

## Mahremiyet kavramı bağlamında kişisel sağlık verileri The concept of privacy in the context of personal health data

M. Cumhuri İZGİ<sup>a</sup>

**Özet:** Bağımsız, tikel varoluşa sahip birey, benliğinin bilincine sahip olarak kendi kararlarını verebilmekte ve bu kararları doğrultusunda eyleyebilmektedir. Bu özellikler mahremiyet kavramının temellendirilmesini sağlamakta, böylece mahremiyet özerk kişi olmanın temel niteliklerinden biri haline gelmektedir. Mahremiyet kavramının bu bağlamda ele alınması sadece özel alana işaret eden bir kavram boyutunu aşmasına neden olmaktadır. Böylece mahremiyet, hem özgürlük bilinci gereği kendi kendini belirleme, hem de kendisi dışındaki çevreyi kendi ilgisine göre kontrol etme anlamına gelmektedir.

Kişisel verilerin korunması, bilgi güvenliğinin sağlanması mahremiyet kavramı içinde yer alarak birey olmanın olanağını sağlayan bileşenlerden kabul edilir, ulusal ve uluslararası belgelerde konunun önemine vurgu yapılır ve gerekli yaptırımlar oluşturulur. Hassas veri olarak kabul edilen kişisel sağlık bilgilerinin korunmasının, sağlık hakkının elde edilmesi, hekimlik mesleğinin temel değerlerinden olan sır saklama sorumluluğunun ve güvenin sürdürülmesi açısından ayrı bir önemi söz konusudur.

Tüm bu değerlendirmelere karşın Türkiye’de bireylerin tüm sağlık bilgileri kendileri bilgilendirilmeksizin, onamları alınmaksızın toplanmakta, depolanmakta ve yaygınlaştırılmaktadır. Bu makalede, mahremiyet ve sağlık hakkının örülenmesine neden olacak, birey olma olanağını zedeleyecek bu yaklaşım insan hakları bağlamında ele alınarak irdelenmektedir.

**Anahtar Kelimeler:** Gözetim, kişisel veri, mahremiyet, özerklik, kişisel sağlık bilgisi

--

**Abstract:** An individual, being independent and having a particular existence, consciously makes his/her decisions and acts upon. Such characteristics lay the foundations of the privacy concept. Thus, privacy becomes a fundamental feature of becoming an autonomous person. Considering the privacy concept within this respect, leads privacy to transcend its dimension highlighting merely the private sphere. Therefore, privacy means self-determination in accordance with liberty consciousness as well as controlling the outer sphere in accordance with his/her interest.

Protecting personal data and ensuring information security are involved in the concept of privacy and deemed as components enabling change of being an individual. National and international certificates emphasize on importance of this issue and necessary related sanctions have been imposed. Protection of personal health information, considered as sensitive data, has a distinct importance in terms of gaining health right, keeping the secret and sustaining the confidence, which are among fundamental values of profession of medicine.

In spite of all these assessments, all health information of individuals in Turkey have been collected, stored and extended without informing them and taking their consent. This study examines this approach, which will cause to tumble privacy and health rights and damage change of being individual, within context of human rights.

**Keywords:** Observation, personal data, privacy, autonomy, personal health data

<sup>a</sup> Öğr. Gör. Dr., Akdeniz Üniversitesi Tıp Fakültesi Tıp Tarihi ve Etik Anabilim Dalı, ✉ mcizgi@yahoo.com

## Giriş

Geçen yüzyılın tüm toplumları etkileyen en temel değişimlerinden birisi insan hakları kavramının kabul edilmesi, hukukla güvence altına alınması ve yaşama yansıtılabilmesidir. Böylece insan olarak doğmuş olmaktan kaynaklanması nedeniyle hukuk tarafından tanımlanmaksızın da varlığını ve kabul edilirliliğini sürdürebilmesi gereken söz konusu haklarla, yaşamın öznesi olan her bir kişinin herhangi bir ayrımcılığa uğramadan varoluşunu sürdürmesinin, kul olmaktan birey olmaya dönüşümünün olanağı sağlanabilmiştir. Birey olmanın sağlanabilmesi, özel ve kamusal alan tanımlanmasına temel oluştururken özel yaşamın da ortak, gizli ve özel alan olarak ayrışmasını sağlamıştır (1).

Birey olabilmenin varoluşsal temelini özerklikle sağlanabilmesinin kanıtı ve ötekinin özerkliğine saygı gösterilmesinin ahlaki zorunluluğu özerklik kavramının tanımında yer almaktadır. Özerkliğin kullanılabilmesi ise bireyin mahremiyetinin sağlanabilmesiyle olanaklıdır. Görüldüğü gibi birey olabilmenin olanağı hem özerklik hem de mahremiyet kavramlarıyla doğrudan bağlantılıdır. Söz konusu bu bağlantı özerklik yanında giz, mülkiyet, özel yaşam, beden, cinsellik gibi birçok kavramın mahremiyetle birlikte anılmasına neden olmuştur. Ancak bu anılma mahremiyet kavramının yerini alma şeklinde algılanmamalıdır.

## Mahremiyet kavramı

Mahremiyet kavramı ilk kez 1890 yılında Amerikalı yargıç Brandeis tarafından "yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak"(2) olarak tanımlanırken birey olabilmenin olanağı özgürlüğe de vurgu yapılmaktadır. Lyon ise yalnız bırakılmanın devlet, ekonomik kurumlar, diğer bireyler gibi tüm dışsal aktörleri kapsayacak şekilde genişletilmesi gerekliliğini belirtmiştir (3). Birey olabilmenin özgürlük, özgürlüğün de mahremiyetle doğrudan ilişkisi, modern devlet yapısı içinde mahremiyetin özgürlüğün kalbi olarak tanımlanmasına neden olmuş (4) ve mahremiyetin örselenmesinin özgürlüğün kısıtlanmasına yol açacağı sonucunu yaratmıştır. Belsey ve Chadwick ise mahremiyet kavramını bedensel-fiziksel, zihinsel-iletişimsel ve bilgi mahremiyeti şeklinde sınıflandırarak dışsal aktörler dışında bireye özgü gerekçeleri de kavrama eklemiştir (5).

Görüldüğü gibi mahremiyet kavramı felsefi anlamını bireyin bağımsız, tikel bir varoluşa sahip olduğu anlayışında bulur. Onun kendi benliğinin bilincine sahip olarak kendi kararlarını verebilme özelliği, tüm diğer bireyler karşısında sahip olunan dokunulamaz ve bağımsız varlık alanının- tikel varoluşa sahip olmasının- temellendirilmesini sağlar. Bu nedenle benliğin bilincine sahip olma, tikel varoluşun onaylanması anlamında mahremiyet kavramının dayanağını oluşturur. İnsanın toplumsal varoluşu ise, öteki ile ilişkiyle oluşması nedeniyle açık olmayı gerektirir. Ortaya çıkan kavram çifti, mahremiyet ve aleniyettir. İnsanın kendi başınlığı ve diğerleriyle birlikteliği olarak ayrılabilen bu iki varoluş tarzı, yaşam içindeki bireyin varlığı için olmazsa olmaz koşul olarak kabul edilir. Her iki durumda da mahremiyet bireyin özgürlük alanındadır ve bu nedenle özgür varoluşun, kendi kendini belirleme gücünün ifadesidir. Birey kavramı, kendi eyleminin tek belirleyicisi olma özelliğiyle kendi dışındaki dünyayı kontrol etme gücünü de kendisinde taşır ve merkezde olan birey için her şeyin paylaşımının sınırını belirleyen mahremiyet hakkının kabulüyle özgür istence ve düşünme yeteneğine dayalı karar verme özelliği oluşabilir. O halde mahremiyet, insanın varoluşu için ötekinin belirlenimine gereksinim duymama durumudur (6).

