YENİ MEDYA
DERGİSİ
Hakemli, uluslararası, e-Dergi

Sayı Vol , 16, Bahar Spring, (2024)
https://dergipark.org.tr/tr/pub/yenimedya
DOI » https://doi.org/10.55609/yenimedya.1424182

Dijital Mahremiyet ve Kurumsal Sorumluluk: Kişisel Verilerin Korunmasında İletişim Teknolojilerinin Kamusal Rolü

Digital Privacy and Corporate Responsibility: The Public Role of Communication Technologies in the Protection of Personal Data

Sıla TANIŞIK • **Sevil BAL**

Araştırma Makalesi Research Article Başvuru Received: 27.01.2024 ■ Kabul Accepted: 29.04.2024

ÖZ

Teknolojinin insan-doğa etkileşimi bağlamında inşa ettiği araç-ortamlar, düşünme ve deneyim biçimlerinin dönüşmesine ilişkin tartışmaların zeminini oluşturmaktadır. Görmenin ve görülmenin yüceltildiği çağın kültürü olarak; göstergeler üzerinden tanımlanan anlamlandırma ve bireysel hazzın bu yeni formu, dijital iletişim teknolojileri üzerinden gerçekleşmektedir. Bu yönüyle; deneyim, ilişki, çatışma, gözetim, mülkiyet, iktidar tartışmasının merkezinde ise dijital mahremiyet olgusu yer almaktadır. 21. yüzyılda, dijital-kamusal alanda "kamu yararı", "hak-yükümlülükler" çerçevesinde öne çıkan mahremiyet sorunsalı; literatürde bilgi-iletişim teknolojilerindeki gelişmeler, kamusal alan-özel alan ikircikliği, teknoloji kullanım yetkinliği ve özel alanın ihlali üzerinden incelenmektedir. Diğer yandan, kişisel mahremiyetin, dijital-kamusal görünürlüğünü, kurumsal sorumluluk ve ortak fayda ekseninde vatandaş-tüketicilerin mahremiyetinin gözetilmesine ilişkin dijital platformlar ve uygulamaları üzerinden değerlendiren araştırmaların oldukça sınırlı olduğu görülmektedir. Bu çalışmanın amacı; kişisel verilerin korunmasına ilişkin hukuki çerçeveyi kapsayan bir kuram-uygulama tartışmasından hareketle; makro kurumların mahremiyet olgusuna ilişkin farkındalık ve görünürlük çalışmalarını ve mahremiyeti konu olan özne deneyimine yansımalarını dijital teknolojilerin sunduğu olanak(sızlık)lar üzerinden tartışmaya açmaktır. Çalışmada nitel araştırma yöntemi, betimsel analiz ve doküman incelemesi gerçekleştirilmiştir. Literatür tartışmasında iletişim teknolojileri ve mahremiyet olgusu, denetim-gözetim bağlamında kavramsal ve kuramsal olarak ele alınmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanun maddeleri yorumlanarak; mahremiyet tartışmasının ilkelerine işaret edilmiştir. Son olarak; kurumların kişisel veri mahremiyeti görünürlüğü/farkındalığı sağlayan çalışmaları, katkıları, sorun alanları ve etik tartışmasına değinilmektedir. Çalışmanın sonucunda, mevzuat üzerinden temel hatları belirlenmiş bir yasal prosedürün tanımlandığı; ancak sistemin yönetimi, kamuoyuna aktarımı ve vatandaş-tüketici farkındalığının artırılmasına yönelik uygulamaların geliştirilmesi-çeşitlendirilmesi gerektiği görülmüştür.

Anahtar Kelimeler: Dijital Mahremiyet, Kişisel Veri, Iletişim Teknolojileri, Kamusal-Özel Alan, Gizlilik.

ABSTRACT

The mediums built by technology in the context of human-nature interaction constitute ground for discussions on transformation of ways of thinking-experience. As the culture of the age where seeing-being seen are glorified, this new form of signification and individual pleasure defined through signs are realized through digital communication technologies. The phenomenon of digital privacy is at the center of the debate on experience, relationship, conflict, surveillance, property and power. In the 21st century, problematic of privacy, which comes to fore within the framework of "public interest", "rights and obligations" in digital-public sphere, is analyzed in literature through developments in information-communication technologies, public-private ambivalence, competence in use of technology, violation of private sphere. There is minimal studies examine digital-public visibility of citizen-consumers' privacy on the axis of corporate responsibility, common good. In this study; starting from a theory-practice discussion covering legal framework on the protection of personal data; to discuss awareness and visibility studies of institutions regarding privacy and reflections on the subject's experience of privacy through possibilities offered by digital technologies. Qualitative research method, descriptive analysis were used. In literature disussion, communication technologies and phenomenon of privacy were discussed conceptually-theoretically in the context of control, surveillance. Law No. 6698 on the Protection of Personal Data was interpreted, principles of privacy debate were pointed out. Studies, contributions, problem areas, ethical discussions are addressed. It is seen that basic outlined legal procedure is defined through legislation. Practices for management of system, public disclosure and raising citizen-consumer awareness need to be developed, diversified.

Keywords: Digital Privacy, Personal Data, Communication Technologies, Public-Private Space, Confidentiality.

Giriş

Bilgi ve iletişim teknolojilerinin gelişmesi ile birlikte dijital uzama olan yakınlık, mahremiyet olgusunun kapsam ve sınırlarının yeniden tanımlanmasına neden olmaktadır. Gündelik hayatta zaman-mekandan bağımsız dijital uzamlar ve bu uzamlar aracılığıyla paylaşılan içerikler; kişisel bilginin "veri" olarak dolaşıma girmesi, erişim güvenliği, denetim mekanizmaları gibi çeşitli başlıkları kapsayan mahremiyet kavramı, teknolojik gelişmelerle birlikte farklı boyutlarıyla ele alınmaktadır. Dijital çağ öncesinde bu olgu daha çok bir "bedensel gizlilik" vurgusuyla ilişkilendirilirken; bilgi ve iletişim teknolojileri çağında kişisel verilerin korunması, sosyal ağların kullanımına yönelik gizlilik gibi hususlarla gündeme gelmekte; teknoloji deneyimi ve denetimine ilişkin bir "veri yönetimi" tartışmasıyla biçimlenmektedir. Kişisel veriler kapsamında e-posta adresleri, sosyal medya hesapları, çevrimiçi alışveriş uygulamaları; eğitim, sağlık elektronik bankacılık ve e-finans gibi alanlarda hizmet sunan sistemlere (e-devlet, e-nabız, medula, eba vb.) erişim güvenliği, veri sahipliği, kullanımı ve denetim mekanizmaları açısından "kişisel verilerin korunması" hususunu gündeme getirmektedir.

Dijital iletişim mecralarında kişisel verilerin toplanması, işlenmesi ve depolanmasının kamusal hizmetler açısından sunduğu olanakların yanı sıra, bireyin istek ve iradesi dışında kamusal platformlar yoluyla gerçekleştirilen kişisel veri paylaşımının gizlilik ve güvenlik ihlalleri kapsamında potansiyel bir risk alanı oluşturduğu görülmektedir. Veri güvenliği ihlalleri, kötü niyetli yazılımlar, phishing saldırıları ve sosyal mühendislik bu risk unsurları arasında gösterilmektedir (Çetin 2014: 5). Veri güvenliği ihlalleri, dijital ortamlarda bireysel kullanıcı hesaplarının yanı sıra; kurumsal sistemlere ve kamusal bilginin arşivlendiği veri bankalarına izinsiz olarak girilmesi ve kişisel verilere erişmesiyle gerçekleşmektedir. Örneğin, bir veri tabanı korsanlığı saldırısı sonucunda kullanıcıların kişisel verileri çalınabilmekte, ifşa edilebilmekte veya değiştirilebilmektedir. Bu tür ihlaller finansal bilgiler, sağlık verileri, sosyal güvenlik numaraları gibi hassas kişisel verilerin kötüye kullanılmasına yol açabilmektedir. Benzer şekilde kötü niyetli/casus yazılımlar, kullanıcıların bilgisayarlarına veya diğer dijital cihazlarına sızarak kişisel verilerin ele geçirilmesi amacıyla kullanılmaktadır. Bu tür yazılımlar genel itibariyle ara yüze kullanıcılar fark etmeden dahil olmakta; veri izleme, çalma veya manipüle etmeye dayalı ihlaller, kullanıcı istek ve iradesi dışında gerçekleşmektedir. Phishing ise dijital ortamlarda kişisel veri güvenliğin tehdit eden bir diğer saldırı yöntemidir (Bhavsar, vd., 2018). Saldırganlar sahte web siteleri, e-postalar veya mesajlar aracılığıyla kullanıcıları yanıltarak kişisel verilerini elde etmeyi hedeflemektedir. Örneğin; burada kullanıcılar, banka hesap bilgilerini veya giriş kimliklerini girmeleri için sahte bir web sitesine yönlendirilmektedir. Bu tür saldırılar sonucunda kullanıcıların, kişisel verilerine ilişkin bir güvenlik açığı oluşmaktadır. Sosyal mühendislik yoluyla ihlal ise, bir kurum personelini taklit veya manipülasyon yoluyla kişisel verilere erişim olarak tanımlanmaktadır. Sosyal mühendislik saldırıları genellikle telefon dolandırıcılığı, kişisel bilgilerin telefonda veya yüz yüze talep edilmesi ve bu veriler üzerinden işlem yapılması gibi uygulamaları içermektedir (Akca, 2016). Dolayısıyla mahremiyet kavramının çerçevesini önemli ölçüde kişisel veri güvenliğinin ihlali tartışması oluşturmakta; manipülasyon, yanıltıcı hikayeler veya dolandırıcılık yoluyla bireyin tasarrufundaki bilgiler, istem dışında dolaşıma girmektedir (Altıntaş&Barkuş, 2023: 50).

