile, politik istek ve Avrupa Konseyi Avrupa Sosyal Haklar Şartı ışığında yaşam kalitesini değerlendirmiştir. Geçmişte bilim kurgu olarak düşünülen yeni uygulamalar günümüzde artık Avrupa'nın politik söylemlerinin merkezinde yer almaktadır.

Yapay zekanın hukuki sonuçlarının özel bir yasa ile düzenlenip düzenlenmemesinin gerekliliği tartışılmaktadır. Yapay zekadan destek olarak sağlık profesyonelinin verdiği kararlarda sorumluluk paylaşımı nasıl olacaktır? Bununla birlikte, pek çok özel ve hassas veri kullanan yapay zekanın bu verilerin güvenliğini nasıl koruyacağı gerek etik gerekse hukuki açıdan bir sorundur.

Özellikle ilaç keşfi ile ilgili özel sektör ilaç firmalarının yapay zeka üzerine yoğun araştırmalarının yanı sıra, devletler ve politika yapıcılar da bu teknolojinin değeri ve uygulanabilirliğini dikkate almaktadır. Örneğin, Avrupa Birliği Avrupa Komisyonu, robotik ve yapay zekayı köşe taşı teknolojiler olarak tanımlamış, bu alanda önemli yatırımlar yapılması ve hukuki sorunlara karşı yeni yaklaşımlara gereksinim olduğunu kabul etmişlerdir (Tsang et al., 2017).

Ulusal ve uluslararası yasalar, yapay zekayı bir hukuk sujesi olarak tanımamakta, bu nedenle yapay zekanın hukuki bir kişiliği olmadığı gibi zararlardan kişisel olarak da sorumlu tutulamamaktadır (Fenwick, Kaal, & Vermeulen, 2017).

Yapay zeka (YZ) uygulamaları açısından değerlendirildiğinde, 108 Sayılı Avrupa Konseyi Sözleşmesi ve veri koruma mevzuatları, otomatikleştirilmiş karar verme sistemlerinde kullanılan YZ algoritmaları dahil, algoritmalara aynı derecede uygulanabilmektedir. Ancak, insanın karar vermediği bir karar verme sürecinin olması, tek başına insan ve otomatikleştirilmiş kararlar arasındaki sınırı çizmek için yeterli bir sebep olarak görülmemektedir.

YZ'nin matematiğe dayalı çözümler sunan sözde güvenilir yapısı, algoritmalara dayanarak kararlar alan kişilerin, kişiler ve toplumun gözünde, analiz ile üretilen sonuçların güvenilir olduğunu yerleştirmesine neden olabilir. Bu da analiz ile üretilen sonuçların kabul edilmeden karar alınmasının yaptırımlara bağlanması olası tehdidi karşısında, kişilerin algoritmaya dayalı karar almaya zorlanmasına neden olabilir. Bu nedenle, insan karar verici de tek başına yeterli görülmemektedir.

Bununla birlikte, 108 Sayılı Avrupa Konseyi Sözleşmesi'nin eski ve yeni metnlerinin her ikisinde de otomatik veri işleme, ya da otomatikleştirilmiş veri işlemeden söz edilmekte ancak otonom veri işlemeden söz edilmemektedir.



Yapay zeka uygulamaları açısından düşünüldüğünde, kişilerin yapay zeka yerine insan ile iletişim kurmayı seçme hakkının kişiye tanınması gerekmektedir. Aynı şekilde, kişi kendi profilinin çıkarılmasını reddetme hakkına da sahip olmalıdır. Bu doğrultuda, Türkiye’de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda yapay zeka uygulamaları da düşünülerek, kişinin; görüşlerini dikkate almadan sadece otomatik olarak işlenmiş verilere dayalı bir şekilde ve kişiyi etkileyen kararlara tabi olmama hakkı tanınmalıdır. Verinin işlenmesi sonrasında ortaya çıkan sonuç kendisine uygulanan kişinin bu veri işlemenin temelindeki gerekçelendirmenin nasıl yapıldığını öğrenme hakkı da yasa ile tanınmalıdır. Bununla birlikte, teknoloji üretmenin sürecinde aktif rol alan şirketlerde etik komiteler oluşturulması bir zorunluluk haline gelmelidir.

Buna ek olarak, nöroteknoloji araştırmaları ile beynin yapısı ve işleyişi hakkında elde edilen bilgiler ve bunların yorumlanması, o kişinin düşünce özgürlüğünün, özel yaşamının gizliliğinin, kişisel verilerinin korunması hakkının ve ayrımcılık yasağının ihlal edilmesi potansiyelini taşımaktadır. Bu nedenle veri koruma yasalarında, görüntüleme teknolojileri ile elde edilen görüntülerin de kişisel veri olarak tanımlanması yerinde olabilir.

Öte yandan, YZ bağlamında, şeffaflık farklı anlamlara gelebilmektedir. Şeffaflık ile ifade edilen, kullanılan YZ uygulamalarının açıklanması olabileceği gibi, mantığının tanımlanması ya da YZ algoritmalarının yapısına ve uygun olan durumlarda, algoritmaların eğitilmesi için hangi veri setlerinin kullanıldığı bilgisine erişimi içerebilir. Bununla birlikte, şeffaflık, veri merkezli karar verme için, *ex-ante* (önceden/planlanan) ya da *ex-post* (nihai olan/gerçekleşen) bir gereklilik de olabilir. Algoritmaların yapısını öğrenmek, potansiyel yanlılığın tespit edilmesi olasılığını da ortaya çıkarabilecektir. Ancak fikri mülkiyet hakları ve rekabet konuları bazen bu erişimi sınırlayabilmektedir. Ayrıca, böyle engeller olmasa dahi, her durumda, uygulanan modellerin karmaşıklığı, insanın bu karmaşıklığı çözme yetisinin üzerinde olabilir.

21. yüzyıldaki tüm bu gelişen teknolojilerin, hukuktaki gerçek ve tüzel kişi ayrımı üzerine etkisi de tartışılan konular arasında yer almaktadır. Gerçek ve tüzel kişi arasındaki hukuki ayrımın giderek belirsizleştiği, özellikle biyoteknoloji ve yapay zekanın biyolojik ve fiziksel yaşam formlarını radikal şekilde dönüştürdüğü ifade edilmektedir. Teknolojinin insan yaşamını yapaylaştırmasının, hukukta gerçek kişinin daha yapay olmasına yol açtığı öne sürülmektedir. Yapay olarak tüzel kişi kategorisinde değerlendirilen kişilerin de insanlaştırıldığı, daha önceden sadece gerçek kişilere tanınan hakların yapay insan haklarına genişlediği dile getirilmektedir. Benzer şekilde, biyomedikal insan ve hayvan arasındaki ayrımın da insan hayvan hibrit oluşturma çalışmaları nedeni ile ortadan kalkmaya başladığı belirtilmektedir. Öne sürülen argümanlardan biri, belirli hayvanlar ya da yapay zekanın belirli formları gibi diğer yaşam formlarının hukuken kişi kavramı çerçevesi içine dahil edilerek genişletilmesi gereğidir.