Türk Dil Kurumu mahremiyeti, gizlilik olarak tanımlamaktadır (7). Ancak yaşamın her zaman gizlemek amacıyla ötekinden saklanmadığı, sadece ötekinin istenmeyen yaklaşımlarından korunmak için göz önüne

açılmadığı dikkate alınırsa gizliliğin sadece mahremiyetin sağlanabilmesinin aracı olduğu görülecektir. Öte yandan Rachels'in de belirttiği gibi mahremiyetin gerçekleştirilmesiyle, ötekiyle paylaşılan bilginin içeriğinin ve derinliğinin değişimi sayesinde bireyin sosyal ilişkilerinin çeşitliliği ve özel yaşamı sağlanabilmektedir (8). Mahremiyet sadece saklanacak şeyi ifade etmek için değil, yaşam niteliğini artırmak için bir gereksinim, kendini gerçekleştirme, özerkliğini koruma yollarından biri olarak ele alınmalıdır (9-11). Sonuç olarak mahremiyet, toplumdan soyutlanma değil, ben ile öteki sınırının belirlenmesi, kontrol edilmesi olarak özetlenebilir.

### **Bilişim, gözetim ve mahremiyet**

Claude Shannon, kişisel özerklik gelişiminde çok önemli rolü olduğu ve bireysel özerklikle toplumsal özerklik kazanabilme arasında benzerlikler bulunduğu için, bilginin ahlaki öneme sahip olduğunu belirtir (12). Cairncross ise bilişim teknolojileriyle bilgiye ulaşmanın, iletişimin hızlanacağına ve bu gelişmelerin bireyin özgürlüğünü artıracığına vurgu yapmaktadır (13). Tam aksi bir düşünceyi Davies, kitleleri gizlice izleme ağının büyümekte olduğunu ve bu gizli izleme sisteminin kârı azamileştirmek, verimliliği artırmak, ulusal güvenliği güçlendirmek ve kolluk kuvvetlerine hizmet etmek üzere tasarlandığını belirterek “harcamalarımız, hayat tarzımız ve tercihlerimiz, mekânsal hareketlerimiz bilgi bankalarına yüklenmektedir. Bilginin hükümet ve iş dünyası tarafından paylaşılması amacıyla tüm bilgisayarlar birbirine bağlanırken bireysel özgürlüklerimize meydan okuyan tehlike ve riskler artmaktadır. Tehlike gerçektir ve sınır tanımamaktadır. Birkaç yıl içinde hepimiz yeni teknolojik düzenin bahtsız özneleri konumuna indirgenebiliriz” (14) şeklinde ifade etmektedir. Diğer yandan teknoloji sayesinde bireyin izlenebilirliği yanında devletin izlenirliğinin de arttığı, bunun da bireyin özgürlüğünün göstergesi olduğu belirtilmektedir. Ancak burada unutulmaması gereken demokratik bir toplumda devletin şeffaf olması, istenen ve demokrasinin tanımında yer alan bir özelliktir. Bu nedenle devletin bireylerce izlenirliğinin artması demokrasiye zarar vermek bir yana onu güçlendiren bir olgudur. Oysa bireyin şeffaflaşması, kendisiyle ilgili bilgilerin kendisinden habersiz toplanması, bunları silme hakkı tanınmaması, gözetim altında olmanın bilinmesi bireyin temel haklarına, birey olma olanağını yaratan özerkliğine, mahremiyetine, özgürlüğüne zarar vermektedir.

Son yüzyılda yükselen insan hakları kavramının toplumları etkilemesi ve birey kavramının merkeze yerleşmesi mahremiyet kavramının da içselleştirilmesini sağlamıştır. Bununla birlikte aynı süreçte teknolojinin hızlı gelişimiyle insanlar, günlük yaşamlarını daha rahat sürdürme, yaşam kalitelerini artırma ve birey haklarını kullanabilme gibi gerekçelerle gündelik işleri için kendilerine ait bilgileri vermeyi, güvenlik gerekçesiyle de kendi onamları olmaksızın konuşma ve davranışlarının kayıt altına alınmasını kabullenebilmişler, hatta kendileri talep etmişlerdir. Kayıt altına alınan bu bilgiler yine teknoloji sayesinde depolanabilmekte, analiz yapılabilmekte, paylaşımı sağlanabilmekte ve çok geniş toplum kesimlerine çok kısa sürelerde yaygınlaştırılabilmektedir. Ayrıca bu bilgilerin kimler tarafından ve nasıl kullanılacağı, bilginin sahibi tarafından da tam olarak bilinmemektedir. Teknolojiden yararlanarak bilgi toplama, depolama, kopyalama, transfer etme ve internet aracılığıyla yayma devlet tarafından toplum yararı temellendirmesiyle yapılırken; günümüzde şirketler de tüketici tercihleri temellendirmesiyle kendi veri tabanlarını oluşturmakta, şirketler arası veri paylaşımını kullanmakta ve bilgi elde etme kaynaklarını ve bunları işleme yeteneklerini her geçen gün artırmaktadırlar. Üretim araçlarını elinde tutan kapitalist sınıfın iktidarla ilişkisi göz önüne alındığında bilginin dolaşımının yaygınlığı anlaşılabilir. Solove da bilgilerin özel sektörler arası, özel sektörden kamuya ve kamudan özel sektöre sürekli bir akış halinde olduğunu belirtmektedir(15). Teknolojinin her geçen gün ucuzlaması gözetimin günümüzdeki sermaye yoğun özelliğini azaltarak daha çok şirketin bu olanağı elde etmesini sağlamaktadır. Böylece önceleri merkezi

yapının ulaşabildiği gözetim, her geçen gün yaygınlaşmakta, toplumlar ise teknolojinin sunduğu yararlardan vazgeçme ile mahremiyeti koruma arasında ikilem yaşamaktadır.

Tüm bu değişimler bireyin, veri tabanları içinde dijital kod olarak algılanmasına, “gözetim toplumu” kavramının ortaya çıkmasına neden olmuştur. Gözetim, iktidarla birey arasında gerilim üretebilen ancak iktidarların kitleleri kontrol etmek amacıyla sıklıkla başvurdukları denetim aracı olarak karşımıza çıkmaktadır. Bir başkası hakkında bilgi toplamanın, özellikli bir olay olmaktan çıkıp gündelik yaşamın içine girmesi, önemsenirliğini artırmıştır. Gözetim, bireyin mevcut sosyal düzene olan uyumunu da kontrol ederek güçlü bir sosyal denetim aracı olabilmektedir. Oysa mahremiyet hakkı gözetimden kaçınmayı gerekli kılar.