21. yüzyılda, dijital-kamusal alanda "kamu yararı" ve "hak-yükümlülükler" çerçevesinde öne çıkan mahremiyet sorunsalı; literatürde bilgi ve iletişim teknolojilerindeki gelişmeler, kamusal alan-özel alan ikircikliği, teknoloji kullanım yetkinliği ve özel alanın ihlali üzerinden incelenmektedir. Diğer yandan, kişisel mahremiyetin, dijital-kamusal görünürlüğünü, kurumsal sorumluluk ve ortak fayda ekseninde vatandaş-tüketicilerin mahremiyetinin gözetilmesine ilişkin dijital platformlar bürokrasisi ve uygulamaları üzerinden değerlendiren araştırmaların oldukça sınırlı olduğu görülmektedir. Bu nedenle dijital mahremiyet, tüketici-vatandaş haklarına ilişkin kurumsal sorumluluğun bir parçası olarak

değerlendirildiğinde, kanun yoluyla sınırları belirlenen kişisel verilerin korunması ilkesinin, kuruluşlar düzeyinde dijital platformlara yönelik hangi çalışma ve uygulamalarla işlerlik kazandığı ve bu noktada olanak ve sorunların neler olabileceği konusu, temel bir araştırma problemi haline gelmektedir. Yeni iletişim teknolojileri ve etkileşim yoğunluğu da göz önünde bulundurulduğunda; mahremiyetin dijital-kamusal alandaki görünürlüğü, dijital eylemlerin bireysel ve gündelik karar ve eylemlerin bir uzantısı olarak kurumsal bir veri iktidarı oluşturması gibi hususlar kişisel veri güvenliği, denetim ve gözetim tartışması açısından önem kazanmaktadır.

Bu çalışmanın amacı; kişisel verilerin korunmasına ilişkin hukuki çerçeveyi de kapsayan bir kuram ve uygulama tartışmasından hareketle; makro kurumların mahremiyet olgusuna ilişkin farkındalık ve görünürlük çalışmalarını ve bunun mahremiyeti konu olan özne deneyimine yansımalarını dijital teknolojilerin sunduğu olanak(sızlık)lar üzerinden tartışmaya açmaktır. Çalışmada, nitel araştırma yöntemi ile betimsel analiz ve doküman incelemesi gerçekleştirilmiştir. Nitel araştırma yöntemi, yukarıda çerçevesi çizilen boyutlarıyla dijital mahremiyet olgusunu kişisel verilerin korunması ve kurumsal sorumluluk hattında kapsamlı olarak ele alınması amacıyla tercih edilmiştir. Bu kapsamda, bu alanda yapılan nitel ve nicel çalışmaların bir derlemesini sunmak amacıyla betimsel analiz; bununla birlikte kişisel verilerin korunmasına yönelik ulusal-uluslararası düzenlemeler ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, nitel araştırmalarda işlevsel bir bilgi kaynağı olarak değerlendirilen doküman analizi yoluyla incelenmektedir. Literatür tartışmasında iletişim teknolojileri ve mahremiyet olgusu, denetim-gözetim bağlamında kavramsal ve kuramsal olarak ele alınmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanun maddeleri yorumlanarak; mahremiyet tartışmasının hukuki kapsamı, özel alan, gizlilik-denetim ilkelerine işaret edilmektedir. Son olarak; kurumların kişisel veri mahremiyeti görünürlüğü/farkındalığı sağlayan çalışmaları, katkıları, sorun alanları ve etik tartışmalarına değinilmektedir.

İletişim Teknolojileri Bağlamında Dijital Mahremiyet ve Gözetim Tartışması

Mahremiyet kavramı, gelişen iletişim teknolojileri ile birlikte; literatürde modern anlamda bilinen mahremiyet (gizlilik) hakkı olarak 1890'da hukuk alanında iki avukatın ifadelerinde yer almakta; Amerikalı yargıç Brandeis tarafından "yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak" biçiminde tanımlanmaktadır (Bennett, 2009; İzgi, 2014). Kavram, Westin (1967) ve Altman'ın (1975) erken dönemli çalışmalarında ele alınmakta; günümüzde de farklı tartışmalara zemin oluşturmaktadır. Altman (1975) mahremiyeti "bir kimsenin kendisine veya grubuna ulaşma gayreti üzerindeki seçici kontrolü" olarak tanımlamaktadır. Bir diğer tanımda mahremiyet; "bireyin yalnız başına kalma ile başkalarıyla birlikte olma isteği arasındaki karşılıklı bir alan" (Yüksel, 2003: 78) ve "kişinin diğer insanların meraklı bakışlarından ve müdahalelerinden uzak olma hali ya da durumu" (Aydemir, 2012:5) olarak belirtilmektedir. Bu bağlamda "mahremiyet"in bireyin genel anlamda bir hak ve özgürlük deneyimi ve sınırı olarak kavrandığı ve tanımlandığı görülmektedir.

Mahremiyet kavramı bu yönüyle; bireysel, toplumsal, iktisadi, politik ve kültürel, teknolojik iklimden etkilenen ve farklı tarihsel, yerel, bölgesel, küresel örnekler üzerinden incelenmesi gereken bir art alana sahiptir (Yıldız, 2021). Bu nedenle, kavrama ilişkin deneyim ve sınırların kapsam ve gerekçelerine yönelik net bir tanımlama ve çerçeveleme yapmak da zorlaşmaktadır (Bennett, 2009). Kokolakis (2017), mahremiyet yaklaşımlarının üç boyutta ele alındığını belirtmektedir. Bunlar; bireyin varlığına yönelik haksız ve izinsiz müdahale olarak "kişi mahremiyeti", bireyin bulunduğu yer, bölge, alanın paylaşımı ve/veya güç/müdahale yoluyla değişikliği olarak "bölgesel mahremiyet" ve bu çalışma kapsamında ifade edilen, izinsiz ve yasal olmayan yollarla kişisel bilgilere erişim, saklama ve değişiklik eylemi olarak "bilgi mahremiyeti"dir. Bu üç boyut mahremiyeti fiziksel, bölgesel ve kişisel bilginin korunmasına ilişkin hak ve sorumluluklar üzerinden güvence altına almanın gerekliliğine işaret etmektedir (Kokolakis, 2017).

Mahremiyet bu açıdan modern insanın kamusal sınır iradesini tanımlayan ve inşa eden temel bir insan hakkı olarak ifade edilebilir. Bu yönüyle de insan onurunu destekleyen örgütlenme özgürlüğü ve ifade özgürlüğü gibi hakların temelini oluşturmaktadır. Mahremiyet ile ilgili tanımlar birçok bağlamda farklılık göstermesine rağmen, hukukta ortak ve yaygın mahremiyet tanımları bedensel, bölgesel, bilgi ve iletişim gizlilikleri üzerine yoğunlaşmaktadır. Kavram olarak mahremiyet, kişilerin yalnız kalabildikleri, düşünebildikleri, davranabildikleri, diğer bireylerle hangi sınırlarda ilişki ve iletişim kuracaklarına kendilerinin karar verdiği bir alanı ifade etmektedir (Yüksel, 2003). Bu bağlamda mahremiyet hakkı da bireylerin özel alan ve kamusal alandaki edimlerini, diğerleri ile ne ölçüde paylaşacaklarını belirleme hakkı olarak değerlendirilmektedir.

Mahremiyet kavramının sınırlarının iletişim teknolojileriyle yeniden çizilmeye başladığı süreçte ise; zaman-mekandan bağımsız dijital uzamlar ve bu uzamlarda üretilen içerikler; birey, grup ve kurumların psikolojik, sosyolojik, kültürel yapı-koşullar çerçevesindeki değişim ve gelişiminden etkilenmekte; aynı zamanda da tüm bu yapı-kurum-eylemin bir veri platformuna dönüşmesiyle sonuçlanmaktadır. Dil, din, etnik köken ve sosyal yaşantı gibi kimlik unsurlarını kapsayacak şekilde kültür, mahremiyet kavrayışını biçimlendirmekte; mahremiyet olgusundaki dönüşüm de kültürel çeşitliliği sağlamakta ve dijital mecralara taşıyarak dönüştürmektedir. Özel hayatın gizliliği ilkesi çerçevesinde, bu alanı daraltan gelişmeler, bireylerin kişisel olarak ifade edilebilecek bilgilerine dair kurumsal bir mahremiyet kavrayışının oluşması, tanımlanması, sınırlandırılması ve ihlalleri ve kamu yararının gözetilmesi gibi konuların yeni iletişim teknolojileri açısından da kapsamlı şekilde açıklanmasını gerektirmektedir.