## **Biyotıp Açısından Kişisel Veri Nedir ve Neden Koruma Altına Alınmalıdır?**

Sağlık kuruluşlarında çok sayıda hasta/başvuran verisi (hasta kayıtları, biyolojik materyal/radyografik tetkikler, patolojik materyal...) bulunmakta olup, bu verilerin alınma amacıyla veya alınma amacı dışında kullanımı konusunda farklı uygulamalar bulunmaktadır. Söz konusu insan biyolojik materyalleri üzerinde mülkiyet hakkı olup olmadığı konusunda da pek çok tartışma yürütülmektedir. Kişinin bu materyaller ve bu materyallerden elde edilen bilgiler üzerinde mülkiyet hakkının kime ait olacağı ve kişiye sağlayacağı hakları, yararları, etik sorunları da beraberinde getirmektedir. Tam ve tedavi amacıyla hastadan alınan bilgiler, veriler, materyaller ve bunların kullanımı ile araştırma için örneğini veren kişinin bu örneği bir kez verdikten sonra örneklerin tekrar başka bir araştırma için kullanılıp kullanılmayacağı, hangi amaç için yeniden kullanılacağı, ne kadar süre saklanacağı, bunlarla ilgili süreci kendisinin belirleyip belirleyemeyeceği önemlidir. Mülkiyet hakkının kişiye sağladığı satma, kiralama, yok etme, değiştirme gibi tüm haklar, insan biyolojik materyalleri ve bu materyallerden elde edilecek olan tıbbi veriler için de söz konusu olacak mıdır? Ya da araştırmayı yapacak olan kurumun şimdiden öngörülmeyle gelecekteki araştırmalar için kullanacağı tıbbi veri ve bilgilerin bir sınırı var mıdır (Örnek Büken & Zeybek Ünsal, 2017).

Mülkiyet hakkının kapsamı dikkate alındığında söz konusu verilerin kullanımı, onlardan yararlanılması ve üzerlerinde tasarrufta bulunulmasının sınırının ne olacağı sorunu etik disiplininin sorduğu bir sorudur. Bu sorunun yanıtı kolay olmadığı için farklı yaklaşımlar ortaya çıkmış, ulusal ve uluslararası düzeydeki yasal düzenlemeler de birbirinden farklı olmuştur.

İnsan biyolojik/genetik kaynaklarının insanlığın ortak mirası olduğu yaklaşımının, Avrupa Birliği'nin ortak değeri olarak benimsenmesinin, verilerin ve bilimsel bilginin yayılmasını, uluslararası platformda ulaşılmak istenen standart ilkelerin oluşturulmasını kolaylaştıracakı düşünülmektedir. Tıbbi bilgi ve verilerin anonimleştirilerek kullanılması durumunda veri sahibi ile veri arasındaki ilişki tamamen ortadan kaldırılmaktadır. Bu şekilde bu bilgi ve verilerin değerlendirilmesine konu olan araştırmalarda, araştırmamanın herhangi bir aşamasında veri sahibine geri dönüş sağlayarak onamının alınması, pratik olarak mümkün olmamaktadır. Bazı çalışmalarda —özellikle genetik çalışmalar— verilerin işlenmesi ile beklenmedik bilgi ve sonuçlar ortaya çıkabilmekte, bu sonuçların veri sahibini ya da gelecek nesillerin sağlığını olumlu ya da olumsuz etkileyebilmesi de söz konusu olabilmektedir.

Bunun yanı sıra, bilimsel araştırmalar için elde edilen verilerin, gerektiğinden fazla depolanabilmesi için söz konusu verileri anonimleştirmek, kişilerin mahremiyetinin korunması konusunda genel bir önlem olarak da bildirilmektedir. Öte yandan, anonimleştirmenin tam bir kuru-

ma sağlayıp sağlamadığı da literatürde tartışılmaktadır. Anonimleştirme yapılmadan yürütülen çalışmalarda veri sahibi, verdiği onamını her zaman geri alma ya da örneğinin kullanılmasından vazgeçme hakkına hem etik hem de hukuki açıdan sahip olmaktadır. Ancak anonimleştirme yapılması bu hakkın kullanımına imkân vermemektedir (Örnek Büken & Zeybek Ünsal, 2017).

### **6698 sayılı Kişisel Verilerin Korunması Kanunu**

AB'ye tam üyelik müzakereleri devam eden Türkiye'nin kişisel verilerin korunması alanı ile ilgili attığı adımlar yeterli görülmemiş, temel bir yasa çıkarılması tam üyelik sürecinin ilerletilmesi için bir ön şart olarak değerlendirilmiştir.

Söz konusu kanunun gerekçesinde Avrupa İnsan Hakları Mahkemesi'nin hastaların hassas verilerinin herhangi bir kanuna dayanmaksızın sağlık kuruluşlarında tutuluyor olması ve verilerin saklanması, kullanılması, aktarılması gibi işlemlerin veri güvenliğinin yeterince sağlanmadan yapılıyor olmasını özel hayatın gizliliğini ihlal kabul ettiği belirtilmektedir. Sağlık alanında gizliliğe işaret eden uluslararası yasalar olmasının yanı sıra e-sağlık alanındaki gizliliğe saygıya açıkça işaret eden uluslararası bağlayıcı bir mevzuat da bulunmamaktadır.

Ayrıca, ülkemizin de üye olduğu, İktisadi İş Birliği ve Kalkınma Teşkilatı (*OECD*)'nin Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafikinin Korunmasına İlişkin Rehber İlkelerini 23/9/1980 tarihinde kabul ettiği ve bu belgenin kişisel verilerin korunması konusunda ilk uluslararası belge olduğu da belirtilmelidir.

Kişisel verilerin korunması konusunun gündeme gelmesi 1980'li yıllardan itibaren uluslararası belgelere girmesi ile birlikte olmuştur. Daha sonra, Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi hazırlanmış Avrupa Konseyi'ne üye tüm ülkelerin aynı standartlarda eşdeğer koruma sağlaması ve ülkeler arası veri paylaşımı ilkeleri belirlenmiştir. 28 Ocak 1981 tarihli Avrupa Konseyi'nin 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ülkemizin de taraf olduğu bir sözleşmedir.

Türkiye'de kişisel verilerin özel bir kanun ile koruma altına alınması 6698 sayılı Kişisel Verilerin Korunması Kanununun 7 Nisan 2016 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe girmesi ile olmuştur.

Kanunun hazırlanması sırasında Avrupa Konseyi'nin kişisel verilerin korunmasına yönelik olarak farklı sektörlerde uygulanmak üzere ilkeler belirleyerek tavsiye kararları aldığı bilinmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu hazırlanırken

(6698 sayılı Kişisel Verilerin Korunması Kanunu, 2016), kanunun çerçeve niteliğinin korunması için Avrupa Konseyi'nin tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi sektörlerde uygulanmak üzere oluşturduğu tavsiye kararlarının dikkate alınmadığı belirtilmiştir. İlerleyen süreçlerde, söz konusu tavsiye kararlarında belirlenen ilkelerin belirtilen sektörlerle ilgili yapılacak düzenlemeler için dikkate alınacağına öngörüldüğünü de biliyoruz. Nitekim Kanun sonrası ilk olarak çıkarılan “Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik” bunun göstergesidir.

AB, üye ülkeler arasında verilerin serbest dolaşımını açık ve kalıcı bir şekilde düzenleyerek kişisel verilerin üst düzeyde eşdeğer korunmasını amaçlamıştır. Bu nedenle, 24/10/1995 tarihinde “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafik Direktifi” (95/46/EC) yürürlüğe girmiştir. Bu direktif ile üye ülkeler arasında kişisel verilerin korunmasına ilişkin mevzuatın harmonize edilmesi hedeflenmiştir.

1970'li yılların başından beri veri işleme ile ilgili düzenlemeler yapmaya başlayan AB'nin bugün veri koruma konusunda reform yapma amacı da; AB'nin kişisel verilerin korunması ile ilgili hukuk sistemini modernize etmeye, özellikle globalleşmenin sonucu olarak ve yeni teknolojilerin kullanımından kaynaklanan problemleri çözmeye, kişilerin haklarını güçlendirmeye, Avrupa Birliği ve dışındaki ülkelerde kişisel verilerin serbest dolaşımı ile ilgili idari formaliteleri de azaltmaya yöneliktir.

Gerçekten de kişisel verilerin işlendiği sektörlerin ve işleme amaçlarının çeşitliliği göz önünde alınırsa; farklı konularda ve sektörlerde o konu veya sektörler için özgü düzenlemelerin yapılmasına şiddetle ihtiyaç vardır. Bu şekilde kurumlara yol gösterici olacak şekilde kişisel verilerin korunmasının gecikmeksizin hayata geçirilmesi sağlanabilir.