Gözetim konusu günümüzde Foucault’la merkezi bir öneme sahip hale gelmiştir. Foucault değerlendirmelerinde, modern toplumun disipliner bir toplum olduğunu belirtir. Söz konusu disiplinin aracı gözetimin, bürokratik örgütlenmenin sınırlarını aşan, sosyal yaşamı derinden etkileyen yapısı olduğunu vurgular ve elde edilen bilginin iktidarla ilişkisini öne çıkarır. Foucault gözetimi incelerken Bentham’ın Panoptikon hapishanesi tasarımını metafor olarak kullanmıştır. Burada dışarı bakan pencereden giren ışıkla hücredeki kişinin silueti kuledeki tek bir görevli tarafından takip edilebilmektedir. Kişiler sürekli görülebilir durumdadırlar; ancak gözetleyen görülememektedir; birey, bilginin nesnesidir, ama iletişimin öznesi olamamaktadır. Yani birey, edilgen durumda ve aynı zamanda da sürekli kontrol edilebilir haldedir. Bu kontrol hissi kişinin beklenen, iktidarca istenen davranışları yapmasına neden olmaktadır. Tüm bunları sağlamak için ise güç kullanmaya gerek kalmamaktadır. Böylece modern toplum gözetim ve disiplinin hâkim olduğu toplum haline gelmiştir (16). Günümüzde her yere yerleştirilmiş kameralar, her türlü kişisel verilerin toplanması bu yapının kanıtları olarak karşımıza çıkmaktadır. Bu noktada tüm bireyler tarafından kullanılan teknolojinin özgürlükleri mi yoksa iktidarı mı güçlendirdiği sorusunun yanıtı aranmalıdır. Giddens’in “totalitarizm, her şeyden önce gözetimin aşırı derecede odaklaşmasıdır” (17) ifadesi teknolojinin özgürleşmeyi sağladığı düşüncesinin, ironisini kendi içinde taşıdığını düşündürmektedir. Diğer yandan bireyin özgürleşme yanılması, daha çok bilginin toplanabilmesine de olanak tanımaktadır. Gary Marx görünmezliğini, irade dışılığını, belirli bireyi değil herkesi şüpheli olarak görmesini, emek değil sermaye yoğunluğunu, kullanım yoğunluğunu ve yaygınlığını teknoloji kullanımıyla genişleyen günümüz gözetiminin bazı özellikleri olarak belirlemektedir(18). Görüldüğü gibi teknoloji tüm dünyayı “Panoptikon” a çevirmekte, bireyleri olabildiğince şeffaflaştırmaktadır.

Mahremiyetin zedelenmesine neden olabilecek kadar bilginin veri tabanlarına verilmeyeceği iddia edilebilir. Ancak günlük yaşantımız içinde çok düşünmeden veya konforumuzun artmasını sağlamak için, kendimize ait birçok veriyi kendi isteğimizle verebilmekte ve tüm veriler veri tabanlarının bilgi kaynağı haline gelebilmektedir. Böylece Doroty Nelkin’in de önemle vurguladığı gibi gözetleme, toplum yaşamının içine olağan bir şeymiş gibi yerleşmektedir (19). Teknolojinin sağladığı bu olanakla insanın yaşamının her alanına -ticari bilgiler, tıbbi bilgiler, genetik bilgiler, tüketici olarak bireylerin ayrı ayrı özellikleri gibi- ulaşabilmek mümkün olmuştur. Gözetim sistemlerini kullanan herhangi bir örgüt kişisel detaylara ulaşmak için bireye sormak ve ondan izin alarak bilgiye ulaşmak yerine, diğer veri tabanlarında ona ait bilgilere ulaşmayı tercih etmekte ve bu durum kişisel bilgilerin meta haline gelmesine neden olmaktadır. James Rule ise bu durumu gözetim sistemlerinin ‘kendi kendisinden beslenmesi eğilimi’ olarak tanımlamaktadır (20). Mahremiyet sosyal ilişkilerin kurulması için gerekli öncülerden kabul edilirken gözetimin ise toplumdaki samimiyet, dostluk, güven değerlerini olumsuz etkilediği, gözetim sistemini anımsatan araçların bile mahremiyeti sınırladığı, örselenmesine neden olduğu belirtilmektedir (21, 22). Bireylerin

kendilerine ait bilgilerin kontrolünü ve denetimini kaybetmesi ve elde ettikleri bilgileri kullanmaya başlayan örgütlerin denetimi altına girmesi tehlikesi ortaya çıkmaktadır. Tüm bunlar bireyin yalnız kalma hakkını kullanabilme kontrolünün, mahremiyetinin, ortadan kalkmasına, insan onurunun zedelenmesine neden olmaktadır.

Dünyanın yaşadığı 11 Eylül saldırısı özel yaşama müdahale, verilerin toplanması ve işlenmesi konusundaki yaklaşımların daha kolaylıkla kabul edilerek yaşama geçirilmesine ciddi katkı sunmuştur. Bu noktada Benjamin Franklin'in "temel bir özgürlüğü, geçici güvenlik için terk edenler, ne özgürlük ne de güvenliği kazanacaklardır" sözünü hatırlamak gerekecektir. Bunun yanında telefon dinleme örneğinde olduğu gibi kanıtlanamayan ancak toplum genelinde hissedilen gözetim genel olarak güvensizliği ve korkuyu da yaratmaktadır. Bu şekilde belli amaç olmaksızın gerekli olabilir anlayışıyla verilerin toplanması bireylerin fişlenmesi olarak değerlendirilmektedir (23). Günümüz teknolojisi içinde geliştirilen 'Bulut' sistemiyle depolanan bilgilerin yok edilmesinin olanaksız hale gelmesi ve bilgileri kayıt altına alınan bireylerin, bilgilerini kayıt altına alanlarca da bilinmeyen gelecekteki olası kullanımların tehdidi altında kalabileceği göz önünde tutulmalıdır.

### **Kişisel veri**

Geçen yüzyılda yaygınlaşan modern devletin, aralarında eşgüdüm sağlanmış ve tek merkezden gelen bilgiyle hareket eden ve o merkezce yönetilen yapısı söz konusudur. Bu yapı kaçınılmaz olarak varlığını sürdürebilmek, amaçlarını gerçekleştirebilmek, sınırları içinde refahı sağlayabilmek gibi birçok nedenle bireylerin bilgisine gereksinim duymaktadır. Modern devlet, yönetenle yönetilen arasındaki ilişkinin yapısının değişmesine neden olmuş ve bireysellikten nesnellığe dönüşümü zorunlu kılmıştır. Bu dönüşüm bilgiye olan gereksinimi artırmıştır. Bununla birlikte gelişen teknoloji, bilgi toplama araçlarındaki çeşitliliği artırmış ve bu birbirini besleyen iki durum bireylerin gözetiminde de farklılaşmayı yaratarak merkezi gözetimi güçlendirmiş ve yaygınlaştırmıştır. Giddens bilginin önemini "bilgi toplama, otorite kaynaklarının kabile kültürlerinden çok daha geniş mekân ve zaman alanlarını kapsayan sosyal sistemlerin yapılanmasındaki rolü açısından temel önem taşımaktadır" (17) ifadesiyle vurgulamıştır.

Belirli veya belirlenebilir nitelikteki bir kişiye ait her türlü bilgi olarak tanımlanan "Kişisel Veri" kavramı, verinin bir kişiye ilişkin olması ve bu kişinin de belirlenebilir olması bileşenlerini kapsar. Kişisel veri kavramı isimden, tercihlere, duygu ve düşüncelere kadar çok geniş yelpazede ele alınan ve "ben" e ait bir kavramdır. Bu nedenle bireyin bu veriler üzerindeki denetim yetkisini kaybetmesi bireyin özgürlüğünün, özerkliğinin, mahremiyetinin kısaca "ben" olma özelliğinin kaybedilmesini getirir. Bu durum, bireye bağlı kavramın temel insan hakları bağlamında ele alınmasını gerekli kılmakta ve özünde bireyin korunmasıyla doğrudan bağlantısını temellendirmektedir. Tüm bunlar bireyin korunması amacıyla verilerin güvenliğinin sağlanmasından öte, bireyin "ben" e ait veriler üzerindeki denetim yetkisini gerektirmektedir.

Yaşadığımız postmodern süreçte, her şeyin metalaştırılması ve değer kavramının ekonomik değerler üzerinde yoğunlaştırılması tüketimin de hızla artmasını getirmiştir. Teknolojinin getirdiği hızla metanın ekonomik değere dönüşümü için sürecin gereksindiği hız boyutu birbirine sinerjik etki yapmaktadır. Kişisel veriler bağlamında süreç, veriyi de metalaştırmakta ve ekonomik değere dönüştürmektedir. Bu noktada dünyaya nasıl bakıldığı temel soru olarak ele alınmaktadır: Kişisel veriler bir meta mıdır? Korunması gereken bir hak mıdır?