Dijital teknolojilerin başlangıcı olarak; internetin bir mahremiyet ağı inşası ve örgütlenmesi biçiminde ortaya çıkışı, bu tartışmanın iki temel eksende ilerlemesine neden olmaktadır. İnternet öncesi çağda, kişisel bilgilerin kapsamlı veri sistemlerinde depolanması ve bireyin mahremiyeti diğer bireyler devletler ya da ticari şirketlerin uygulamalarının güvenliğine ilişkin tartışmalar sınırlı iken; internet tabanlı erişim olanakları ile birlikte; gittikçe yaygınlaşan farkındalık, güvenlik ve hukuki sorumluluk tartışmaları ve nitelik-niceliğe ilişkin çeşitli araştırmalar önem kazanmaktadır. Toplumsal ilişkiler ağı, bankacılık uygulamaları, interaktif etkileşim, platformların dijitalleşmesi hususları birlikte düşünüldüğünde, bireysel hareketliliği hızlandıran ve özel-kamusal alanı aşındıran bir nitelik arz etmektedir. "Dünyayı küçük bir bilgisayar ekranına ya da telefona sığdıran bu dijital ortam, yarattığı sınırsız özgürlük illüzyonu ile bireyin kendisine dair ne varsa hiç sorgulamadan sanal ortama aktarmasını normalleştirmiş ve onu bu ortamın öznesi haline getirmiştir" (Kalaman, 2017:2).

İletişim olgusu ve yeni iletişim teknolojileri bağlamında da mahremiyet tartışması önemlidir. Bilgi, birikim, tutum ve davranışların aktarımı ve anlamlandırılma pratiği olarak iletişim, özellikle son yıllarda teknoloji tartışmalarıyla birlikte tanımlanan bir hal almaktadır. Dijital platformların birey, grup, kurum ve ilişkiler yoluyla etkileşimi, özel alanın sınırları itibariyle, "mahremiyet" kavramının üzerinde düşünmeye sebep olmaktadır. Mahremiyet kavramının sınırlarının iletişim teknolojileriyle birlikte yeniden çizilmeye başladığı süreçte; siber uzamda güvenirlik açısından belirsizlik oluşturan ve güvenli erişim ilkesini ihlal eden hususlar, kişisel veri tartışmasında bilginin nerede ve hangi koşullarda görülebileceği, paylaşılabileceği, saklanabileceği tartışmalarına ve bu kapsamda da bireysel veriyi kullanan kurumların sorumluluğuna işaret etmektedir.

Teknolojik determinizm ve gözetim toplumu tartışmaları çerçevesinde, her türlü verinin denetim mekanizmasının işlevsel bileşeni olarak kaydedilmesi ve arşivlenmesi hususunda belirleyici bir rol üstlendiği ve teknolojik gelişmelerin bu gözetim sürecini sıradanlaştırdığı görülmektedir. Bilgi ve iletişim teknolojileriyle beraber sosyal paylaşım ağlarının, etkileşimli iletişim medyasının özel alan olmaktan çıkıp kamusal hale gelmesiyle iktidar ve sermaye sahiplerinin "gözetleme ve

sergileme" ifadelerini meşru hale getirdiği ve bunun sıradan bir uygulama olduğunu savunan görüşler mevcuttur. Özel olanın teşhiri bu anlamda, yeni teknolojinin olanakları ekseninde özel alanların kamusallaşmasının kurumsallaşması olarak ifade edilmektedir (Çaycı, 2016; Bağlı, 2011: 72). İletişim ve bilgi teknolojilerinin gelişmesi beraberinde gözetim kavramının gündeme gelmesine ve bireylerin gündelik hayatlarının denetim mekanizmaları (sermaye sahipleri ve iktidarlar) tarafından gözetime maruz kalmalarına sebebiyet vermektedir. Bireylerin huzur ve güven arayışı tesisi referansıyla gözetime razı olmaları (Dolgun, 2005, s.84-93) ve bunu içselleştirmelerine yönelik değerlendirmeler Foucault'un (2015; 2019) panoptikon kavramının, sinoptikon ve omniptikona dönüşen bir gözetim-denetim süreci üzerinden değerlendirilebilir Örneğin; 11 Eylül 2001 terör olayları bu açıdan, gözetim teknolojileriyle var olan veya yok edilen verinin dijital platformlarla izlendiği ve bu şekilde aynı anda birey-kurum-eylem-ülke-yönetim açısından da tüm eylemlerin takip edilebildiği ve yeni eylemlerin inşa edilebildiği bir iktidar formu olarak değerlendirilebilir. Böylelikle Francis Bacon'a atıfla "bilgi" bir güce dönüşürken; gözetim ve iletişim teknolojileri devletin ideolojik aygıtları olarak görünür olmanın temsiline karşılık gelmekte ve giderek kabul görmektedir. Bazı sonuçlar, otoriter ulusların gözetim ve sansüre dayalı faaliyetlerini arttırdığı önermesini ortaya koymaktadır. Özellikle İran, Suriye ve Çin: ABD Şirketlerinin ya da kendi teknolojileriyle gözetim, takip ve sansür yazılımları satın almaktadır. Amerikan Sivil Özgürlükler Birliği tarafından yapılan bir araştırmada, çok sayıda şehirde polis departmanlarının yasal izin olmaksızın binlerce kişiyle ilgili konum takip verilerini edindiği belirtilmektedir (akt. Çaycı, 2016, Gore, 2014, s.116-118). Dolayısıyla mahremiyet, kişisel verilerin korunması ve kurumsal sorumluluk bağlamı açısından teknolojik belirlenim, enformasyon toplumu ve gözetimin iletişim teknolojilerine ilişkisini irdeleyen kuramsal tartışmaların temel savları incelenebilir.

Tarihte ilk kez 1900'lü yılların başında Amerikan Sosyolog Thorstein Veblen (1909) tarafından ortaya atılan bir kavram olan teknolojik belirlenimcilik (determinizm) ilkesi; toplumsal dönüşümün temel gerekçesini teknoloji kavramıyla temellendirerek açıklamaktadır. Teknolojik determinizmin savunucuları, toplumun teknolojik gelişmeden etkilendiğini ve teknolojik gelişmeyle şekillendirildiğini iddia etmektedir. Buna göre; herhangi bir sosyal değişimin teknoloji kavramını içerisinde barındıran "teknoloji, iletişim teknolojisi ve medya" aracılığıyla denetlenmesinin mümkün olduğu görüşü savunulmaktadır. Toplum, yeni teknolojilere ve yeniliklere uyum sağlamak durumundadır. Dolayısıyla, teknolojik gelişmenin olumsuz sonuçları, teknolojinin doğasından değil, insanlar tarafından kullanım niteliği, yoğunluğu ve yetkinliğine dair kısıtlardan kaynaklanmaktadır. Toffler (1996) da teknolojiyi, insan yaşamının tüm alanlarında kaçınılmaz bir etkiye sahip olan tüm değişikliklerin belirleyicisi olarak yorumlamaktadır. McLuhan'ın (1994) teknolojik deterministyaklaşımı, iletişim teknolojilerindeki güç potansiyelini ve mahremiyet tartışmasıyla bağlantısını ifade etmek açısından katkı sunmaktadır. Luhan'a göre; aynı mesaj farklı ortamlarca iletildiğinde, farklı kitlelere farklı etkilerle ulaşabilmektedir. Bu noktada tarım toplumu ve sanayi toplumu olarak adlandırılan süreçlere enformasyon toplumunun eklenmesinde bilişim teknolojileri önemlidir. Bunun sonucunda da enformasyon teknolojileriyle gelişen gözetim pratikleri, mahremiyet yerine şeffaflık prensibinin kabul görmesine neden olmaktadır.

Manuel Castells (1996: 158-163) bilgi iletişim teknolojilerini, topluma dışsal ve adapte olunması gereken bir mekanizma olarak yorumlama fikrini eleştirmektedi "Teknoloji toplumu belirlemez, teknoloji toplumdur" ifadesiyle Castells, teknolojiyi, toplumun teknik değişimle şekillendiği ve teknik değişimin toplum tarafından şekillendirildiği bir sosyal süreç olarak ele almaktadır. Pierre Lévy tek taraflı teknolojik belirlenim kavramını da kabul etmeyi reddetmektedir. Ona göre "küresel sosyo-teknik sistemlerin analitik bir bakış açısı olarak teknoloji, geri kalandan bağımsız olarak oluşan, çeşitli etkileri olan ve kendi kendine çalışan gerçek bir nicelik değil, insan fenomeninin maddi ve yapay tarafına vurgu yapan bir görüştür." Siber

uzayın bir sosyal hareketin parçası olduğunu, grup liderlerinin, şifrelerinin ve mantıksal beklentilerinin olduğunu söylemektedir. Dahası, Levy, herhangi bir ilişkinin göz önünde bulundurulması durumunda, siber uzayın belirlenmeden çok daha karmaşık olacağını savunmaktadır. Ona göre, sosyal ve kültürel olgular, son derece karmaşıktır ve kısmen, otomatik olarak sürdürülen veya bastırılan, birbiriyle ilişkili belirsiz süreçler bütünüdür. Toplum teknolojik gelişmelerden etkilenmekte, olumsuz etkiler teknolojinin doğasından değil, insanların teknolojiyi yetersiz kullanımından kaynaklanmaktadır ve yeni teknolojilerin ortaya çıkması ve kullanılması sosyal düzenin sonucudur.

Gözetim toplumu tartışmalarıyla da bağlantılı olarak teknolojik belirlenim ilişkisi bugünün koşullarında; kimlik gösterme, parola girme, yüz tanıma ve parmak izi tanıma teknolojilerinden birini kullanma gibi birçok örnek üzerinden gündelik yaşamda rutin uygulamalar olarak içselleştirilen bir gözetim ağına işaret etmektedir. Bu noktada gözetimin kuramsal tarihine değinmek önem arz etmektedir. Michel Foucault (2015) ve Zygmunt Bauman'ın (2013) vurgularıyla, iletişim ve eyleme yönelen bir sistematik izleme yoluyla kontrol altına alma biçiminde tanımlanan gözetim kavramı, yine Bauman tarafından modernite kavramıyla ilişkilendirilmekte; yazar tarafından bu dönemde yeniden inşa edilen toplumsal yapı ve ilişkilerde gözetimin, yaşamın birçok alanına sızdığı ve yayıldığına dikkat çekilmektedir (Bauman ve Lyon, 2013: 10-11 ve 90).