### **Hassas veriler ve bu verilerin işlenmesi için istisnalar**

Kişisel veri gerek ulusal mevzuatımızda gerekse Avrupa Birliği ve Avrupa Komisyonu'nun hukuki metinlerinde “bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi” olarak tanımlanmaktadır. Kişinin sağlık bilgileri, biyolojik örnekleri ve bu örneklerden elde edilen bilgiler gibi kişisel verileri “hassas kişisel veri” olarak nitelendirilmektedir. AB 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 4(1) maddesine göre de veri, eğer tanınabilir ya da tanımlanabilir bir kişi ile bağlantılı ise kişiseldir. Kişinin tanınabilir olmasını sağlayan verinin kişisel veri olarak nitelendirileceğini düzenleyen bu maddenin tanınabilirlik eşliğini düşük tuttuğu dile getirilmektedir. Eşsiz, tek (unique) kelimelerinin tanımı olmamakla birlikte,

eşsiz kimlik tanıma en yüksek tanıma derecesi olarak ifade edilmektedir. Bu nedenle bu eşik biyometrik veriler için yüksektir (Örnek Büken & Zeybek Ünsal, 2017).

Biyometrik veriler, 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 4 (11) maddesinde, kişinin eşsiz, tek olarak tanınmasına izin veren, fiziksel, psikolojik veya davranışsal karakteristik özellikleri ile ilgili, yüz görüntüleri, daktiloskopik verileri gibi her türlü veri olarak tanımlanmıştır ve hassas veri olarak kabul edilmektedir. Biyometrik veriler arasında, bireye ait parmak izi, avuç içi izi, yüz, iris, retina, kulak, ses, imza, yürüyüş biçimi, el damarı, vücut kokusu veya DNA bilgisi şeklinde bir veya daha fazla fiziksel veya davranış karakterleri bulunmaktadır.

Etik disiplininin tartışma konularının merkezinde yer alan bir diğer konu da biyometrik ve genetik veriler gibi hassas verilerin, işlenmesi durumunda kişilerin ayrımcılığa uğramasından korkulduğu için “hassas veri” olarak adlandırılan verilerin, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında belirlenen Veri Koruma Kurulu'na alınacak önlemlerle —ki bu önlemlerin ne olduğunu henüz bilemiyoruz— işlenebilir olmasıdır.

6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında biyometrik veriler, özel nitelikli kişisel veriler olarak düzenlenmiştir. İlgili yasanın 6. maddesinin 3. fıkrasında, özel nitelikli kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenemeyeceği belirtilmek suretiyle yasal güvence altına alınmıştır (6698 sayılı Kişisel Verilerin Korunması Kanunu, 2016).

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda “hassas veri” olarak tanımlanan veriler aşağıda belirtilmiştir;

- Irk,
- Etnik köken,
- Siyasi düşünce,
- Felsefi inanç,
- Din,
- Mezhep veya diğer inançlar,
- Kılık ve kıyafet,
- Dernek, vakıf ya da sendika üyeliği,
- Sağlık,

- Cinsel hayat,
- Ceza mahkûmiyet ve güvenlik tedbirleriyle ilgili veriler
- Biyometrik ve genetik veriler

İlgili Yönetmeliğin üçüncü bölümünde yer alan kişisel sağlık verilerinin işlenmesi maddesinde, açık rıza aranan ve aranmayan durumlara göre kişisel verilerin iki şekilde işlenebileceği düzenlenmiştir.

1) Açık rıza aranmadan kişinin sağlık verilerinin işlenebileceği durumlar;

- Kamu sağlığının korunması,
- Koruyucu hekimlik,
- Tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi,
- Sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla toplanan veriler olarak sayılmıştır.

2) Ayrıntılı bilgilendirme ve yazılı rıza alınmasını gerektiren durumlar;

Yukarıda belirtilen amaçlar dışında kalan amaçlar için kişisel verilerin işlenmesinin söz konusu olduğu durumlar içindir.

Anılan madde kapsamında biyomedikal araştırmalar amacıyla kişisel verilerin işlenmesi konusu gündeme alınmamış, daha çok sağlık hizmeti kapsamında (tanı, tedavi, koruyucu sağlık, sağlık yönetimi ve finansmanı) yürütülen hizmetlere değinilmiştir. Ancak bugünün biyomedikal araştırmalarının geleceğin sağlık hizmeti olduğu öngörüsü ile araştırma amaçlı alınan materyalin kullanımı veya materyalden elde edilecek verilerin kullanımı konusunda “açık rıza aramamak” haklı çıkarılabilir mi? Tartışmalıdır...

Görüldüğü gibi, ülkemizde, sağlık, cinsel hayat, biyometrik ve genetik veriler Kişisel Verilerin Korunması Hakkındaki Kanun kapsamında özel nitelikli veriler olarak tanımlanmıştır. AB düzenlemelerine bakıldığında hassas veriler AB Veri Koruma Direktifinin 8. maddesinde düzenlenmiştir. Anılan maddede, ırk veya etnik köken, politik düşünceler, inançlar, sendika üyelikleri ve sağlık ve cinsel hayat ile ilgili veriler hassas veri olarak sayılmıştır. Avrupa veri koruma reform paketi kabul edilene kadar biyometrik veri kavramı ile ilgili açık bir düzenleme olmadığı gibi bu verilerin işlenmesi ile ilgili belirli kurallar da bulunmamaktaydı. Biyometrik verilerin tanımlanması ve hassas veriler listesine eklenmesi 2016 yılında olmuştur.

2016/679 sayılı AB Genel Veri Koruma Tüzüğü’nde, genetik veri, biyometrik veri ve sağlığı ilgilendiren veriler ayrı ayrı tanımlanmıştır. Genetik veri, gerçek kişinin kalıtsal ya

da edinilen genetik özelliklerle ilişkili kişisel verisidir. Bu veriler o gerçek kişinin fizyolojisi veya sağlığı hakkında söz konusu kişinin özellikle biyolojik örneğinin analizi sonucunda eşsiz bilgi verir. Sağlıkla ilgili veriler de gerçek kişinin fiziksel veya akıl sağlığı (mental) ile ilgili kişisel verilerdir (Örnek Büken & Zeybek Ünsal, 2017).

## **Biyometrik Veriler**

Biyometrik veri, gerçek kişinin fiziksel, psikolojik veya davranışsal özellikleriyle ilgili belirli teknik işleme sonucu elde edilen kişisel verilerdir. Söz konusu biyometrik veriler, yukarıda da ifade edildiği gibi, yüz görüntüleri veya daktiloskopik veri gibi o gerçek kişinin eşsiz tanınabilir olmasına izin veren ya da o kişi olduğunu onaylayan verilerdir.

Hukuki niteliği bakımından biyometrik veri diyebilmek için biyometrik verinin tanımlanmış bir kişi ile ilişkisinin olması gerekir. Biyometrik tanıma, ölçümler, benzerlik ve farklılıkların olasılıklarına dayanmaktadır. Veri Koruma Reform Paketi biyometrik veriyi de hassas veri listesine eklemiş, gerçek kişiyi eşsiz bir şekilde tanımlamak amacıyla biyometrik veri işlemeyi yasaklamıştır.

Parmak izleri üzerine yapılan bazı çalışmalar ile biyometrik verilerin sağlıkla veya ırk ya da etnik kökenler gibi hassas verileri açığa çıkarabildiğinin gösterildiği dile getirilmektedir. Bilimsel perspektiften bakıldığında biyometrik özelliklerin benzersizliği, eşsizliği adli uzmanların üzerinde tartıştığı bir varsayımdır. İki kişinin aynı parmak izine sahip olmadığının bilimsel açıdan gösterilmediği söylenmektedir. Parmak izleri üzerinde tıbbi araştırmalar yapılmış ve çalışmalar parmak izi üzerindeki şekillerin paternlerinden kişinin şeker hastalığı gibi bir hastalık riski olup olmadığını anlaşıldığını göstermiştir. Aynı şekilde kişilerin etnik kökenleri hakkında bilgi sahibi de olunabilmektedir.