Kişisel verilerle ilgili ortaya konan ekonomik temelli düşüncelerde söz konusu bilgilerin mülkiyet kavramı bağlamıyla ele alınması gerektiği vurgulanır. Bu düşüncede, mülk sahibi olarak bireyin istediği pazarlık

olanağını elde ettiği belirtilir. Ancak burada da mülkleştirilen bilgi yine metalaştırılmış hale gelmekte, birey olmaktan uzaklaşarak alıcı/satıcı rolü üstlenilmekte ve pazarlıkta tarafların eşit olmaması nedeniyle bireyin söz konusu mülkiyet hakkından vazgeçmesi söz konusu olabilmektedir (23).

Her bir birey için bir numara belirlenip ve bireye ait verilerin bu numarayla bağlantılı bir araya getirilerek tümleşik bilgi oluşturma düşünceleri 20. yüzyılın ikinci yarısında uygulanmaya başlanmış ve kişisel verilerle ilgili tartışmaları alevlendirmiştir. Bilgisayarların kullanılmaya başlanmasından sonra kişisel verilerle ilgili tartışmaların daha da artmasına neden olan diğer dönüm noktası internetin gelişmesidir. Günümüzde artık bilgisayar ekranlarının bir pencere olduğu genel kabul görmektedir. İnternet kullanıcısının aradığı her bilgi dışarıya da akararak veri tabanlarında depolanmaktadır. Bilgi akışı IP adresinin izlenmesi, çerez'lerin, casus yazılımların kullanımı, GPS'ler gibi araçlara kadar uzanan birçok teknikte sağlanmaktadır. Bireylerin kendi istemleriyle internet kullanıcı olmaları, web sitelerine üye olabilmek için kendi bilgilerini vermelerinin bireylerin rızası olarak kabul edilmesi gerektiği belirtilmektedir. Oysa bu noktada, bireylerin söz konusu bilgilerin nasıl depolanacağı, kullanılacağı, yaygınlaşacağı, ne kadar süreyle depolanacağı, ileride nasıl kullanılabileceği hakkında farkındalığının olup olmadığı, konuyla ilgili yeterli bilgilendirilmenin yapıp yapılmadığı dikkate alınmamakta, aydınlatılmış onamın aydınlatma bileşeni göz ardı edilmektedir. Ayrıca ilk kez bireyin kendi istemiyle bilgilerini vermesi nedeniyle rızaya dayandığı düşünülse bile, bu verilerin daha sonra toplanma amacı dışında amaçlarla işlenmesinin rızaya dayanmadığı son derece açıktır.

### **Kişisel veri ve hukuksal boyut**

Kişiyeye ait bilgilerin toplanması uygulamaları çok eskilere dayanmakla birlikte dünyada bireylerin mahremiyetlerinin bu örseleniştikten kurtarılmasına ilişkin özel yasal düzenlemeler 1970'li yıllara dayanmaktadır. Yirminci yüzyıla kadar kişisel verilerin korunması, en tipik örneğinin hekimlikte görüldüğü gibi güven değeri üzerinden sağlanmıştır. İnsan hakları kavramının toplumsal kabul edilirliliğinin ve bireysel içselleştirilmesinin yaygınlaşmasıyla birlikte teknolojiye yaşanan hızlı değişim bu süreci etkilemiştir.

Gözetim, toplumun her bireyini etkilediği gibi normatif sistemleri de etkilemektedir. Örneğin farklı veri tabanlarında ayrı ayrı duran veriler eşleştirmeler yardımıyla suçlarının hiçbir kanıtı oluşmamış kişiler için polis soruşturmasının başlamasına neden olabilmekte ve suçlu olduğu kanıtlanıncaya kadar kişilerin suçsuz olduğu ilkesi tersine işleyerek kişinin suçsuz olduğu kanıtlanana kadar suçlu olduğu varsayılabilmektedir (24). Sonuçta temellendirilebilir ve yasal olarak kabul edilir gerekçe olmaksızın söz konusu verilerin toplanması hukukun temel ilkelerinden olan suçsuzluk karinesiyle çelişmektedir.

Bireylerin sır alanlarına ait olduğu kabul edilen cinsel yaşam, dinsel tercihler, ırksal köken, sağlık bilgileri, genetik bilgi gibi konular hassas kişisel veri olarak kabul edilmekte ve daha özel koruma gerektirmektedir. Genetik bilgi biyolojik olarak bireyi "ben" yapan tüm bilgileri içermesi yanında o bireyle biyolojik bağı olan diğer bireyler hakkında da bilgi içermesi açısından farklı bir öneme sahiptir. Avrupa Birliği(AB) Yönergesi bu konuyu 8. maddede ele almış ve istisnai durumlarını ayrıca belirtmek şartıyla "Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır." ifadesini kullanmıştır (25).

Kişisel veriler bağlamında konunun hak boyutu unutulmamalıdır. İnsan Hakları Evrensel Bildirgesi(İHEB) madde 12 (26), Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi madde 17 (27), Avrupa



İnsan Hakları Sözleşmesi (AİHS) madde 8 (28) gibi birçok uluslararası belge mahremiyetin korunabilmesi amacıyla özel yaşamın gizliliğini temel insan hakkı olarak kabul ederek kişisel verilerin korunmasına vurgu yapmaktadır. Kişisel veriler 1950’de kabul edilen AİHS’de özel hayatın gizliliği bağlamında değerlendirilirken, 2000 yılında kabul edilen AB Temel Haklar Şartı’nda kişisel verilerin korunmasına ait özel bir madde oluşturulmuştur (29). Görüldüğü gibi günümüzde artık kişisel verilerin korunması özel yaşamın korunmasını aşan boyutuyla farklı bir hak başlığı olarak kabul edilmeye başlanmıştır. Kişisel verilerin korunmasına ilişkin ilk yasal düzenleme 1970 yılında Almanya Hessen Eyaletinde yapılmış ve 1977 yılında federal düzeyde Federal Almanya Veri Koruma Yasası haline dönüşmüştür. Ulusal düzeydeki ilk düzenleme ise 1973 yılında İsveç’te yürürlüğe girmiştir. Bu yasalardaki ortak amaç devletin elinde bulunan veri bankalarının şeffaflaşması ve böylece devlet lehine gelişen güç yoğunlaşmasının dengelenmesidir. Kişisel verilerin korunmasına yönelik ilk uluslararası çalışma ise OECD’nin 1980 yılında yayınladığı “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Kullanımının Korunmasına İlişkin Rehber İlkeleri”dir. Konunun gündemdeki önemi ve AİHS’de kişisel verilere yönelik özel bir madde bulunmaması nedeniyle 1981 yılında Avrupa Konseyi (AK) “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme”yi yayınlamıştır. Daha sonra 1990 yılında ilk kez, ortaya konan ilkelerin uygulanmasını denetleyecek yetkili ve bağımsız veri koruma organı kurulması önerisini de içeren BM’in “Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri” kabul edilmiştir(23). Avrupa Parlamentosu ve Konseyi’nin 24 Ekim 1995 tarihli ve 95/46/AT sayılı Kişisel Verilerin Korunması Yönergesi hem yarattığı uluslararası etki hem de yönergenin 57. maddesinin gerekçesindeki “...yeterli ve elverişli koruma seviyesini sağlamayan üçüncü bir ülkeye, kişisel verilerin transferi yasaklanmalıdır” ifadesiyle önemini korumaktadır (25).