Gilles Deleuze benzer bir tartışmayı "kontrol toplumu" ifadesiyle değerlendirmekte; William Staples (2008) ise günümüz gözetiminin, "modern yaşamın bir zamanlar sorgulanması bile akla gelmeyen anlamlarının, sembollerinin ve kurumlarının gözlerimizin önünde çözülmesinden dolayı, temel özelliği parçalanma ve belirsizlik olan" kültürlerde meydana geldiğini ileri sürmektedir (Staples, 2008: 85).

Yukarıda tartışılan çerçevede; kişisel verilerin korunması bağlamında mahremiyet olgusu ve gözetimi-denetimi tartışmasını, yapılan araştırmaların bir tasnifi üzerinden değerlendirebilmek mümkündür. Türkiye'deki literatüre bakıldığında; mahremiyet kavramını tarihsel olarak iktisadi ve sosyokültürel temelde, kamusal alan-özel alan ikiliği ve modernite kavramları çerçevesinde inceleyen çalışmalar (Yüksel, 2003a; 2003b); hak-sorumluluk ilişkisi kapsamında ulusal ve uluslararası hukuk kuralları ve müktesebatı üzerinden değerlendiren araştırmalar (Tekin, 2014); mahremiyeti denetim ve gözetim tartışmaları çerçevesinde ele alan incelemeler (Yavuz, 2022); özellikle son dönemde yapay zeka tabanlı program ve uygulamaların kullanımı ve güvenirliğini irdeleyen araştırmalar (Başkaya ve Karacan, 2022); sağlık, finans gibi belirli sektörlerdeki kişisel veri ve mahremiyet tartışmasına odaklanan çalışmalar (İzgi, 2014); mahremiyet ve kişisel veri paylaşım farkındalığına ilişkin ampirik araştırmalar (Eroğlu, 2018) öne çıkmaktadır. Bu açıdan, mahremiyet kavramını iletişim alanı üzerinden kurumsal ve hukuki sorumluluk bağlamında değerlendiren disiplinlerarası çalışmaların literatürde katkı sunacağı düşünülmektedir.

Kişisel Veriler Korunmasına İlişkin Uluslararası ve Ulusal Düzenlemeler

Bilişim teknolojilerinin gelişmesiyle eş zamanlı olarak; kişisel verinin ağ sistemlerde dolaşıma girmesi ve erişim güvenliğinin kurumsal-hukuki boyutu gündeme gelmektedir. Dolayısıyla Kişisel Verileri Koruma Kurumunun yayınladığı 6698 sayılı Kişisel Verilerin Korunması Kanunu[1] ve uygulaması kapsamında, kamu kurumları ve özel sektör kuruluşları açısından hak ve yükümlülüklerin ortaya çıktığı görülmektedir. Bu doğrultuda, 1970'li yıllardan bu yana, ulusal ve uluslararası düzenlemeler yoluyla kişisel verilerin korunmasına yönelik çalışmalar yürütülmektedir. Uluslararası anlamda ilk veri koruma kanunu 1970 tarihli Almanya'nın Hessen Eyalet Veri Koruma

1 Kanun için bkz: https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf

Kanunu'dur. Bu kanun, bilişim sistemleri yardımıyla tapu kayıtlarına erişim sağlanabilmesi, verileri elde etme ve depolamaya ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır. Benzer şekilde, 1973 tarihli İsveç ve 1978 tarihli Fransa veri koruma kanunları da devlet elinde bulunan çok sayıdaki verinin "kimlik numarası" benzeri bir sistemle kaydı yoluyla entegre edilebilmesi sonucunda, etkin bir şekilde veri işlemenin mümkün hale gelmesi ve bu kapsamda muhtemel riskler karşısında hukuken koruma gereksinimi ile yapılandırılmaktadır.

Avrupa Konseyi'nin 1973 ve 1974 yıllarında, özel ve kamu kesimindeki elektronik veri bankalarında tutulan kişisel verilerin korunmasında gerekli standartları belirlemek için kabul ettiği iki karar, kişisel verilerin korunması ile ilgili sonradan çıkarılan düzenlemelere kaynaklık etmektedir. Kişisel verilerin korunmasına ilişkin geniş kapsamlı ilk uluslararası sözleşme ise Avrupa Konseyi bünyesinde kabul edilen 1981 tarih ve 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" olmuştur. Ayrıca Avrupa Konseyi Bakanlar Komitesi tarafından, 108 sayılı Sözleşme'nin uygulanmasına yönelik usul ve esasları belirleyen toplam 13 tavsiye kararı çıkarılmıştır. Bu gelişmelerin ardından, Avrupa ülkelerinde ve ABD'de ulusal düzlemde yasal mevzuat oluşturulurken Birleşmiş Milletler (BM), Avrupa Konseyi, İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) ve Avrupa Birliği (AB) kapsamında da çeşitli yönerge, direktif ve uluslararası anlaşmalar hazırlanmıştır (KVKK, 2018; 2019). Avrupa Konseyinin, kişisel verilerin korunmasına yönelik, tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi çeşitli sektörlerde uygulanacak ilkeleri belirleyen tavsiye kararlarının da bulunduğu görülmektedir. Buna ek olarak; AB üyesi ülkelerdeki bireylerin kişisel verilerinin üst düzeyde korunması ve kişisel verilerin Avrupa Birliği içerisinde özgür dolaşımını sağlayacak açık ve kalıcı bir düzenleme yapılması amacıyla 24/10/1995 tarihinde "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi"ni (95/46/EC) yürürlüğe girmiştir. Kişisel verilerin korunması konusunda bireysel ve kamusal sorumluluğun, ülkemizdeki mevcut kanunda da benzer uluslararası belgeler temel alınarak düzenlenmesine yönelik çalışmaların sürdürüldüğü anlaşılmaktadır. İlgili düzenlemeler kişisel verinin yaşam süresi sonrasında da güvence altına alınmasına dair hak ve sorumlulukları kapsamaktadır. Örneğin; Amsterdam Bildirgesi 4. maddesinde hastadan tedavi süreci sırasında elde edilen kişisel bilgilerin sadece yaşarken değil; ölümü sonrasında da korunması gerekliliğini ve hastanın izin ve onayı olmaksızın kullanılamayacağı belirtilmektedir (Dülger, 2015).

Bir verinin "kişisel veri" niteliği kazanması veya belirli bir kişiyi temsil etmesi; ancak verinin işlenme sürecinde kesinlik kazanabilmektedir. Kişisel verilerin işlenmesi, verilerin elde edilmesi, kaydedilmesi, düzenlenmesi, uyarlanması, dönüştürülmesi, kullanımı, açıklanması, birleştirilmesi, silinmesi gibi süreçlerden oluşmaktadır (Kaya, 2011). 1980 yılında yayımlanmış ve 2013 yılında güncellenmiş olan Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Rehber İlkeleri; kişisel verilerin korunması ve işlenme sürecinde dikkate alınması gereken prensipleri şu şekilde belirlemektedir (OECD, 2013):

Sınırlılık ilkesi çerçevesinde; kişisel verilerin, hukuka uygun sebepler ve araçlarla toplanması, veri sahiplerinin toplama konusunda bilgilendirilmesi ve bilinçli rızalarının alınması gerekliliği esastır. *Kalite ilkesi*, toplanan verilerin kullanılan amaç doğrultusunda mümkün olduğunca tam, güncel ve doğru olmasını açıklamaktadır. *Amaca özgülük ilkesi* doğrultusunda, kişisel verilerin toplanma amacı belirlenmelidir. Veriler sadece belirlenen amaç için kullanılmalıdır. *Kullanım sınırlaması ilkesi* çerçevesinde toplanan veriler belirtilen amaçlar dışında yayılamaz, bulundurulamaz veya başka amaçlarla kullanılamaz. Veri sahibinin bilinçli rızası ve kanuna dayalı yetkiler bu maddenin sınırlaması olabilir. *Güvenlik ilkesinde* toplanan verilere yönelik oluşabilecek tehlikelere karşı (kayıp, yetkisiz erişim, zarar verme, değiştirme, açıklama) uygun güvenlik tedbirleri ile korunmalıdır. Kişisel verilerle ilgili

gelişmeler, uygulama ve politikalar hakkında genel bir *açıklık ilkesi* bulunmalıdır. Bireyler kendileri ile ilgili veri barındıran kurumların politikalarına kolayca ulaşabilmelidirler. *Bireyin Rızası ilkesi* veri sahibinin rızası olmaksızın verilerin erişilebilir hale getirilmemesi ve açıklanmamasını ifade eder. *Hesap verebilirlik ilkesinde* ise veri sahipleri veri toplayıcı ve yayınlayıcılarına karşı sayılan diğer ilkeler çerçevesinde hesap sorma hakkına sahiptir.