## **Genetik Verilerin Korunması ve Tesadüfi genetik verilerin bildirilmesi**

AK No. R (97) 5 sayılı tıbbi verilerin korunması hakkındaki tavsiye kararında bir bireyin genlerinde taşınan her türlü genetik bilgi ya da tanımlanabilir özellikleri olsun ya da olmasın hastalık veya sağlığın herhangi bir yönüyle ilgili genetik hat genetik veri olarak değerlendirilmiştir. Genetik veriler, hangi tipte olursa olsun, kişinin kalıtsal özellikleriyle ya da ilgili gruptaki kişilerin bu tür kalıtım partnerleriyle ilgili tüm verilerini içermektedir. Genetik verilerin kendine özgü niteliği, bu verilerin kişinin sadece kendisiyle ilgili olmaması nedeniyle de doğuracağı sonuçlar açısından farklılıklara yol açmaktadır. İlgili tavsiyeye göre genetik hat, doğum sonucu ve iki ya da daha çok kişi tarafından paylaşılan genetik benzerliklerden oluşur. Söz konusu tavsiyeler, ulusal yasalarda başka uygun önlemler alınmadığı durumda, tıbbi bilginin toplanması ve otomatik işlenmesi hakkında uygulanır. Ancak üye ülkeler, bu

tavsiye metninde belirtilen ilkeleri, otomatik olarak işlenmeyen tıbbi veriler için de genişletilebilir (Örnek Büken & Zeybek Ünsal, 2017).

Anılan tavsiye kararı, sağlık verileri, özellikle genetik veriler, genetik testler sonucunda ortaya çıkan tesadüfi/kazai sonuçlar, onam, veri güvenliğinin sağlanması, bilimsel araştırmalar, bireylerin temel hak ve özgürlüklerine, mahremiyetine saygı ve gizlilik çerçevesinden demokratik toplumun gerekleri gözetilerek kaleme alınmıştır. Bu bağlamda, genetik veriler, bilimsel araştırmalar, mahremiyete saygı, veri sahibinin hakları ve ona verilecek bilgiler, hukuken yeterliliği olmayan kişiler ile doğmamış çocukların tıbbi bilgilerinin statüsünün ne olacağı konuları ayrı başlıklar altında düzenlenmiştir.

Genetik veriler ile ilgili düzenlemeye bakıldığında, önleyici, tedavi edici, tanısal ve veri sahibinin tedavisi ya da bilimsel araştırma için toplanan ve işlenen genetik veriler sadece bu amaçlar için ya da veri sahibinin bu konularda özgür ve bilgilendirilmiş karar/izin vermesi koşuluyla kullanılabilir. Yargı süreci ya da suç araştırması nedeniyle adli amaçlarla işlenen genetik verilerin, uygun önlemlerin alındığı özel bir kanunla düzenlenmesi gerekmektedir. Genetik veri, sadece kanıt göstermek, gerçek bir tehlikeyi önlemek ya da belirli bir cezayı gerektiren suçu engellemek için genetik bir bağlantı olup olmadığını anlamak için kullanılabilir. Genetik veri, genetik olarak bağlantılı olabilecek başka özellikleri belirlemek için hiçbir şekilde kullanılamaz. Söz konusu tavsiye kararında belirtilen amaçlar dışında, genetik verinin toplanması ve işlenmesine, kural olarak sadece sağlık nedenleri ve özellikle veri sahibinin ya da üçüncü kişilerin sağlığına yönelik ciddi durumları önlemek için izin verilmelidir. Ancak üstün çıkar ya da kanunda belirtilen uygun önlemlerin alınmış olması halinde hastalığı tahmin etmek için genetik verilerin toplanması ya da kullanılmasına izin verilebilir.

Aşağıdaki şartlar karşılandığı durumda, kişinin genetiği analiz edilirken beklenmedik tesadüfi sonuçlar ortaya çıkması halinde, bilgilendirilmesi gerektiği düzenlenmiştir. Anılan tavsiye kararının 8.4. maddesine göre, eğer ulusal yasalar tesadüfi/kazai olarak ortaya çıkan bilgileri vermeyi yasaklamamışsa, kişinin kendisi bu bilgiyi almayı talep etmişse, tesadüfi sonuçlarla ilgili bilgi vermek, kişinin sağlığıyla ilgili ciddi zarar oluşturmayacak ya da ulusal yasalarca başka uygun önlemler alındıysa ve bu bilgi kişinin sosyal ailesinin bir üyesine, akraba ya da soyuna, kişinin genetik hattıyla direk bağlantısı olan kişiye ciddi zarar vermeyecekse, kişi beklenmedik sonuçları ile ilgili olarak bilgilendirilebilir. Ulusal yasalarda herhangi bir yasak getirilmemişse ve beklenmedik genetik sonuçlara ilişkin bilgiler kişinin doğrudan tedavisi veya hastalığının önlenmesi için önemliyse kişi bilgilendirilmelidir.



## **Olumlu bir gelişme; verilerin silinmesi, yok edilmesi, anonim hale getirilmesi**

Tanı, tedavi ya da sağlığı koruma, geliştirme ve sağlık finansmanını yönetebilme amaçlı olarak toplanan ve işlenen sağlık verilerinin, kişinin talebi halinde silinmesi, yok edilmesi veya anonim hale getirilmesi etik, insana verilen değer, insan hak ve onuru açısından önemlidir. Kanunda bu durum “yönetmelikle düzenlenecek” şeklinde belirlenmiş, daha sonra çıkan ilgili Yönetmeliğe göre, “veri işlemeyi gerektirecek durumlar ortadan kalktı ise veriler anonim hale getirildikten sonra silinecektir” denmiştir. Öte yandan adli mercilerce talep edilmesi halinde ve sadece bu amaçla söz konusu verilere erişim sağlanabilecektir. Rızanın açıklanmadığı (yoğun bakım hastası olmak, anestezi altında bulunmak...) ya da geçerli olmadığı bazı durumlarda (kişi yeterliliğini ortadan kaldıran sebeplerle), kişilerin hayat veya beden bütünlüğünün korunması için ve onların yararı gözetilerek (en üstün tıbbi çıkarları; *the best interest*) kişisel verilerinin işlenmesi söz konusu olabilir. Örneğin kişinin bilincinin yerinde olmadığı veya gerçeği değerlendirme yetisini bozan bir akıl hastalığı olması durumunda, bilişsel ve istençsel yetersizliği nedeniyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale yapılması sırasında, kişisel verileri işlenebilecektir. Bu bağlamda kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar gibi veriler ilgili sağlık sistemi üzerinden işlenebilecektir (Örnek Büken & Zeybek Ünsal, 2017).

Özetle, Sağlık Bakanlığı, sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve finansmanı amacıyla elde edilen kişisel sağlık verilerini toplayabilecek, işleyebilecektir. Bu veriler 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda öngörülen şartlar dışında aktarılamayacaktır. Bakanlık, toplanan ve işlenen verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kuracaktır. Bu sistem kişisel verilerin sınırsız bir şekilde toplanmasına neden olmaktadır. Bu açıdan, tüm sağlık verilerinin bu şekilde bir merkezde toplanmasının yol açacağı etik sorunların tartışılması önem kazanmaktadır. Özellikle veri güvenliği konusu önem kazanmaktadır; verilerin ne kadarı, nerede, hangi amaçla kullanılacaktır? Bu verilere kim, hangi amaçla erişebilecektir? Ne için ve ne kadarı hangi kişilerle paylaşılacaktır? Tüm bu soruların yanıtızsız kalması ve sınırsız bir şekilde tüm verilerin Bakanlık nezdinde tutuluyor olması da etik ve hukuki açıdan değerlendirilmesi gereken bir sorundur. Bakanlık, düzenleme uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri alacağını, bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi kuracağını belirtmiştir (Örnek Büken & Zeybek Ünsal, 2017).