Federal Almanya Anayasa Mahkemesi 1983 yılında Parlamento tarafından oy birliğiyle kabul edilen ve yapılacak nüfus sayımında yurttaşlardan bilgi edinilmesine olanak tanıyan, bilgi vermek istemeyen yurttaşa da yaptırım öngören, veri açıklığı ile gerekçelendirilen Nüfus Sayımı Yasası’nı Anayasa’ya aykırı bulmuştur. Aykırılığın gerekçesini de insan onurunun korunması ve kişiliğin korunması haklarına dayandırmış ve bu bağlamda bilgilerin geleceğini belirleme hakkını türetmiştir. Şeffaflaşan bireyin onurunun zedeleneceğini, kişiliğini özgürce gerçekleştirme olanağını kaybedeceğini vurgulayan yüksek mahkeme bireyin basit bir veri haline dönüşümünü engellemiş ve bireye kendi verileri üzerine tasarruf etme hakkını sağlamıştır(30).

Tüm belgeler genel olarak değerlendirildiğinde; kişisel verilerin hukuka uygun olarak işlenmesi, toplanma amacının belirli ve meşru olması, amacı aşan toplama olmaması, gereklilik süresince güncellenmesi ve amacın gerektirdiğinden daha uzun tutulmaması kriterlerinde ortaklaşıldığı görülmektedir. Bunlara ilaveten günümüzdeki metinler bireylere, kişisel verileri toplama ve işleme süreçlerinde bireyin bilgilendirilmesi, verilere erişim, verilerin düzeltilmesini isteme, verilerin işlenmesini istememe gibi hakları da tanımaktadır.

Kişisel verilerin korunması kadar önemli olan bir diğer konu ise verilerin güvenliğinin sağlanabilmesidir. Kişisel verilerin korunması birey olma olanağıyla doğrudan ilişkili olarak bireyin korunmasını sağlarken, veri güvenliği bireyin korunması için bir araç konumundadır. Kişisel veriler, bireyin sağlık gibi temel haklarına ulaşımı, yaşamın kolaylaştırılması gibi birçok nedenle bireyin onamıyla üçüncü kişilere verilebilmektedir. Bu aşamadan sonra artık verilere yetkisiz erişim, verilerin yayılması, verilerin yetkisiz kullanımı gibi verilerin güvenliğinin sağlanması ön plana çıkmaktadır. Sağlık hizmeti gibi güven değerinin temel olduğu alanlarda veri güvenliğinin sağlanması, hakkın elde edilebilmesi açısından önemlidir. Uluslararası tüm belgelerde önemi nedeniyle veri güvenliğinin sağlanmasına vurgu yapılmaktadır. Veri güvenliğinin sağlanması hakkında temel önlemlerden birisinin şifreleme olduğu belirtilirken bireylerin

şifreleme yöntemlerini kullanmasına suçla mücadele gerekçesiyle şüphelye bakılması, elektronik ortamdaki işlemlerin birçoğunda TC kimlik numarasının istenmesi ve son günlerde yürürlüğe giren sağlık hizmeti alabilmek için biyometrik kimliğin kullanılması uygulamasının birbiriyle çelişik olduğu görülmektedir. Türkiye'de kişisel verilerin korunmasına yönelik yasa hazırlamak amacıyla 13 Eylül 1995'te bir komisyon kurulmasına karşın henüz oluşturulmuş bir yasa mevcut değildir(23). Ancak yasanın olmaması konuyla ilgili yasal koruma olmadığı anlamına gelmemektedir. Birçok ülkede olduğu gibi Türkiye'de de konu, kaynağını 2010 yılına kadar özel yaşamın gizliliği hakkından almıştır. Ancak 2010 yılında Anayasa'nın 20. Maddesine eklenen fıkrayla<sup>b</sup> (31) konu farklı boyuta taşınmıştır. Bu maddede söz edilen kanunun halen yürürlüğe girmemiş olması, kişisel verilerin toplanması ve işlenmesini denetleyecek bağımsız bir organdan söz edilmemesi eksiklik olarak görülmekle birlikte kişisel verilerin korunmasının Anayasal güvence altına alınması önemlidir. Anayasa'nın Temel Hak ve Özgürlükler başlığı altında toplanan kişinin dokunulmazlığı, maddî ve manevî varlığı, kişi hürriyeti ve güvenliği, özel hayatın gizliliği ve korunması başlıklı maddeleri de kişisel verilerin korunmasıyla bağlantılıdır (31). Ayrıca Anayasa'nın 90. Maddesiyle (31) İHEB, AİHS, Biyotıp Sözleşmesi gibi kişisel verilere vurgu yapan birçok uluslararası belge yasal mevzuatın içine ve mevzuat hiyerarşisinin en üstüne yerleştirilerek mahremiyet hakkının yasal dayanakları oluşturulmuştur. Türk Ceza Kanununda da kişiler arasındaki konuşmaların rıza olmaksızın dinlenmesi ve kayda alınması, özel hayatın gizliliğinin ihlali, kişisel verilerin hukuka aykırı kaydedilmesi, süresi geçmiş olmasına karşın toplanan verileri yok etmeme gibi eylemlere karşın yaptırımlar belirlenmiştir. Bunların dışında Medeni Kanunda kişilik haklarıyla ilgili hükümler, Borçlar Kanununda ise işçilerin kişisel verilerinin korunmasıyla ilgili maddeler konunun yasal boyutlarını oluşturmaktadır (23).

### **Kişisel sağlık verileri ve mahremiyet**

Elektronik teknolojinin gelişmesi öncesi hasta hekim ilişkisinin tek boyutluluğu, Dünya Hekimler Birliği(DHB)'nin Sağlık Veri Tabanları ile İlgili Etik Düşünceler Bildirgesi'nde "bireyin kimliğini ortaya koyan fiziksel ve mental sağlığı ile ilgili kayıtlı tüm bilgi"(32) olarak tanımlanan kişisel sağlık bilgisinin hekimin kontrolü altında kalmasını, hekimin sır saklama ilkesini yerine getirmesini kolaylaştırmaktaydı. Ancak teknolojinin gelişmesi ve hakların bile metalaştırılması hasta hekim ilişkisini çok boyutlu hale getirmiştir. Bunun yanında sağlık bilgilerinin hassas kişisel veri olarak kabul edilmesi ve daha özenle korunmayı gerektirmesi, sır saklamanın yaşama geçirilmesini zorlamakta, konuyla ilgili yalnızca sağlık çalışanlarının duyarlılığı yeterli olmamaktadır. Diğer yandan bireyin sağlık bilgilerine ulaşımın daha iyi sağlık hizmeti sunmak için gerekliliğinin kabul edilmesi bu hassas bilgilere erişimin tartışma konusu olmasına neden olmaktadır. Oysa bu verilere ulaşımın kolaylaşmasının ve yaygınlaşmasının bireyin en temel haklarından olan sağlık hakkından bile vazgeçeceği durumları yaratabileceği, bireyin etiketlenmesi, sosyal ayrımcılığa uğraması gibi farklı birçok zararlanımlara da neden olabileceği göz ardı edilmektedir.

İnsana dair tüm uğraşların temel amaçlarından en önemlisi bireyin özerkliğinin korunması olmalıdır. Bu da tıp disiplinine hukuki gerekçeler dışında özerkliği koruma sorumluluğu vermektedir. Bireyin özerkliğine saygı göstermek onunla ilgili eylemlerde onamını almayı gerektirir. Sağlığa yaklaşım ve bu konudaki öncelikler bireyin yaşama dair değerleriyle ilintilidir ve teknik bilgi ile çelişebilir. Bu değerlere yapılacak müdahaleler, sağlığın genel kabul gören fiziki, psikolojik ve sosyal yönden tam bir iyilik hali biçimindeki tanımıyla çelişerek iyilik halinin sürdürülebilirliğine engel oluşturabilecektir. Olumlu amaç

<sup>b</sup> "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."



doğrultusunda yapılan eylemler bile önemli değer kayıplarına neden olurlarsa o amacın değer yükü tartışmalı konuma gelebilir. Bu nedenle amaç uğruna her araç kullanılabilir düşüncesinin etik geçerliliği kuşkuludur. Araç kullanımı etik açıdan tutarlı bir biçimde temellendirilmelidir(33).