Ulusal düzenlemeler çerçevesindeki mevzuat planlamalarında kişisel verilerin korunması konusu ile ilgili kavramların 1980'li yıllardan itibaren uluslararası belgelerde yer almaya başladığı görülmektedir. Ülkemizin de üyesi bulunduğu, İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 23/9/1980 tarihinde "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler"in kabul edilmiştir. Avrupa Konseyi tarafından, 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"nin 28 Ocak 1981 tarihinde ülkemiz tarafından da imzalanmıştır. Türkiye Cumhuriyeti Devleti, kişisel verilerin korunmasına yönelik olarak 1989 yılında kanun tasarısı hazırlık çalışmasına başlamıştır. 2006 yılına kadar yapılan tasarı çalışmaları devam etmiş ve 2008'de Türkiye Büyük Millet Meclisi'ne (TBMM) gönderilmiş ancak yasalaşma aşamasına geçmeden geçersiz sayılmıştır. Kamu kurumlarının kullandığı bilgi iletişim teknolojileri doğrultusunda oluşabilecek mahremiyet ihlallerini konu edinen en kapsamlı yasalara bağlı düzenleme olarak bu tasarıyı söylemek mümkündür (Tataroğlu, 2009). Güncel yasal düzenlemeler çerçevesinde, 07/04/2016 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun[2] gerekçesi incelendiğinde; ülkemizde, kişisel verilerin korunmasına ilişkin bir kanun ve çeşitli yasal düzenlemeler bulunmakla birlikte; OECD Rehber İlkelerinden "güvenlik" ve "bireyin rızası" ilkelerine referansla; kişisel verinin paylaşımı, arşivlenmesi, gibi hususlarda, bireyler ve kurumlar düzeyinde çeşitli hak ihlalleri ve denetim sorunlarıyla karşılaşılabildiği görülmektedir. Kişisel veriye erişim düzenlemeleri kadar; verilerin kurum kuruluş ve yönetimlerindeki dijital iletişim teknolojileri kullanılarak işlenmesi de mahremiyetin hukuki çerçevesine ilişkin bir tartışmanın konusudur. 5237 sayılı Türk Ceza Kanunu'nun[3] 135 ila 140. maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenerek ve yaptırıma bağlanmıştır. Ancak kişisel verilerin işlenmesine yönelik özel bir kanuni düzenleme bulunmadığından, verilerin hukuka aykırı olarak elde edilip edilmediği hususunda bir takım tereddütler yaşanmaktadır.

Kişisel verinin "sınırlılık", "amaca özgülük" ve "kullanım sınırlaması" ilkeleri çerçevesinde; birey, kurum ve kuruluşlar açısından hak ve yükümlülükler doğuran bir insan hakkı olarak tanımlanması önemlidir. Bu çerçevede, Anayasa'nın 20. maddesinde 2010 yılında yapılan değişiklikle, kişisel verilerin korunması hususunun temel bir insan hakkı olarak güvence altına alındığı ve detayların kanunla düzenlenmesi öngörülmektedir. "Özel yaşamın gizliliği, İnsan Hakları Evrensel Bildirgesi'nin 12. maddesinde ve Türkiye Cumhuriyeti Anayasası'nın 20. maddesinde korunmaya değer bir hak olarak yer almakta ve bu başlıkta ele alınan kişisel verilerin korunması konusu mahremiyetin sağlanması ile yakından ilişki içerisinde bulunmaktadır" (Dülger&Erdinç, 2017). Yasal prosedürlere ve mevzuat hükümlerine uygunluk konusunda özel bir kanun hazırlanması, ülkemizin Avrupa Birliği müktesebatına uygunluk kriterleri çerçevesinde Türkiye Katılım Ortaklığı Belgesi'ne[4] cevap olarak oluşturduğu 2003 Ulusal Programı'nda taahhüt edilen bir yükümlülüktür.

OECD Rehber ilkelerinden "güvenlik" hususuna ilişkin olarak; Avrupa Birliği üyesi ülkeler ile birliğin ortaklık kurduğu diğer ülkelerin güvenlik güçleri arasında, uluslararası organize suçlar ve terörizm

2 Kanun için bkz: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

3 Kanun için bkz: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5

4 Türkiye Katılım Ortaklığı Belgeleri (KOB) için bkz: https://www.ab.gov.tr/katilim-ortakligi-belgeleri_46226.html

konusunda iş birliği ve etkili çalışma ortamı sağlamak amacıyla kurulmuş Avrupa Polis Teşkilatı (EUROPOL) ile ülkemiz güvenlik birimleri arasında operasyonel işbirliği anlaşmasının yapılamadığı (Akalın, 2016) ve elektronik bilgi değişiminin gerçekleştirilemediği; benzer şekilde, Avrupa Birliği üyesi ülkeler arasında yargısal iş birliğini öngören ve ulusal yargı mercilerinin yetkinliğini arttırmak ve sınır ötesi organize suçların soruşturmalarını yürütmek amacıyla kurulan EURO JUST ile çok sayıda sınır ötesi suçun işlendiği geçiş güzergahında bulunan ülkemiz arasında bu suçlarla mücadeleye yönelik işbirliğinin sağlanamadığı görülmektedir[5].

Sağlık kuruluşlarında hastalara ilişkin olarak veya ülkemizde yaşayan yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından resmi kamu kurumlarında çok sayıda özel nitelikli veri arşivlenmektedir. Bu verilerin erişim ve muhafaza koşullarının net bir hukuki çerçevede yapılandırılmaması ve işlerliği konusunda bir mutabakat olmaması, kurumsal görev tanımı itibariyle yetkisi bulunmayan kişilerce bu nitelikteki bilgilerin ifşa edilmesine neden olmaktadır. Kişisel verilerin güvenliğinin sağlanmasına yönelik önlemlerin alınması ve düzenlemelerin teşvik edilmesi hususunda, Avrupa İnsan Hakları Mahkemesi bu durumu (AİHM) özel hayatın gizliliğine müdahale olarak nitelendirmekte (Roagna, 2012) ve mahremiyete yönelik ihlale ilişkin emsal kararlar almaktadır.

Kişisel verinin iktisadi ve finansal alanda dolaşıma girmesi; yabancı sermayenin ülkemizde yatırım yapması ve ülkemizdeki yatırımlarını etkin bir şekilde yönetebilmesi için ihtiyaç duyduğu veri aktarımının[6] güvence altına alınmasına ilişkin olarak 5411 sayılı Bankacılık Kanunu[7] ve 7222 sayılı Bankacılık Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun[8] Gerekçesi gibi çeşitli kanun hükümleri bulunmakla birlikte; mahremiyet hususuna dair tanım, kapsam ve yaptırımlar yeterli ölçüde vurgulanmamaktadır.

Yukarıda genel olarak ifade edilen tartışmanın 6698 sayılı Kişisel Verilerin Korunması Kanun maddeleri üzerinden, dijital mahremiyet-kurumsal sorumluluk ekseninde genişletilmesi kamusal faydanın gözetilmesi, sorun alanlarının tespiti ve önerilerin oluşturulması bakımından önem taşımaktadır. Örneğin; Atalay (2021); Kişisel Sağlık Verileri Hakkında Yönetmelik[9] (2019) değerlendirmesinde; kamusal hizmet sağlayan resmi dijital platformlarda (e-nabız vb.) hesabı olan bireylere gizlilik koşulları ile bilgilendirmeler yapıldığı ve kendi rızaları ile erişim izni verdikleri için oluşabilecek zararlardan ilgili bakanlığın sorumlu tutulmadığına işaret etmektedir. Bir başka ifadeyle; bireyin paylaşma yetkisi verdiği andan itibaren; kişisel verilerin mahremiyetinin olası bir ihlal durumunda, Kanun'da yetkiyi veren birey sorumlu olmaktadır. Dolayısıyla mahremiyet tartışmasında hak ve yükümlülüklerin bireylerin irade ve eylemleri kadar kurumsal sorumluluğu da kapsadığı görülmektedir. Bu çalışmada 6698 sayılı Kişisel Verilerin Korunması Kanunu da bu çerçevede değerlendirilmektedir.

6698 Sayılı Kanun'un İncelenmesi

6698 sayılı Kanun incelendiğinde; uluslararası düzenlemelere paralel olarak kişisel verilerin işlenme koşullarının, bireylerin kişisel verileri konusunda aydınlatılmasının, bu alanı denetleyecek ve düzenleyecek bir kamu otoritesinin oluşturulmasının ve veri güvenliğine ilişkin gerekli tedbirlerin alınmasının temel ilkeler olarak kabul edildiği görülmektedir.

5 https://diabgm.adalet.gov.tr/Resimler/SayfaDokuman/121020211113843AB-K%C4%B0TAP-14-09-2021.pdf

6 Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi için bkz: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/12236bad-8de1-4c94-aad6-bb93f53271fb.pdf

7 Kanun için bkz: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5

8 Bkz: https://www.resmigazete.gov.tr/eskiler/2020/02/20200225-12.htm

9 Yönetmelik için bkz: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=32610&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5

Kanun'un "Amaç" başlıklı 1. maddesine bakıldığında, özel hayatın gizliliği başta olmak üzere kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunması ile kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlemesi amacıyla hazırlandığı anlaşılmaktadır. Kanun'un "Kapsam" başlıklı 2. maddesinde, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı belirtilmektedir. Burada dikkati çeken iki husus bulunmaktadır.