Avrupa Komisyonu'nun yukarıda bahsettiğimiz tavsiye kararında, bilimsel araştırma amaçları için kullanılan tıbbi verilerin mümkün olan ilk anda anonimleştirilmesi gerektiği hüküm altına alınmıştır. Anonimleşmeyi güvence altına almak ve bu yönde prosedür ve tekniklerin geliştirilmesi için de kamu otoriteleri ile birlikte profesyonel ve bilimsel organizasyonlarına da görev verilmiştir. Anonimleştirmenin yaratabileceği zorluklar da göz önüne alınarak, bilimsel araştırma projesinin yapılabilmesi anonim verilerle mümkün değilse ve proje yasal amaçlar için yürütülüyorsa aşağıdaki şartların varlığı halinde kişisel verilerle proje yürütülebilecektir.

- Veri sahibi bir veya birden fazla araştırma için aydınlatılmış onam vermişse,
- Yasal olarak kişi karar verme yeterliğine sahip değilse ve yasa, o kişinin kendisi adına karar vermesine izin vermiyorsa,
- Yasal temsilci ya da kanunen onun adına karar vermeye yetkili kişi ya da organlar, veri sahibinin tıbbi durumuyla ya da hastalığıyla ilgili araştırma projesi çerçevesinde onam vermişse,

Bilimsel araştırma kamu sağlığı için gerekli ise ya da kamu yararını ilgilendiren önemli bir bilimsel araştırma projesi için verilerin açıklanması gerekiyor ise aşağıdaki şartların da sağlanması halinde kişisel veriler kullanılarak projeye devam edilebilir. Buna göre, veri sahibi veriyi açıklamaya açıkça karşı çıkmamışsa, veri sahibine tüm makul çabaya rağmen yeniden ulaşılıp, onamını aramak pratikte mümkün değilse ve araştırma projesinin çıkarları gözetildiğinde yetkilendirmeyi haklı çıkarıyorsa kişisel veriler kullanılabilir (Örnek Büken & Zeybek Ünsal, 2017).

### **Kişisel Verilerimin silinmesini talep edebilir miyim?**

Bu talep uygulamada “unutulma hakkı” şeklinde tartışılmaktadır. Kavram olarak Avrupa Adalet Divanı'nın Google Spain SL v. Agencia Española de Protección de Datos and Mario kararında 2014 yılında ortaya çıkmıştır. Bu hakkın bir insan hakkı olup olmadığı tartışma konusudur. UNESCO, “...uluslararası insan hakları hukukunun böyle bir hak tanımadığını, konunun yerel olduğunu, çünkü dijital çağda, geçmişteki hataların silinmesinin imkansız olduğunu, teknolojinin kişilere nerede çalışır ya da yaşıyor olurlar ise olsunlar, bir başka kişinin internet üzerinden yaptıkları paylaşımları, yorumları, fotoğrafları veya kayıtlarını bulma imkanını sağlamakta” olduğunu dile getirmiştir. Ancak UNESCO, İnsan Hakları Evrensel Beyanamesi'nin 12. maddesinin “Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışamaz, şeref ve onuruna saldıramaz. Herkesin bu gibi karışma

ve saldırılara karşı yasa tarafından korunmaya hakkı vardır” hükmünü dikkate almamıştır (Örnek Büken & Zeybek Ünsal, 2017).

Unutulma hakkı, AB’nin bilgi ve iletişim teknolojileriyle gelen yenilikleri, bireylerin temel hak ve özgürlüklerini ihlal etmeden, damgalanmaya yol açmadan şekillendirmeye çalıştıkları bir anlayışın ürünü olarak ortaya çıkmıştır. Bu hak, AB tarafından, bir kişinin kendisinin herhangi bir arama motoruna ismi yazıldığında, o kişinin hangi bilgilerine çevrimiçi olarak erişilebileceğine karar verebilme ve hangi bilgilerine erişilip erişilemediğinden emin olma hakkı olarak tanımlanmaktadır. Kişinin bu kararı verebilmesi sadece kendi elinde olmalıdır. Kişinin kendisi dışında, herhangi bir algoritma ya da üçüncü bir kişi tarafından o kişinin bilgilerine çevrimiçi olarak ulaşılabileceğinin kararı unutulma hakkı kapsamında verilemez.

AB 95/46/EC sayılı Veri Koruma Direktifi’nde unutulma hakkına yer verilmemiş, ancak 2016/679 sayılı AB Genel Veri Koruma Tüzüğü’nün 17. maddesinde hüküm altına alınmıştır. Unutulma hakkı kapsamında, kişinin verilerinin toplanma amacı için o verilerin artık kullanılmasına gerek olmadığında, kişi tüm verisinin ortadan kaldırılmasını isteme hakkına sahiptir.

Ancak, 17. maddenin 3. fıkrasının d bendine göre, kamu yararı için arşivleme, bilimsel veya tarih araştırmaları yapmak ve istatistiksel çalışmalar için verilerin işlenmesi gerekiyor ancak verilerin silinmesi bu amaçları gerçekleştirme için ciddi şekilde olumsuz etkileyecek veya imkansız hale getirecek ise unutulma hakkından söz edilemeyecektir. Ancak bunun için söz konusu araştırmalar 89(1) maddede belirtilen şartlara uygun olmalı, 17. maddenin 1. fıkrasındaki düzenlemeler dikkate alınmalıdır (Örnek Büken & Zeybek Ünsal, 2017).

Türkiye’de ‘unutulma hakkı’ olarak ifade edilen, kişisel verilerin internetten silinmesi, yasal düzenlemeyle ilk kez sabitlenmiş olacaktır. Özellikle, Google, Facebook, Twitter ve diğer veri toplayan hizmetler, başvurunuz üzerine hesaplarınız ve kişisel verilerinizi silmek zorunda olacak ve üçüncü taraflara da iletemeyecektir. Yasayla ayrıca veriler taşınabilir hale gelecek, hizmet sunucusunu değiştirdiğinizde verilerinizi de yeni hizmet sunucusuna aktarabilmeniz olanaklı olacaktır. Verileri işleyenler, talep etmeniz durumunda hangi verilerinizi depoladıklarını, bu verilerle ne yaptıklarını ve kimlere ilettiklerini açıklamak zorunda olacaktır. Bu hizmetin hem anlaşılır hem de ücretsiz olarak sunulması da esastır.

Unutulma hakkını sadece internet ortamındaki verilerin ele alınması olarak tanımlamanın çok sınırlayıcı olacağı, bu durumun söz konusu hakkın gelişimini engelleyeceği yönünde görüşler bulunmaktadır. Yargıtay Hukuk Genel Kurulu’nun 17 Haziran 2015 tarihinde (E. 2014/4-56, K. 2015/1679), unutulma hakkı ile ilgili verdiği kararında da dört yıl önce cinsel saldırıya uğraması nedeniyle mağdur olan ve mağdurun adının rızası olmadan açık bir şekilde

rumuzlanmadan bir kitapta yazılmasını, dijital ortamda olmamasına karşılık, unutulma hakkını ve özel hayatın gizliliğini ihlal kapsamında değerlendirmiştir.

Anılan kararda kişisel veriler; bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları olarak kabul edilmiştir.

Kişisel verilerin ne kadar süre saklanacağı ile ilgili olarak mevzuatta öngörülen süre, veriyi işlemek için belirlenen amacı gerçekleştirmek için gereken süredir. Buna göre, veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacaklardır. Böyle bir düzenleme yok ise, veriler ancak işlendikleri amaç için gerekli olan süre kadar saklanabilecektir. Söz konusu biyomedikal alan olduğunda tanı/tedavi/araştırma amaçlı olarak toplanan verilerin ne kadar süre saklanacağı konusu netlik kazanmalıdır.