Siegler'e göre mahremiyet, tıpta 'hastanın kişisellik ve gizlilik düşüncesine saygının gelişmesine' ve 'tıbbın temel bir amacı olan hastanın sağlık bakımının geliştirilmesine' olmak üzere iki amaca hizmet eder. Kişisellik ve gizlilik düşüncesine saygının bir sonucu olarak, hastanın en kişisel fiziksel ve psikolojik sırları mahcubiyetini ve hassasiyetini azaltmak için gizli tutulur. Mahremiyet olgusu hastanın hekime açıkladığı bilgilerin bir başkasına anlatılmayacağına inanmasına olanak sağlar. Bu şekilde hastalar doktorlarıyla dürüstçe ve açık açık konuşmaya teşvik edilir. Hasta ile doktor arasındaki bu güven bağı hem teşhis hem de tedavi sürecinde hayati önem taşır. Mahremiyetin bu önemli iki fonksiyonu, geçmişte olduğu kadar günümüzde de önemli ve gereklidir. Ne tıbbi teknolojideki gelişmeler ne de bazı hastalarla hekimler arasındaki haklar temelinde tüketici modeline doğru değişimler bu fonksiyonların yerini alamaz(34).

Mahremiyeti koruyarak kurulan güven tüm insan ilişkilerinde temel değer olarak ele alınır. Bu değer in izdüşümü olan güvenilir olmak da dinamik bir süreç olan yaşam içinde her gün yeniden üretilmesi gereken bir kavramdır. Kişiler ancak bu koşullarda gereksinim duydukları sağlık hizmetini almak için rahatlıkla başvururlar. Hasta hekim ilişkisinin güvene dayalı olması özelliğinin cinsiyetler arası ilişkilerin dini öğelerce düzenlendiği toplumlar da dahil olmak üzere herkes tarafından kabul görmesi, bu ilkenin evrenselleşmesini sağlamıştır (33). Hastaya ait bilgi, aitlik-mülkiyet ilişkileri bağlamında değerlendirilebilir ve bunların korunması ve gizliliği temelde sağlık profesyonellerinin sorumluluğundadır.

## Türkiye'de kişisel sağlık verileri

Mahremiyet kavramı, birey olma, bireyin kişisel bilgileri üzerindeki hak ve yetkisi kuramsal, hukuksal ve etik açıdan açık bir şekilde temellendirilmiş, kabul görmüş ve belgelere yansımış iken Türkiye'de kişisel sağlık verilerinin, Sağlıkta Dönüşüm Projesi anlayışının sonucu sağlık hizmetlerinin özelleştirilmesine bağlı olarak Sağlık Bakanlığı (SB), Sosyal Güvenlik Kurumu (SGK) ve özel sağlık sigortaları aracılığıyla toplanması ve metalaştırılarak ulusal ve uluslararası paylaşımı sağlanmaktadır. SGK'nun bütçe açıklarını kapatmak amacıyla sağlık verilerini sattığı iddiasının ulusal basında yer alması (35) konunun önemini artırmıştır. SGK'nın kuruluşuyla birlikte daha çok muhasebe amaçlı oluşturulmuş MEDULA adlı elektronik kayıt sistemiyle sınırlı olarak toplanan kişisel sağlık verileri artık daha kapsamlı toplanmakta ve yaygınlaştırılmaktadır. Son olarak SGK tarafından 1 Aralık 2013 tarihinden itibaren özel hastanelerde kullanımı zorunlu hale getirilen "Biyometrik Kimlik Doğrulama" (36) sistemiyle bireyin kimliğinin biyolojik ve değiştirilemez bir şekilde tespit edilmesi sağlanmaktadır. Halbuki AİHM'nin gözetimine alınan kişinin gözetim süresince alınan parmak izi ve DNA bilgilerinin suçsuzluğu kanıtlandığı zaman silinmesi gerektiğini belirten kararı söz konusudur (37). Ayrıca SB Türkiye Kamu Hastaneleri Kurumu Hastane Hizmetleri Başkan Yardımcılığı'nın Valiliklere yazdığı bilgilendirme yazısında "...kişisel veriler kapsamında olduğu hususunda tereddüt bulunmayan ve şahsa mahsus özellikleri yansıtan; parmak izi, göz retinası, iris, yüz şekli, ses, imza, avuç içi vs. gibi karakteristiklerin ölçülerek, bu bilgilerin bilgisayar sistemleri ve veri bankalarına kaydedilmesi suretiyle kimlik doğrulaması yapabilen cihazların -kişilerin açık rızaları olmaksızın- mesai takibi maksadıyla kullanılması hukuken uygun olmadığı" ifadesi özel hastanelerdeki biyometrik kimlik doğrulamasının hukuksuzluğunun ve bu uygulamanın bireylerin sağlık hizmeti alamama tehdidiyle bir anlamda zorunlu olarak gerçekleştirildiğinin itiraf edilmesidir(38). Bununla birlikte 23 Ekim 2013 tarihinde yayınlanan Özel Sağlık Sigortaları Yönetmeliği(39) hükümleri gereği sigorta yaptırmak isteyen her bireyin, sigorta şirketinin depolanan kişisel sağlık verilerine ulaşımına

izin vermesi veya sigorta şirketinin kişinin sağlık durumunu tespit edebilmesi amacıyla isteyeceği hekim görüşü için gerekli masrafı kendisinin karşılaması gerekmektedir. Tamamlayıcı sağlık sigortasının gündemde olduğu günümüzde sigorta yaptırmak isteyen kişi sayısının her geçen gün artacağı göz önüne alındığında kişisel sağlık bilgilerinin nasıl yaygınlaşabileceği tahmin edilebilir. Ayrıca yine aynı yönetmeliğin 16. Maddesinde sigorta şirketinin, elindeki sağlık bilgilerini “diğer yetkili merciler” şeklinde açık uçlu olarak tanımlanan kurumlara da verme zorunluluğu, yaygınlaşmanın farklı boyutunu göstermesi açısından önemlidir. Kişisel sağlık verilerinin bilimsel çalışmalar kapsamında, nitelikli sağlık hizmetinin planlanması ve uygulanması, sağlık politikalarının geliştirilmesi, yasal belge oluşturulabilmesi amacıyla sınırlarının etik değerlerce de çizilmiş olması koşuluyla kullanımının gerekliliği genel kabul görür. Ancak, hukukun ve etik ilkelerin birey mahremiyetinin korunması bağlamında kişisel sağlık verilerini koruma ve veri güvenliğini sağlama ödevini yüklediği SB’nın, bu yükümlülüğü yerine getirmemesi ve Sağlık-Net 2 adlı bilgisayar programı aracılığıyla tüm kamu ve özel sağlık kuruluşlarından hastalara ait her türlü bilgiyi -bütün kimlik, adres, iletişim bilgileri, sağlık geçmişi, özürüllük durumu, medeni hal, alkol-madde-sigara kullanımı, tetkik sonuçları, 15-49 yaş arası kadınların, doğum, düşük türü ve sayıları, kullanılan aile planlaması yöntemi vs.- herhangi bir filtreleme, koruma ve denetleme önlemi ve hastaların aydınlatılmış onamlarını almadan depolaması, yaygınlaştırması bireyin şeffaflaşması, mahremiyetinin örselemesi tehlikesini içermekte, mesleğin andlara yansıyan binlerce yıllık en temel değerlerini sarsmaktadır. Söz konusu bilgisayar programı zorunlu olması ve ülke çapında merkezi bir sistem olması nedeniyle dünyada uygulanan tek örnektir(40). Bu sistem nedeniyle DHB Hasta Hakları Bildirgesi, Avrupa Hasta Haklarının Geliştirilmesi (Amsterdam) Bildirgesi, İnsan Hakları ve Biyotıp Sözleşmesi, Hekimlik Meslek Etiği Kuralları, Hasta Hakları Yönetmeliği, Deontoloji Tüzüğü gibi birçok ulusal ve uluslararası belgede hasta hakkı olarak belirlenen gizlilik hakkı engellenerek yasal sorumluluk çığnenmektedir.