İlk hususta, Kanun'un sadece gerçek kişilerin kişisel verilerini korumak amacıyla yapıldığı, tüzel kişilerin verilerinin bu Kanun kapsamında korunmadığı anlaşılmaktadır. Tüzel kişilerin vergi mahremiyetleri, ticari sırları vb. pek çok verinin farklı mekanizmalar tarafından sistematik şekilde korunmakta olduğu, 6698 sayılı Kanun kaynağını Anayasa'nın kişisel haklar içerisinde yer alan özel hayatın gizliliğini düzenleyen (bu husus da gerçek kişileri ilgilendirmektedir) 20. maddesinden aldığı değerlendirilmektedir. İkinci husus ise kişisel verileri bir veri kayıt sisteminin parçası olmaksızın otomatik olmayan yollarla işleyenler ve bu durumun doğal sonucu olarak kayıt altına alınan kişisel veriler de kapsam dışındadır. Bu istisnada, küçük çapta otomatik olmayan yollarla veri işleyen, esnaflar gibi küçük ölçekli ya da amatör işletmelerin korunmasının amaçlandığı düşünülmektedir. Burada, işletmelerin bu Kanun'dan kaynaklı yükümlülükleri hüküm dışı bırakılmakla birlikte; elde edilen kişisel verilerin gizliliğinin ihlal edilmesi suç unsuru oluşturmaktan çıkarılmış değildir. Kapsam bakımından özel sektör ile kamu sektörü ayrımı yapılmamış olup, öngörülen usul ve esasların her iki sektörde de uygulanması benimsenmektedir.

Kanun'un "Tanımlar" başlıklı 3. maddesinde Kanun'a yön veren kavramlar tanımlanmaktadır. Bunlardan ilki "kişisel veri" kavramıdır. Kişisel verinin kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade ettiği belirtilmiştir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve T.C. kimlik numarası gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, varlıkları ve finansal hareketliliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri de kişisel veri olarak görülmektedir. Örneğin; sağlık sektörüne ilişkin mahremiyet ve kurumsal sorumluluk tartışması çerçevesinde, hastane ve hasta sayıları yoğun kişisel bir veri havuzu oluşturmaktadır. Hasta mahremiyeti ve sağlık verilerinin paylaşılması, aktarımı ve arşivlenmesi konusunda güvenli bir dokümantasyon altyapısının oluşturulması, sağlık kurumlarının sorumluluğundadır[10]. Gelişen iletişim teknolojileri ve dijital platformlarda bu alt yapı, fiziki arşivin ötesinde; kişisel verilerin işlendiği ve depolandığı e-nabız, bulut bilişim, hastane bilgi yönetim sistemleri (HBYS) mecraları ve uygulamalarını da kapsamaktadır (Atalay,2021). Bu nedenle; kurumlar sorumluluğunda bulunan ve uyulması zorunlu dijital veri koruma standartları oluşturulmalı ve bu standartlara işlerlik kazandırılmalıdır.

Bir diğer önemli kavram ise "kişisel verilerin işlenmesi" dir. Kanun Gerekçesi'nde de belirtildiği üzere kişisel verilerin işlenmesi, ilk defa elde edilmesinden başlayarak veriler üzerinde

10 Bayındır'a (2019) göre; Birey ve kamu kurumlarının kişisel sağlık verilerine erişiminin ilke ve esasları Sağlık Bakanlığı tarafından düzenlenmekte ve erişim geçmişi kayıtları tutulmaktadır. "Bu sayede ulaşan bireylerin kullandıkları amaç ve veri seti denetlenebilmekte herhangi bir bilgi sızıntısında sorumlu kişiler tespit edilebilmektedir. Özel sağlık kurumları tarafından Sosyal Güvenlik Kurumu (SGK) Medula sağlık bilgi sistemi aracılığıyla kişisel sağlık verilerinin gönderilmesinde yurt içindeki üçüncü kişiye gönderme söz konusudur. KVKK md.8/b.1 uyarınca ilgili kişinin açık rızası bulunuyorsa, özel sağlık kurumları tarafından SGK'ya Medula aracılığıyla kişisel sağlık verilerinin gönderilebileceği gibi KVKK md.8/b.2-b veya md.8/b.3 uyarınca da açık rıza aranmaksızın da aktarma gerçekleştirilebilir".

gerçekleştirilen tüm işlem türlerini ifade etmektedir. "Veri kayıt sistemi" ise kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade etmektedir. Bu tanımlamaya göre, bu sistemlerin elektronik yahut fiziki ortamda oluşturulabilmesi yönünden herhangi bir fark arz etmemektedir. Diğer önemli kavramlar ise "veri sorumlusu" ve "veri işleyen" dir. Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olanlar şeklinde tanımlandığından bu kişilerin, gerçek kişi ya da kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler de olabileceği anlaşılmaktadır. Veri işleyen ise veri sorumlusu adına verileri işleyen gerçek ve tüzel kişiler olarak tanımlanmaktadır. Bu iki kavramın açıklanması ile Kanun Koyucu muhatap alacağı kişileri açıkça belirtmiş ve ilerleyen maddelerde bunların sorumluluk alanları açıklanmaktadır.

Kişisel Verilerin Korunması Kanunu'nun 28. maddesinin (a) bendi, kişisel verilerin belirli koşullar altında işlenmesinin yasal düzenlemelerden muaf tutulduğunu belirtmektedir. Bu muafiyet, gerçek kişiler veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında gerçekleşen veri işleme süreçlerini kapsamaktadır. Ayrıca, kanun, istatistiki verileri işleyen bazı kamu kurumlarının (örneğin TUİK, İŞKUR) araştırma, planlama ve istatistiksel amaçlarla kişisel verileri kullanmasını öngörmektedir. Bununla birlikte; Kanun, milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbarat faaliyetleri kapsamında kişisel verilerin işlenmesini istisna olarak tanımaktadır. Bu istisna, MİT, Polis ve Sağlık Bakanlığı gibi kurumların, önleyici sağlık hizmetleri gibi belirli amaçlar doğrultusunda kişisel verileri işlemesine olanak tanır. Ayrıca, kanun, suç işlenmesini önlemek ve suç soruşturmasını desteklemek amacıyla kişisel verilerin işlenmesinin gerekliliğini öngörmektedir. Bu bağlamda, adli kolluk kuvvetleri (polis, jandarma, sahil güvenlik) gibi kurumlar, suç teşkil eden herhangi bir unsurun sonucunda suç işlenmesini önlemek için kişisel verileri işleyebilir. Son olarak, kanun, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının, görevlerini yerine getirmek veya denetleme, düzenleme, disiplin soruşturması veya kovuşturması gibi amaçlarla kişisel verileri işlemesine olanak tanımaktadır. Bu çerçevede, belediyeler emlak vergilerini tahakkuk ettirirken, Sayıştay denetçileri denetim kapsamında verileri kullanabilir veya TOBB gibi meslek kuruluşları oda aidatı veya sicil gibi konularla ilgili kişisel verileri işleyebilir.

Kişisel verilerin korunması hususunun önemli boyutlarından biri olan, kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir otorite olarak Kişisel Verilerin Korunması Kurumu'ndan (KVKK) bahsedilmektedir. Kanun'un "Kişisel verilerin işlenme şartları" başlıklı 5. maddesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceği genel prensibi belirtilerek; maddenin devamında da hangi istisnai şartlar altında bu genel prensibin hilafına hareket edilebileceği açıklanmaktadır. Bu istisnalar arasında tartışmaya açılabilecek hususlardan biri, "ilgili kişinin kendisi tarafından alenileştirilmiş olması" ifadesidir. Madde gerekçesinde: "İlgili kişinin kendisi tarafından alenileştirilen bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri işlenebilecektir. Çünkü ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir" şeklinde belirtilmektedir.

Yeni iletişim teknolojileri ve dijital platformlarda mahremiyet tartışması açısından ilgili istisnai durum, kurumsal sorumluluk ve kişisel verinin kullanımına yönelik boşlukları ve eleştirileri beraberinde getirmektedir. Sosyal medya, web sayfaları ve üretilen içerikler açısından kullanıcıların bu mecralara sundukları verinin erişim ve dolaşım sınırları belirsizleşmektedir. Dolayısıyla buradaki kısıtın "verinin alenileştirilmesi" ile "verilerin bazı nedenlerle başkaları tarafından bilinebilir hale gelmesi" hususlarının karışma ihtimalinden kaynaklanabileceği değerlendirilmektedir. Bu husus Kanun'un Meclis Adalet Komisyonu

görüşmeleri[11] sırasında da gündeme gelerek ve tutanaklarda şu şekilde geçmektedir:

> Ayrıca Komisyonumuz, bir noktaya burada özellikle işaret etmeyi gerekli görmüştür. Şöyle ki, alenileştirmeye ilişkin istisnai ve ilkesel hükümler ayrı kalmak üzere, kişisel verilerin bazı nedenlerle başkaları tarafından bilinebilir hâle gelmesi, bilginin salt bu nedenle kişisel veri olma niteliğini kaybetmesine neden olmaz. Zira bu durumda söz konusu bilgiye kişisel veri olma niteliğini kazandıran husus, o bilgi hakkında başkalarının bilgi sahibi olması veya olamaması değil, aksine ilgilinin o bilgiyi kişisel veri olarak tutma yönünde bir iradeye sahip olmasıdır. Örneğin; ilgilisi tarafından alenileştirilmemiş olmasına rağmen bir biçimde başkaları tarafından hakkında bilgi sahibi olunabilir hâle gelen kişisel veri, salt bu nedenle bu niteliğini kaybetmez ve korumadan yararlanır.