Özellikle araştırma amaçlı toplanan veriler açısından, araştırmaya katılacak kişilerden aydınlatılmış onam alma sürecinde, hangi verilerin hangi amaçla ve nerede kullanılacağı, ne kadar süre nerede saklanacağı bilgisinin kişilere verilmesi araştırmaya katılıp katılmama kararlarını vermelerinde belirleyici rol oynayacaktır (Zeybek Ünsal & Örnek Büken, 2018).

Bu açıdan kişisel verilerin etkili bir şekilde korunması, var olan araştırmaların ilerleyebilmesi ve veriye dayalı olarak gelecekte yeni araştırmalar yapılmasının önünün açılması açısından önemlidir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda getirilen düzenleme ile bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir. Gelecekte kullanma ihtimalinin varlığına dayanarak veri saklanamayacaktır. Bu açıdan araştırma dünyasında bu kanunun uygulanabilirliği bu madde kapsamında yeniden tartışılmalıdır.

### **Bilgi talep edebilir miyim?**

6698 sayılı Kişisel Verilerin Korunması Kanununun 11. maddesinin 1. fıkrasının b bendine göre, “Herkes, veri sorumlusuna başvurarak kendisiyle ilgili kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkına sahiptir. Ancak AB/95/46 sayılı Veri Koruma Direktifi'nin aksine veri sorumlusunun bilgi talep eden kişiye cevap veremediğinde oluşabilecek sonuçlardan veri sahibinin haberdar olma hakkından da söz edilmemiştir. Daha sonra çıkarılan yönetmelik, veri sahibinin veri sorumlusundan bilgi talep edebileceğini, açık ve anlaşılabilir bir şekilde, yazılı ya da elektronik ortamda veri sahibine bilgilendirme yapılacağını düzenlemiştir.

AB Veri Koruma Direktifinin 10. maddesinde, veri sahibinin veri sorumlusundan bilgi talep edebilmesi, veri sorumlusunun ilgili kişiye cevap verememesi durumunda oluşabilecek sonuçlardan da veri sahibinin haberdar olma hakkı düzenlenmiştir. Anılan maddenin c fıkrasının üçüncü bendinde verisi işlenen kişi, veri sorumlusundan bilgi talep ettiğinde cevap verilemediği durumlarda veri sahibinin karşılaşılabileceği olası sonuçların kendisine anlatılması gerektiği düzenlenmiştir (Örnek Büken & Zeybek Ünsal, 2017).

### **Veri Transferi İçin Eşdeğer Koruma:**

AB 95/46/EC sayılı Veri Koruma Direktifi'nin 25. maddesi, kişisel verilerin 3. ülkelere transferi için gereken yeterli korumanın hangi ölçütlere göre belirleneceğini düzenlemiştir.

Anılan maddede, verinin niteliğine, amacına ve öngörülen işleme süresine, verinin nereden nereye aktarılacağına, hukuk kurallarına, verinin aktarılacağı ülkenin profesyonel kuralları ile aldıkları güvenlik önlemlerinin neler olduğu da belirlenerek yeterli korumanın olup olmadığının değerlendirilmesi gerektiği düzenlenmektedir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yeterli korumanın olup olmadığının değerlendirilmesinin Kişisel Verileri Koruma Kurulu tarafından yapılacağı, Kurulun da yeterli korumanın bulunduğu ülkeleri ilan edeceği belirtilmiştir. Kurulun yapacağı değerlendirmenin ölçütleri de bu madde kapsamında sıralanmıştır.

Öte yandan, ilgili yönetmeliğin 8. maddesinin 1. fıkrasında öngörülen, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacı dışında kalan amaçlar için işlenecek olan kişiler sağlık verileri, ilgili maddenin 2. fıkrasına göre ancak anonim hale getirilmek suretiyle aktarılabilir. Bu durumda, arşiv materyali olarak ya da araştırma biyobankalarında toplanan ve işlenen kişisel sağlık verilerinin araştırma amaçlı olarak, anonim hale getirilmeden aktarılması mümkün olmayacaktır.

Dünya Hekimler Birliği'nin "Sağlık Veritabanları ve Biyobankalarla ilgili Etik Kaygıları üzerine Dünya Tabipler Birliği, Taipei Bildirgesi"nde de verilerin ve materyalin kimliksizleştirildiği durumlarda ilgili bireyin kendi verileriyle/materyaliyle ne yapıldığını bilemeyebileceği ve yararlanamayabileceği, bu nedenle verdiği onamı geri çekme seçeneğinin kişiden onam alınırken mutlaka belirtilmesi gerektiği ifade edilmiştir (Örnek Büken & Zeybek Ünsal, 2017).

### **Kişisel Verileri Koruma Kurulu:**

AB'nin 95/46/EC sayılı Veri Koruma Direktifine göre, kişisel verilerin hukuka aykırı olarak elde edilmesi, silinmesi, verilere erişilmesi gibi eylemlerin denetiminin bağımsız bir

kurul tarafından yapılması öngörülmüştür. Bağımsızlık, kurumsal, işlevsel ve ekonomik bağımsızlığın hepsinin birlikte bulunması şeklinde anlaşılmalıdır.

Söz konusu Direktifin 18. maddesinde düzenlenen denetleyici otorite (Supervisory authority) benzeri bir yapı 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 19. maddesinde düzenlenmiştir. Söz konusu kanun ile Kişisel Verileri Koruma Kurum ve Kurulları kurulmuş, Kurul idari ve mali özerkliğe sahip karar verici organ olarak belirlenmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 21/2. maddesinde, kurulun dokuz üyeden oluşacağı belirtilmiştir. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanlığı, iki üyesi Bakanlar Kurulu tarafından seçilmektedir. Söz konusu kanunun tasarisında 9 üyeden beşinin, Yargıtay, Danıştay, Türkiye Barolar Birliği, Yüksek Öğretim Kurulu ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu tarafından belirleneceği yönündeki düzenleme değiştirilmiştir. Bu açıdan tasarı halindeki düzenlemenin kurulun bağımsızlığı ve çeşitliliği açısından daha uygun olduğu kanaati oluşmuştur.

AB vatandaşı olan bireyler, eğer veri koruma haklarının ihlal edildiğini düşünüyorlarsa, Avrupa Birliği'nin yapısı içerisinde bulunan *European Personal Data Supervisor (EPDS)*'ye doğrudan başvuru yapabilmektedirler. *EPDS*, bu şikâyetleri dinleyip, inceleyebilir ve düzenlemelerin uygulanıp uygulanmadığından emin olmak için süreci izleyebilir. Bununla birlikte, *EPDS* AB Kurum ve organlarına kişisel verilerin işlenmesiyle ilgili her türlü tavsiyede bulunabilir. AB Komisyonu, herhangi bir sektörde kişisel verilerin işlenmesi ile ilgili yasa tekliflerini kabul edeceği zaman *EPDS*'ye danışmak zorundadır (Örnek Büken & Zeybek Ünsal, 2017).

### **Hassas verilerin korunması açısından 6698 Sayılı Kanun yeterli güvenceyi veriyor mu?**

Kişilerin savunmasız olmasına neden olabilecek potansiyele sahip olması nedeniyle özellikle kişinin sağlık verileri, cinsel yaşamı, genetik ve biyometrik verileri gibi biyomedikal alanı ilgilendiren hassas verilerin korunması konusu, hukuki ve etik açıdan büyük bir hassasiyet gerektirmektedir. Bu nedenle Avrupa Komisyonu'nun 108 sayılı Sözleşmesinde ve Avrupa Birliği'nin 95/46/EC sayılı Veri Koruma Direktifinde, bu tür veriler için geniş koruma istenmekte ve söz konusu veriler özel bir hukuki rejime tabi tutulmaktadır.