Değerlerle çelişen söz konusu uygulama 2.8.2013 tarihli Bazı Kanun ve Kanun Hükmünde Kararnelerde Değişiklik Yapılmasına Dair Kanun’un 73. Maddesinin “h” fıkrasının 3. bendiyle<sup>c</sup> (41) yasalaştırılmıştır. Söz konusu yasada kişisel sağlık bilgilerinin toplanma amacı tüm uluslararası belgelerin aksine genel bir ifadeyle açıklanmakta, gerekçe açık olarak ifade edilmemektedir. Ayrıca toplanacak verilerle ilgili herhangi bir sınıflandırma yapılmamakta, tüm veriler toplanmakta, bilgi toplama süreklilik göstermekte, verilere kimlerin nasıl ve hangi oranda ulaşacağı ve toplanan verilerin üçüncü kişilerle paylaşımıyla ilgili herhangi bir düzenleme yer almamaktadır. Bunlarla birlikte bilgisi toplanan bireyler uygulamayla ilgili bilgilendirilmemekte, onamları alınmamakta, bireylerin kendi bilgilerine ulaşımı, düzeltilmesi ve/veya silmesi olanakları düzenlenmemektedir.

Sonuç olarak yürürlüğe konan yasal düzenlemeler ve sürdürülen uygulamalar göz önüne alındığında SB’nın kişisel sağlık verilerinin toplanmasını sağlık hizmetlerinin programlanabilmesi temellendirmesi ile sürdürdüğü ancak verileri metalaştırmak yanında bireyleri şeffaflaştırmak gibi isteklerinin de olduğu görülmektedir. Bunun yanında Türkiye’deki sağlık ve hukuk alanının temel bileşenlerinden olan Türk Tabipleri Birliği, Türk Dişhekimleri Birliği, Türk Eczacılar Birliği ve Türkiye Barolar Birliği’nin 3.12.2013 tarihli ortak basın açıklaması, alanın meslek örgütlerinin görüşlerini ortaya koymaktadır. Söz konusu basın açıklamasında; kişisel sağlık verilerinin kayıt altına alınmasının hizmetlerin sürekliliğinin sağlanması ve niteliğinin artırılması, yasal belge oluşturulması, bilimsel ve istatistiksel çalışmaların yapılabilmesi açısından önemi belirtilmekle birlikte uygulamanın ulusal ve uluslararası belgelerle koruma

<sup>c</sup> “(1) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işleme ve paylaşmaya yetkilidir.”

altına alınan kişinin mahremiyetinin ortadan kalkmasına ve böylece kişilerin zarar görmesine neden olmaması gerektiği vurgulanmaktadır. Ayrıca Türkiye’de kişisel sağlık verilerinin kamu ve özel kurumlar tarafından açıkça, amaç belirlenmeksizin ve zorunluluk yaratılarak toplandığının ve verilerin ticari meta haline getirildiğinin altı çizilmekte ve bu uygulamaların kabul edilemez olduğu belirtilmektedir. Böylece sağlık çalışanlarının en temel meslek etik ilkesi gereği olan ve hastanın ölümüyle bile sonlanmayan sır saklama sorumluluğunun ortadan kaldırılmakta olduğu vurgulanmaktadır. Toplumun bilgilendirilmesi ve düzenlemelerin yasal kurallara ve etik ilkelere uygun olarak ivedilikle yeniden yapılandırılmasının da önemi ifade edilmektedir (42).

Tüm bunların yanında ulusal basında “Flaş talimat” başlığıyla verilen bir haberde; Cumhurbaşkanı’nın Devlet Denetleme Kurulu (DDK)’ndan “Kamuya ait veri bankalarının (vergi, nüfus, tapu, emniyet ve adli veri sistemleri gibi) güvenlik ve kişisel veri mahremiyetine ilişkin iç kontrol sistemlerinin yeterliğinin denetimi ve değerlendirilmesi”ni istediği belirtilmektedir (43). DDK’nun konuyla ilgili raporu(44) ve “yurttaşın gizli bilgileri ortalıkta dolaşüyor” başlığıyla (45) ulusal basına yansımaları incelendiğinde; konuyla ilgili acilen yasal yapının oluşturularak hayata geçirilmesinin, toplumu bilinçlendirmenin ve bu düzenlemelerin devlet yapısını tek bir kurum olarak ele almadan kendi içinde her bir kurumun özellikleri ayrı ayrı göz önüne alınarak özel düzenlemelerin yapılmasının gerekliliği ortaya çıkmaktadır.

## Sonuç

Kişisel verilerin korunması kavramının özel yaşamın gizliliğinin ihlalini aşan boyutları olduğu, konunun mahremiyetin zedelenmesiyle ilişkisi aşıkardır. Günümüzde genel anlamda bilginin güç olduğu kabul görürken kişisel verilerinin toplanması, gözetim altında olmak bilginin nesnesi konumundaki birey için mahremiyetinin örülenmesi nedeniyle güçsüzlük anlamına gelmektedir. İnsan onuruna saygı, insan varoluşunun özel ahlaki değerlere sahip olduğunu ve kişinin kendi ilgileri, amaçları ve seçimlerine göre davranması ve mahremiyetinin korunması gerektiğini kabul etmeyi getirir. Bu anlayışın tıbbi yansımaları, sağlık profesyonellerinin kişisel bilgilerin korunmasına yönelik görevlerini oluşturur. Mahremiyetin korunması görevinin tarih sürecinde tıbbi antlarda ve etik kodlarda yerini alması, bu kavramın ahlaki öneminin güçlü göstergesi olarak karşımıza çıkar.

Teknolojinin sağladığı bilgi akışındaki özgürlük, bunun sağladığı çıkar ilişkileri ve bilgi kaynağının sağladığı yarar ile birey olma kavramının gerektirdiği denetim yetkisi günümüzde yaşanan ikilemlerin temelini oluşturmaktadır. Çözüm, harcanacak değer minimumda tutulması ve birey olmanın olanağını yaratan özerklik, mahremiyet kavramlarının gereği bireye denetim yetkisinin sağlanmasıyla yaşama geçirilebilecektir. İnsanın saf bilme merakından kaynaklanan bilim yolculuğu doğayı kontrol etme ve yaşamı kolaylaştırma istemleriyle birleşerek devam etmiştir. Bu yolculuğun günümüzde bireyin özgürlüğünün sınırlandırılmasını yaratması, ironisini kendi içinde taşır ve kabul edilemez bir durumdur.

Gözetim nedeniyle bireyin bir matriks içinde dijital bir veri haline gelmesi kendini çıplak, korumasız hissetmesine neden olabilmektedir. Bu matrikste matematiksel bir kesinlik içinde rakamsal bir anlatıma dönüşen birey için yaratıcılık, doğanın sağladığı rastlantısallık olumsuz etkilenecektir. Bu şekildeki varoluşu, halen “insan” olarak kavramsallaştırmak ne kadar olanaklı olabilecektir? Tüm bunların yaşanmasının önlenmesi, öncelikle kişisel verilerin korunmasının sağlanması ve böylece mahremiyet hakkının bireye geri verilmesiyle olanaklı olabilecektir. Refahın, mahremiyet hakkını kullanan bireye de ulaşabileceği toplumsal yapıların oluşturulması gerekecektir. Kişisel verilerin korunmasına yönelik yasal düzenlemelerin önemi yadsınmamakla birlikte yeterli değildir. Bireylerin hakları konusunda yeterince aydınlatılması ve mahremiyet hakkına yönelik farkındalıklarının artırılması yasal düzenlemelerin yaşama

geçirilebilmesinin olanağını yaratacaktır. Kişisel verilerin mahremiyeti örselemeden kullanımının sağlanabilmesinin temel yolu, kavramın tanımında yer alan kişinin belirlenebilirliğinin kaldırılması yani bilgilerin anonimleştirilmesi olacaktır. Böylece bilgilerin kişisel niteliği ortadan kalkarak sadece veri özelliği söz konusu olacaktır.