Konu ile ilgili görüşmelerde "'alenileştirme' terimi ile kastedilenin ne olduğu anlaşılamamakla birlikte, bu soyut kavram tehlikeli bir nitelik arz etmektedir. Örneğin sosyal medyada bir takım bilgilerini paylaşan kişi ya da bir konferansta fikirlerini belirli bir grupla paylaşan kişi bu bilgileri alenileştirmiş sayılmakta mıdır? Sayılacaksa bu verilere güven nasıl sağlanacaktır? Bu verileri kim, nasıl işleyecektir? Kişi belirli bir hususta ifşa ettiği bilginin alenileştirme sınırlarına girip girmediğini nasıl bilecek ve belirleyecektir? Bu bent ile tasarının aslında temel hak ve özgürlükleri korumaktan ziyade, iktidarın daha fazla kişisel veri elde etmeyi amaçlamasına hizmet etmesinin bir yansıması olarak değerlendirilebilir.

İlgili değerlendirme, AB Veri Koruma Direktifi'nin (1995) 7. Maddesinde alenileştirme teriminin yer almaması dikkate alındığında daha da somutlaşmaktadır. Bu nedenle "2. fıkranın d bendi tasarıdan çıkarılmalıdır" şeklinde muhalefet şerhi konulmakla birlikte; konunun netleştirilmeye ihtiyaç duyduğu anlaşılmaktadır. Kişisel verinin alenileştirilmesi hususu sosyal medya kullanımının yaygınlığı göz önüne alındığında, önümüzdeki dönemde daha çok karşımıza çıkacak gibi görünmektedir. Ancak konunun müphemliği nedeniyle uygulamaya büyük oranda KVKK kararları ve yargı kararları ile yön verilecek gibi durmaktadır. Bu yasal düzenlemelere ilişkin 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun[12] yorumlaması bir örnek olarak verilebilir. Bu kanunun 10. maddesinde; "hizmet sağlayıcı[13] veya aracı hizmet sağlayıcılar, kişisel verileri korumak için gerekli önlemleri alacaktır. İlgili kişinin rızası olmaksızın kişisel verilerin aktarılması ya da başka bir gaye ile kullanılması da söz konusu olamaz" hükmüyle kişisel verilerin korunması hususu açıkça düzenlenmiştir. Elektronik Ticaretin Düzenlenmesi Kanunu 10. maddede, "kişisel verileri korunacak kişinin, hizmet sağlayıcı ve aracı hizmet sağlayıcılar ile arasında bir sözleşme ilişkisinin bulunması şart değildir. Alıcıların ya da herhangi bir şekilde elektronik ortama kişisel verisi girilmiş olan herkesin kişisel verilerinin korunması söz konusu olacaktır" ifadesi yer almaktadır. Ancak, 10. maddeye aykırı hareket edilmesi herhangi bir yaptırıma bağlanmamıştır. Kişisel verilerin korunması alanında önemli bir düzenleme de Ticaret Bakanlığı tarafından hazırlanan Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik'tir. Kişisel veriler, ilgili kişinin açık irade beyanını içerecek şekilde önceden alınan onayı olmaksızın üçüncü kişilerle paylaşılamaz, işlenemez ve başka amaçlarla kullanılamaz" (Kuntoğlu, 2021).

Bu durumun Kanun kapsamında yer almadığı yine Kanun'un 28. maddesinde tekrarlanmaktadır. Kanun'un ilerleyen kısımlarında; kişisel verilerin nasıl işleneceği anlatılarak; kişilerin hakları ile veri sorumlularının yükümlülüklerinin neler olduğu belirtilmekte, veri sorumluluğuna başvurusunun ve Kişisel Verilerin Korunması Kuruluna şikâyet başvurusunun nasıl yapılacağı, veri sorumlularının sicillerinin nasıl tutulacağı açıklanmakta, kişisel

11 Türkiye Büyük Millet Meclisi, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu http://www.tbmm.gov.tr/develop/owa/sirasayi_sd.sorgu_baslangic

12 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf

13 ETHDK'nın 2. maddesinde; hizmet sağlayıcı, "elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişiler" aracı hizmet sağlayıcı ise "başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişiler" olarak tanımlanmıştır.

verilere ilişkin hangi eylemlerin suç hangilerinin ise kabahat olarak değerlendirileceği hususlarına açıklık getirilerek nihayetinde de KVKK'nun kurulmasına ilişkin hükümler ile istisna hükümlerine yer verilmektedir.

Sonuç

Enformasyon ve iletişim teknolojilerinde yaşanan dönüşüm ve artan bir hızla yaygınlaşma farklı açılardan gündeme gelen teknolojik determinizm ve gözetim toplumu kavramlarının, mahremiyet tartışması çerçevesinde yeniden ele alınmasına neden olmaktadır. İletişim teknolojileri çağında süreklilik gösteren yeni gelişmeler ve veri ağlarının ortaya çıkışı; dijital çağ öncesinde daha çok bedensel gizlilik üzerinden kavranan mahremiyet kavramının "bedensel-iradi gizlilik" tanımının ötesinde, kamusal alan ve kurumların sorumluluğuna da işaret eden bir "veri yönetim iradesi" ile açıklanmasını gerekli kılmaktadır. Dijital iletişim teknolojileri açısından; mobil ağ kullanımındaki hız ve hareketlilik kişisel verilerin, genel olarak da hak ve özgürlüklerin korunmasının iki boyutuna vurgu yapmaktadır: Bunlardan ilki, çalışmada detaylı olarak ele alınan ve kurumlar açısından tanım, kapsam, istisnalar üzerinden işleyişi belirlenen hukuki mevzuat boyutudur. İkincisi ise; kurumların kişisel verilerin korunmasına dair mahremiyet kavrayışını ve uygulamalarını değerlendirmek üzere bu alanda farkındalığı bulunan vatandaş-tüketicilerin gerekliliğine işaret eden ilgili kişi boyutudur. Dolayısıyla, dijital çağın bir gerekliliği olarak önemli ölçüde kurum ağları ile entegre olan dijital veri mahremiyeti tartışmasının, kurumsal sorumluluk ve etik açısından bu iki boyutu irdeleyen disiplinlerarası kuramsal çalışmalara ve saha araştırmalarına ihtiyaç duyduğu görülmektedir.

Kişisel verilerin korunması, birçok ülkenin yasal düzenlemeleri ve dünya genelinde artan bir farkındalıkla ele alınan bir konu haline gelmiştir. Bilgi ve iletişim çağında dijital mahremiyet, bireylerin kişisel verilerini koruma ve iradi biçimde yaygınlaştırma konusunda giderek daha karmaşık ve önem arz eden bir durum olmaktadır. Dijital ortamlardaki gelişmelerin sonucunda, gündelik yaşamlarını büyük ölçüde dijital platformlara taşıyan vatandaş-tüketicinin kişisel verilerinin toplanması, depolanması ve paylaşılması konusunda hukuki ve bürokratik düzenlemelerin gerekliliği ortaya çıkmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesi sürecinde bireylerin veri gizliliğini korumayı amaçlamaktadır. Kanun, kişisel verilerin işlenmesi sürecinde şeffaflığı, rızayı ve güvenliği ön planda tutarak bireylerin veri gizliliğini korumak adına kişisel verilerin korunması ve işlenmesine ilişkin düzenleyici bir çerçeve sunmaktadır. Kişisel verilerin korunması ve işlenmesine ilişkin koruma politikalarının uygunluğunu denetleyen Kişisel Verilerin Korunması Kurumu ise bu bilinçlendirme faaliyetlerinin aktif bir biçimde yürütülmesi adına aracı bir konumdadır. Denetim ve idari yaptırımların uygulanması, sürecin aktif bir biçimde işletilmesine yönelik çözüm önerileri sunulması ve bilinçlendirme faaliyetlerinin kapsamlı bir biçimde yürütülmesi adına önemli bir rol oynamaktadır. Ancak kanunun belirlenen amaca uygun olarak kamu kurumları ve özel sektör kuruluşları tarafından etkin bir şekilde uygulanması ve işletilmesi gerekmektedir. Diğer yandan, çalışmada ele alınan kilit kavramlar olarak enformasyon, mahremiyet, kişisel veri ve gizlilik, bireylerin dijital iletişim teknolojileri etkileşimi açısından çeşitli sonuçlar doğurma potansiyeline sahiptir. Bulgular bölümünde bahsi geçen örnekler ışığında, mevzuat üzerinden temel hatları belirlenmiş bir yasal prosedürün tanımlandığı; ancak sistemin yönetimi, kamuoyuna aktarımı ve vatandaş-tüketici farkındalığının arttırılmasına yönelik uygulamaların geliştirilmesi ve çeşitlendirilmesi gerektiği görülmüştür.