Avrupa Komisyonu Statüsü'nün 15.b maddesine istinaden AK No. R (97) 5 sayılı tavsiye metninde Bakanlar Komitesi üye ülkelerin hükümetlerine tavsiyelerde bulunmuştur. Bu tavsiye kararında belirtilen ilkelerin hukuki metin ve uygulamalara da yansıtıldığından emin olunması için gerekli adımların atılması gerekliliğinden söz edilmiştir. Söz konusu tavsiye

kararında sağlık verilerinin, tıbbi bakım ve araştırma ya da hastane yönetiminin dışında farklı sağlık bakımı sektörlerinde de kullanımının arttığına dikkat çekilmiştir (Örnek Büken & Zeybek Ünsal, 2017).

Kişisel verileri elde etme ve işleme aşamasında mahremiyetin korunması gerekliliği mutlaka vurgulanmakta, tıbbi verilerin de yalnız yerel kanunlarda uygun önlemler alındığında toplanıp işlenebileceği dile getirilmektedir. Buradan hareketle ülkelerin yerel kanunlarında uygun önlemleri alarak, temel hak ve hürriyetler ile mahremiyetin korunması, gizlilik en önem verilen değerler olarak ortaya çıkmıştır.

Gizlilik, bir kişinin kişisel verilerine üçüncü kişiler tarafından erişilmesini kontrol etme hakkı olarak nitelendirilmektedir. Dünya Sağlık Örgütü (DSÖ)'nün 2012 yılında yapmış olduğu bir çalışmada, artık günümüzde gizliliğe saygı ödevini kamu görevi olan tıbbın ilerlemesine yardımcı olma görevi içine katmaya ihtiyaç olduğu yönünde tartışmalar gelişmeye başlamıştır. Aynı çalışmada, Brezilya'nın, kişilerin verilerini kontrol etmelerine izin vermesi ve kişisel verilere yüksek derecede koruma sağlayan yasalara sahip olması açısından öncü olduğu belirtilmiştir. Ancak diğer ülkelerde olduğu gibi Brezilya'da da elektronik sağlık kayıtlarında hakların uygulanabilir olması için kullanılacak veri takibi (*data tagging*), uzaktan erişim (*remote access*) ve veri gizleme (*data obfuscation - data masking*) gibi teknik çözümlere referans gösteren bir mevzuat bulunmadığı da dile getirilmiştir (Örnek Büken & Zeybek Ünsal, 2017).

AK No. R (97)5 sayılı tavsiye kararında, bilgiye erişimin reddedilebileceği, sınırlandırılabilir ya da ertelenebileceği durumlar da dört başlık halinde sıralanmıştır. Eğer yasada öngörülmüşse ve demokratik toplumunun gereği olarak suçu önlemek ya da kamu güvenliği ve devletin güvenliğini korumak için gerekliyse, tıbbi verilere erişim reddedilebilir, kısıtlanabilir ya da ertelenebilir.

Bununla birlikte, kişinin bu bilgiye ulaşması onun sağlığı için ciddi bir zarar doğuracaksa, bilgiye ulaşması üçüncü kişiler hakkındaki bilgileri de ortaya çıkarıyorsa, ya da eğer genetik verilere dayalı olarak ortaya çıkan bilgi akraba, ya da soyuna ciddi zarar verecekse de erişimin reddedilip, kısıtlanabileceği hüküm altına alınmıştır.

İstatistik ya da bilimsel araştırma amaçlarıyla kullanılan verilerin, açıkça veri sahibinin gizliliğini ihlal etme riski varsa da veriye erişim reddedilebilir, kısıtlanabilir ya da ertelenebilir (Zeybek Ünsal & Örnek Büken, 2018).

## Sonuç

Bilgi ve iletişim teknolojileri alanındaki gelişmeler kaçınılmaz olarak tıp alanını da etkileyecek ve tanı/tedavi/rehabilitasyon alanlarındaki tıbbi uygulamaları değiştirecek, dönüştürecek. Bu değişim ve dönüşümden hem sağlık hizmetini sunanlar hem de bu hizmeti talep edenler kaçınılmaz olarak etkileneceklerdir. Tıbbi bilişimin ortaya koyduğu/koyacağı bu “yeni” durumların, en az etik değer harcayan ve en çok etik değeri koruyan bir yapıda olması, insana yararı gözetmesi, insanı amaca araç olarak gören yaklaşımdan uzak olması önemli olmalıdır.

Tıbbi bilişimdeki gelişmeler karşısında da aşağıdaki sorulara yanıt verebilecek disiplinler arası etik kurulların danışmanlık niteliğindeki kararları önemli olacaktır; Ne yapılmalıdır? Neye nereye kadar izin verilebilir? Yapılması mümkün olan her şey yapılmalı mıdır, yoksa bir sınırlama getirilecek midir? Bu sınırlama nasıl getirilecektir? Gerekli olan ile olmayan, izin verilebilir olan ile olmayan arasındaki sınır nasıl temellendirilebilir? Neyin yasaklanması nasıl temellendirilecektir?

Günümüzde sağlık verileri, sosyal medya, akıllı telefon uygulamaları, akıllı bilgisayarlar, hastane kayıt sistemleri vb. gibi pek çok araç aracılığı ile işlenebilmekte, saklanabilmekte ve aktarılabilir. Ancak, henüz gerekli ve yeterli teknolojik önlemler alınmadan kişisel sağlık verilerine erişim sağlanması, olumsuz ve geri dönülemeyecek sorunlara neden olabilecektir.

Kişinin özel alanlarının ve özel yaşamının ve bu alanlarla ilgili olarak elde edilen bilgi ve verilerin devlet müdahalesine karşı korunma hakkının, Birleşmiş Milletler İnsan Hakları Evrensel Beyannameyi düzenlemeleriyle güvence altına alındığı unutulmamalıdır. Devlet tarafından izlenen sağlık politikalarının, oluşturulan yasal düzenlemelerin de bu çerçevede değerlendirilmesi demokratik toplum gerekleri açısından önemlidir.

Diğer taraftan daha iyi sağlık hizmeti sunmak, en pahalı ve en son teknolojiyi uygulamak demek değildir, olmamalıdır. Çünkü daha yüksek teknolojinin sınırı yoktur. Ne yazık ki tıbbın bugün geldiği noktada geçerli olan tıbbi sistemler, kendisini sadece teknoloji uygulayıcısı teknik bir adam olarak gören ve yüksek teknolojiyi uygulamadığı zaman sürekli bir şey atladığı, hastası için “en iyiyi” yapmadığını düşünen bir hekim ya da araştırmacı tipolojisi yaratabilmektedir.

Bu alanda çalışan profesyoneller etik sorumluluklarının farkına varmadıkça, hiçbir düzenleyici sistem uygun şekilde çalışmaz. Fazladan yapılacak düzenlemelerin bir tehlikesi de profesyonellerin kendi sorumlulukları yerine, düzenlemelerle uyumlu olmaya dikkat sarf etmeleri yüzünden, ahlaki sorumluluk duygusunun göz ardı edilebilecek olmasıdır. Yani dış



denetim elbette önemli ve gereklidir (Araştırma Etik Kurulları, Hastane Etik Kurulları, Oviedo Biyotıp Sözleşmesi, Ulusal yasalar, Dünya Hekimleri Birliği Bildirgeleri, Türk Tabipleri Birliği Bildirgeleri...) ancak daha önemlisi iç denetim mekanizmalarının varlığıdır. Herhangi bir dış yapı/kurum tarafından denetlenmeden de içten gelen doğruyu yapma konusundaki motivasyonun varlığıdır.