Teknolojik ilerlemeyi engellemenin olanağı olmamakla birlikte, onun yaygın bir etik duyarlılıkla geliştirilmesinin ve bu bilinçle kullanılmasının sağlanması gelecek açısından çok önemlidir. Mahremiyetin tıbbi uygulamaların merkezindeki yerinin korunması gerekmele birlikte bunun gerçekleştirilmesi için sadece sağlık çalışanlarının duyarlılığı yeterli değildir. Sağlık alanında mahremiyetin korunmasının yalnızca sağlık çalışanları üzerinden temellendirilmesi toplumun ve bireylerin sağlık hakkının sağlayıcısı devletin sorumluluğunun göz ardı edilmesi demektir.

## Kaynaklar

1. Yüksel, M. Modernleşme ve mahremiyet. *Kültür ve İletişim Dergisi*, 2003, 6 (1): 15-27
2. Diffie W., Landau S. *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge, Massachusetts, The MIT Pres, 1998
3. Lyon D. *Elektronik göz gözetim toplumunun yükselişi*. Çev. D. Hattatoğlu, Sarmal Yayınevi, İstanbul, 1997
4. Westin AF. *Privacy and Freedom*, London, Mansell Pres, 1970
5. Belsey A., Chadwick R. *Medya ve Gazetecilikte Etik Sorunlar*, Çev. N. Türkoğlu, Ayrıntı Yayınları, İstanbul, 1998, s.110
6. İzgi MC, *Etik Açısından Yaşlı Mahremiyeti: Huzurevi Örneğinde Hizmet Alanlar ve Verenler Açısından Bir Değerlendirme*. Doktora Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü. 2009.  
<https://tez.yok.gov.tr/UlusalTezMerkezi/SearchTez>
7. [http://www.tdk.gov.tr/index.php?option=com\\_bts&arama=kelime&guid=TDK.GTS.52a9fe5e09a762.06529287](http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.52a9fe5e09a762.06529287) Erişim Tarihi 12.12.2013
8. Rachels J. *Why privacy is important*, Computers, Ethics, and Society, ed., M. Ermann D. Williams, M. B. Shauf, Oxford University Press, Inc. 1997,s:69-76
9. Akgüç Ö. *Mahremiyet açısından elektronik gözetim ve denetim: Tüketicinin denetimi, gözetimi ve online alışveriş siteleri üzerine bir uygulama*, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2004.
10. Newell PB. Perspectives on Privacy, *Journal of Environmental Psychology*, 1995, 15(2): 87-104
11. Beauchamp TL., Childress Jf. *Principles of Biomedical Ethics*, 2nd edition, Oxford university press, New York, 1983
12. Alfino M., Pierce L. *The Social Nature of Information*, Library Trends, 2001, 49 (3): p.471
13. Cairncross F. *The Death of Distance*, London, Orion Business Books, 1997
14. Davies S. *Big Brother: Britain's Web of Surveillance and the New Technological Order*, London, Pan Books, 1996
15. Solove DJ. *The Digital Person, Technology and Privacy in the Information Age*. ABD, New York University Press, 2004 s: 3
16. Foucault M. *Hapishanenin Doğuşu*. Çev: Mehmet Ali Kılıçbay, 3. Baskı, İmge Kitabevi, Ankara, 2006
17. Giddens A. *The Nation-State and Violence*. University of California Press. 1987
18. Marx GT. *Undercover: Police Surveillance in America*. University of California Press, 1988
19. Dedeoğlu G. Gözetleme, Mahremiyet ve İnsan Onuru. *TBD Bilişim Dergisi*, 2004(89)  
<http://okul.selyam.net/docs/index-43267.html> Erişim Tarihi 13.12.2013
20. Rule JB., Mcadam D., Stearns L., Uglow D. Documentary identification and mass surveillance in the

- United States. *Social Problems*, 1983, 31 (2): 222–234
21. Johnson Deborah G. *Computer Ethics*, Prentice-Hall, Inc., 2001, s: 120-127
22. Değirmenci P. *Net toplumunda etik ve mahremiyetin ihlal edilmesi kaygılarına yönelik bir araştırma*. Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2002
23. Küzeci E. *Kişisel Verilerin Korunması*. Turhan Kitabevi, Ankara, 2010
24. Shattuck, J. Computer matching is a serious threat to individual rights. *Communications of the ACM*, 1984, 27 (6): 538–541
25. [www.ihop.org.tr/dosya/coe/EC\\_DIRECTIVE\\_95\\_46\\_Kisisel\\_Veriler.pdf](http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf) Erişim Tarihi 13.12.2013
26. <http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf> Erişim Tarihi 13.12.2013
27. <http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktarafli-soz/bm1.html> Erişim Tarihi 13.12.2013
28. <http://www.inhak.adalet.gov.tr/temel/temel.html> Erişim Tarihi 13.12.2013
29. <http://www.ihd.org.tr/index.php/san-haklarylgeleri-mainmenu-96/900-avrupa-birligi-temel-haklar-bildirgesi.html> Erişim Tarihi 13.12.2013
30. Michael J. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Development in Information Technology*, London, Dartmouth & UNESCO Publishing, 1994
31. <http://www.tbmm.gov.tr/anayasa.htm> Erişim Tarihi 13.12.2013
32. *Sağlıkla İlgili Uluslararası Belgeler*, TTB Yayınları, 2. Baskı, 2009, s:177
33. Oğuz NY. *Psikiyatride onam ve aydınlatılmış onam: Etik, hukuk ve bilim açısından*. Doktora Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, 1994
34. Siegler M. Confidentiality in Medicine – A Decrepit Concept., *N.Engl. J. of Med.* 1982, 307 (24): 1518 – 1521
35. <http://www.taraf.com.tr/haber/2-4-milyarlik-is-golge-sirketin.htm> Erişim Tarihi 13.12.2013
36. [http://www.sgk.gov.tr/wps/portal/tr/e\\_sgk/diger\\_uygulamalar/duyurular?CSRT=2299697816787176046](http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular?CSRT=2299697816787176046) Erişim Tarihi 13.12.2013
37.
38. TC Sağlık Bakanlığı Türkiye Kamu Hastaneleri Kurumu Hastane Hizmetleri Başkan Yardımcılığı'nın 2.10.2012 tarih ve 00438835 sayılı yazısı
39. <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2013/10/20131023.htm&main=http://www.resmigazete.gov.tr/eskiler/2013/10/20131023.htm> Erişim Tarihi 13.12.2013
40. <http://www.ttb.org.tr/ksv/index.php/hakkinda/toplanma> Erişim Tarihi 13.12.2013
41. <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2013/08/20130802.htm&main=http://www.resmigazete.gov.tr/eskiler/2013/08/20130802.htm> Erişim Tarihi 13.12.2013
42. *Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştay Kitabı*. Yayına Hazırlayan: Hasan Oğan. TTB yayınları, Ocak 2014, s 88-93
43. <http://www.sabah.com.tr/Gundem/2012/11/07/gulden-flas-talimat> Erişim Tarihi 13.12.2013
44. <http://www.tccb.gov.tr/ddk/ddk56.pdf> Erişim Tarihi 13.12.2013
45. <http://birgun.net/haber/yurttasin-gizli-bilgileri-ortalikta-dolasiyor-8088.html> Erişim Tarihi 13.12.2013