## Kaynakça / References

- 6698 sayılı Kişisel Verilerin Korunması Kanunu, RG. Tarih: 07.04.2016 RG. Sayı: 29677 (erişim tarihi 3 Nisan 2017).
- Andorno, R. (2013). Principles of International Biolaw, Seeking common ground at the intersection of bioethics and human rights. Brussels: Bruylant.
- Büken N. (2016-I). Clinical trial ethics in Turkey in the context of some expectations and predictions. *Int J Clin Trials*, 3 (4), 180-186. doi: <http://dx.doi.org/10.18203/2349-3259.ijct20163954>
- Büken, N. (1997). Yardımcı Üreme Teknolojisi ve Bu Tekniklerin Uygulanmasından Doğan Etik Sorunlar, Etik Bunun Neresinde?. *ATO Yayını*, 85-99.
- Büken, N. (2011). UN Millennium Goals and Universal Declaration on Bioethics and Human Rights, Universal Declaration on Bioethics and Human Rights, Social Responsibility and Health Workshop, Bioethics Committee Turkish National Commission for Bioethics, İstanbul, Turkey.
- Büken, N. (2016-II). Opinions about the future of Clinical Trial in Turkey. *Journal of Clinical and Experimental Investigations*, 7 (3), 258-264. doi: 10.5799/ahinjs.01.2016.03.06072017
- Büken, N. (2019). CRISPR ve Etik. *Bilim ve Ütopya*, 298 (25).
- Büken, N. (2019). İnsan biyolojik materyalinin araştırma amaçlı olarak kullanılması ile ilgili araştırmacı ve araştırma etik kurul sorumluluğu. *Turkish Journal of Clinics and Laboratory*, 10(3), 413-405. <https://doi.org/10.18663/tjcl.413878>
- Cochrane, A. (2012). Evaluating 'Bioethical Approaches' to Human Rights. *Ethical Theory and Moral Practice*, 15(3), 309-22.
- Council of Europe contribution to the UN 2030 Agenda for Sustainable Development (2018). Retrieved from <https://www.coe.int/en/web/un-agenda-2030/home?desktop=true>
- Council of Europe. (2018). The modernised Convention 108: novelties in a nutshell. Retrieved from <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>.
- Council of Europe. (2019). Consultative Committee Of The Convention For The Protection Of Individuals with regard to Automatic Processing Of Personal Data (Convention 108) Report (T-PD(2018)09Rev) on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies
- Curtiss, T. (2016). Privacy Harmonization and the Developing World: The Impact of the EU's General Protection Regulation on Developing Economies. *WASH J.L. TECH & ARTS*, 12(1), 1-27.
- Dimitrov, DV. (2016). Medical Internet of Things and Big Data in Healthcare. *Healthc Inform Re*, 22(3), 156-163. <http://dx.doi.org/10.4258/hir.2016.22.3.156>
- Dolgin, E. (2019). AI face-scanning app spots signs of rare genetic disorders. *Nature*, doi: 10.1038/d41586-019-00027-x
- Fenwick, Kaal, & Vermeulen. (2017). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *American University Business Law Review*, 6 (3). <http://digitalcommons.wcl.american.edu/aublrvol6/iss3/1>
- Finn, Wright, & Friedewald. (2013). Seven Types of Privacy. In Gutwirth, Leenes, Hert, & Poulet (Eds.), *European Data Protection: Coming of Age* (s.3-33). Springer.

- Friedewal, Wright, Gutwirth, & Mardini. (2010). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation: The European Journal of Social Science Research*, 23(1), 61-7. <https://doi.org/10.1080/13511611003791182>
- Imison, Castle-Clarke, Watson, & Edwards. (2016). Delivering the benefits of digital health care. Nuffield Trust. Retrieved from <https://www.nuffieldtrust.org.uk/files/2017-01/delivering-the-benefits-of-digital-technology-web-final.pdf>
- Jones, L. D. et.al. (2018). Artificial intelligence, machine learning and the evolution of healthcare. *Bone Joint Res*, 7(3),223–225. <https://doi.org/10.1302/2046-3758.73.BJR-2017-0147.R1>
- Kang, Park, Cho, & Lee. (2018). Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices. *Int Neurourol J*, 22 (Suppl 2), S76-82. <https://doi.org/10.5213/inj.1836144.072>
- Kang, Park, Hwan Cho, & Lee. (2018). Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices. *Int Neurourol J*, 22, S76-82. 10.5213/inj.1836144.072
- Kuçuradi, İ. (2016). İnsan Hakları: Kavramları ve Sorunları. Ankara, Türkiye: Türkiye Felsefe Kurumu.
- Loh, E. (2018). Medicine and the rise of the robots: a qualitative review of recent advances of artificial intelligence in health. *BMJ Leader*, 2(2), 59-63. doi:10.1136/leader-2018-000071
- Methodist, H. (2016). Artificial intelligence expedites breast cancer risk prediction. *ScienceDaily*. Retrieved from [www.sciencedaily.com/releases/2016/08/160829122106.htm](http://www.sciencedaily.com/releases/2016/08/160829122106.htm)
- Nuffield Council on Bioethics. (2018). Artificial Intelligence in Healthcare and Research. Retrieved from <https://www.nuffieldbioethics.org/publications/ai-in-healthcare-and-research>
- Örnek Büken, N., & Zeybek Ünsal, Ç. (2017). Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi. *Hacettepe Hukuk Dergisi*, 7(2), 33-54.
- Quintana, O. (1993). International Bioethics? The role of the Council of Europe. *Journal of Medical Ethics*, 19,5-6. <http://dx.doi.org/10.1136/jme.19.1.5>
- Robinson, WK. (2018). Emerging Technologies Challenging Current Legal Paradigms. *MINN. J.L. SCI. & TECH*, 19 (2).
- Servick, K. (2019). Artificial intelligence turns brain activity into speech. *Sciencemag*. Retrieved from <https://www.sciencemag.org/news/2019/01/artificial-intelligence-turns-brain-activity-speech>
- Shaw, Hines, & Kielly-Carroll. (2017) Impact of Digital Health on the Safety and Quality of Health Care. Sydney: Australian Commission on Safety and Quality in Health Care. ACSQHC, ISBN: 978-1-925665-32-1.
- Stahl, Timmermans, & Flick. (2017). Ethics of Emerging Information and Communication Technologies: On the implementation of responsible research and innovation. *Science and Public Policy*, 44(3), 369–381. <https://doi.org/10.1093/scipol/scw069>
- The Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No 164).
- Tsang et. al. (2017). The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States. *Intellectual Property & Technology Law Journal*, 29 (8).
- Tzafestas,SG. (2018). Ethics and Law in the Internet of Things World. *Smart Cities*, 1(1), 98-120. <https://doi.org/10.3390/smartcities1010006>
- UNCTAD. (2016). Data protection regulations and international data flows: Implications for trade and development. Retrieved from [https://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)
- UNCTAD. (2019). Data Protection and Privacy Legislation Worldwide 2019. Retrieved from [https://unctad.org/en/Pages/DTL/STI\\_and ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx](https://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx)
- United Nations. (2018). Closing the Technology Gap in Least Developed Countries. UN Chronicles. Retrieved from <https://unchronicle.un.org/article/closing-technology-gap-least-developed-countries>

- Van der Sloot, B. (2018). A new approach to the right to privacy, or how the European Court of Human Rights embraced the nondomination principle. *Computer Law & Security Review*, 34 (3), 539-549. <https://doi.org/10.1016/j.clsr.2017.11.013>
- Van Est, Rinie et al. (2014). From Bio to NBIC convergence – From Medical Practice to Daily Life. Report written for the Council of Europe, Committee on Bioethics, The Hague, Rathenau Instituut
- Zanfır-Fortuna, G. (2018). Policy Brief: European Commission’s Strategy for AI, explained. Future of Privacy Forum. Retrieved from <https://fpf.org/2018/07/19/policy-brief-european-commissions-strategy-for-ai-explained/>
- Zeybek Ünsal Ç. & Örnek Büken N. (2018). Biyotıp Araştırmaları ile ilgili Olarak,” Kişisel Verilerin Korunması Kanunu” ve “Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik” Ne Diyor?. *Türkiye Klinikleri J Med Ethics Law Hist-Special Topics*, 4(1), 82-90.