Çözüm konusunda, yasal düzenlemelerle birlikte iletişim teknolojilerine yönelik öznel duyarlılıkların gelişimini teşvik etmek, bu çalışmadan çıkarılabilecek sonuçları temsil etmektedir. Çalışmada elde edilen sonuçlara istinaden bazı öneriler şöyledir; Bireylerin kişisel verilerinin gizliliği ve mahremiyetine dair algıları ve farkındalığı arttırmak amacıyla, internet üzerinden kişisel verilere ve bu verilerin korunmasına yönelik bilgilendirme ve farkındalık kampanyaları düzenlenmelidir. Bunun yanı sıra gelecekte bilgi hizmeti sunabilecek bilgi profesyoneli adaylarının,

bu hizmetleri planlarken mahremiyet kavramı, mahremiyet ihlali, kişisel verilerin mahremiyeti, kişisel verilerin işlenme koşulları ve doğrudan ve/veya ikincil kullanımdan kaynaklanabilecek sorunlar konularında farkındalıklarını arttıracak içeriklere derslerde, dijital ve basılı kaynaklarda, dijital platformlarda, kamusal alanlarda, seminerlerde daha etkin bir şekilde vurgu yapılması önerilmektedir. Kişisel Verileri Koruma Kurulu tarafından belirlenen görev ve yetki alanına ilişkin bilgilendirme çalışmaları yapılmalıdır, zira bu kurum kanunen kişisel verilerden sorumlu olarak kabul edilmektedir. Dijital mahremiyetle ilgili bu gibi mevcut zorlukların ele alınması ve etkili çözümler geliştirilmesi, bireylerin dijital dünyada daha güvenli ve kontrol sahibi olmalarına yardımcı olacaktır. Bu süreçte, hukuki düzenlemeler, teknolojik güvenlik önlemleri ve bireylerin dijital okuryazarlıklarının artırılması gibi çeşitli faktörlerin bir araya gelmesi, dijital mahremiyetin korunmasında kritik bir rol oynayacaktır.

Kaynaklar

Akalın, M. (2016). EUROPOL: Türkiye'nin operasyonel işbirliği tartışması. *Türk İdare Dergisi*, (482), 11-32.

Algül, A. (2018). Sosyal ağ kullanıcılarının "abartılı paylaşım", "benlik sunumu" ve mahremiyet tüketimleri. *Marmara Üniversitesi Öneri Dergisi*, *13*(49), 21-44. https://doi.org/10.14783/maruoneri.vi.322970

Altıntaş, S. & Barkuş, F. (2023). Dijital ortamlarda kişisel veri güvenliği kavramı üzerine bir derleme çalışması. *Electronic Journal of Vocational Colleges*, *13*(1), 46-69. https://doi.org/10.17339/ejovoc.1311027

Atalay, H. N. (2021). Mahremiyet kapsamında kişisel sağlık verilerinin korunması ve depolanması. *Journal of Academic Perspective on Social Studies*, *1*(1), 1-20. https://doi.org/10.35344/japss.786353

Bağlı, M. (2011). *Modern bilinç ve mahremiyet*. Yarın Yayınları.

Başkaya, F., & Karacan, H. (2022). Yapay zeka tabanlı sistemlerin kişisel veri mahremiyeti üzerine etkisi: Sohbet robotları üzerine inceleme. *Bilişim Teknolojileri Dergisi*, *15*(4), 48-491. https://doi.org/10.17671/gazibtd.1053803

Bayındır. H, (2019). *Özel sağlık kurumları kapsamında kişisel sağlık verilerinin işlenmesi ve korunması.* [Yayımlanmamış Yüksek Lisans Tezi]. İstanbul Üniversitesi.

Bahvsar, V., Kadlak, A., Sharma, S. (2018). Study on phising attacks. *International Journal of Computer Applications*, *182*(33), 27-29.

Bauman, Z., Lyon, D. (2013). *Akışkan gözetim*. Ayrıntı Yayınları.

Bennett, L (2009). Reflections on privacy, identity and consent in on-line services. *Information Security Technical Report, 14(3)*, 119-123.

Bolton, R. N., Parasuraman, A. P., Hoefnagels, A., Migchels, Kabadayı, S., Gruber, T., Komarova, Y., Solnet, D. (2013). Understanding generation y and their use of social media: A review and research agenda. https://keep.lib.asu.edu/system/files/c160/Bolton_Understanding_GenY__Social_Media_Final_33p.pdf

Castells, M. (2005). *Enformasyon Çağı: Ekonomi, toplum ve kültür*: *Ağ toplumunun yükselişi*. İstanbul Bilgi Üniversitesi Yayınları.

Çaycı, A. E. (2016). Dijital iletişim çağında teknolojinin açığa çıkardıkları: Gözetim ve mahmremiyet. *İnonü Üniversitesi İletişim Fakültesi Elektronik Dergisi*, *1*(2), 157 -169.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, *14*(29), 86-105.

Dalkıç-Örs, Ö. (2018). *Mahremiyet ve Instagram mahremiyetinin insanın yaşam olgusuna etkileri* [Yayımlanmamış Yüksek Lisans Tezi]. Fırat Üniversitesi.

Demir-Güneş, C. (2013). Foucault'da söylem ve iktidar, *Kaygı. Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi,* (21), 55-69.

Dolgun, U. (2005). *Enformasyon toplumundan gözetim toplumuna*. Ekin Basım Yayın.

Dülger, M. V. (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, *1*(2), 43-80.

Eroğlu, Ş. (2018). Dijital yaşamda mahremiyet (gizlilik) kavramı ve kişisel veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü öğrencilerinin mahremiyet ve kişisel veri algılarının analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi. 35*(2), 130-153. https://doi.org/10.32600/huefd.439007

Foucault, M. (2015). *İktidarın gözü* (I. Ergüden, Çev.). (4. Baskı). Ayrıntı Yayınları.

Foucault, M. (2019). *Hapishanenin doğuşu*. İmge Kitabevi.

Feenberg, A. (1999). *Questioning technology*. Routledge.

Goffman, E. (2009). *Günlük yaşamda benliğin sunumu* (B. Cezar, Çev.). Metis Yayınları.

İzgi, M. C. (2014). Mahremiyet kavramı bağlamında kişisel sağlık verileri. *Türkiye Biyoetik Dergisi,* 1(1), 25-37.

Kalaman, S. (2017). Yeni medya ve mahremiyetin dönüşümü: Facebook Türkiye örneği. *Uluslararası Hakemli İletişim ve Edebiyat Araştırmaları Dergisi*, *14*(1), 1-19.

Kişisel Verileri Koruma Kurumu, (2018). *6698 sayılı Kanun'da yer alan temel kavramlar.* KVKK Yayınları.

Kişisel Verileri Koruma Kurumu, (2019). *Örneklerle kişisel verilerin korunması.* KVKK Yayınları.

Kuntoğlu, Ö. F. (2021). Elektronik ticarette kişisel verilerin korunması. *Bilişim Hukuku Dergisi*, *3*(1), 176-229.

Liverber-Göçmen, T. (2018). *Toplumsal yaşamda bıreylerın mahremıyet yönelımlerı: Sosyal ağ kullanıcıları üzerıne bır saha araştırması*. [Yayımlanmamış Yüksek Lisans Tezi]. Selçuk Üniversitesi.

Mary, M. (2012). Privacy management on social media sites research. https://a51.nl/sites/default/files/pdf/PIP_Privacy_management_on_social_media_sites_022412.pdf

McLuhan, M. (1994). *Understanding Media*. The MIT Press Cambridge.

Roagna, I. (2012). *Avrupa İnsan Hakları Sözleşmesi kapsamında özel hayata ve aile hayatına saygı gösterilmesi hakkının korunması* (A.G.Alkış-Schäling, Çev.). Avrupa Konseyi. https://rm.coe.int/16806f15ae

Schmidt, E. & Cohen, J. (2014). *Yeni dijital çağ*, Optimist Kitap.

Staples, W. G., & Decker, S. K. (2008). Technologies of the body, technologies of the self: House arrest as neo-liberal governance. In *Surveillance and governance: Crime control and beyond* (pp. 131-149). Emerald Group Publishing Limited.

Tataroğlu, M. (2009). E-Devlet'te kullanılan gözetim ve kayıt teknolojilerinin mahremiyet üzerinde etkileri. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *9*(1), 95-120.

Tekin, Nurullah (2014). Kişisel verilerin korunması ile ilgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi ışığında değerlendirilmesi, *Uyuşmazlık Mahkemesi Dergisi,* (4), 222-262.

Toffler, A. (1996). *Üçüncü Dalga*. Altın Kitaplar.

Türten, E. (2018). Yüksek lisans öğrencilerinin sosyal

medyada mahremiyet algısı: Gümüşhane Üniversitesi İletişim Fakültesi örneği, *Akdeniz İletişim Dergisi*, (29), 143-162. https://doi.org/10.31123/akil.460160

Veblen, T.B. (1909) "The Limitations Marginal Utility", Journal of Political Econonomy, 17(9), 620-636.

Yavuz, B. (2022). Gözetim ve mahremiyet toplumu, *Yaşar Hukuk Dergisi, 4*(2), 60-82.

Yıldız, İ. (2021). Sosyal medya ve mahremiyet sorunsalı: Panoptikondan süperpanoptikona mahremiyetin dönüşümü. *Abant Kültürel Araştırmalar Dergisi*, *6*(11): 122-132.

Yüksel, M. (2003a). Mahremiyet hakkı ve sosyo-tarihsel gelişimi, *Ankara Üniversitesi SBF Dergisi*, 58(1), 181-213.

Yüksel, M. (2003b). Modernleşme ve mahremiyet, *Kültür ve İletişim,* 6(11), 75-108.

Extended Abstract

With the development of information and communication technologies, the proximity to the digital space is a factor in defining the phenomenon of privacy and starting a new process. The structure and functioning of the concept of privacy has started to be addressed in different dimensions with technological developments. While before the digital age, this phenomenon was associated only with bodily privacy, in the age of information and communication technologies, issues such as the privacy of personal data and privacy regarding the use of social networks have come to the fore. Within the scope of personal data, e-mail addresses, interactions in social media environments, online shopping applications, storage of personal data in health systems, and the registration of digital data in the system as a result of financial transactions in online environments have an important place in ensuring data security. It is possible to say that the collection, processing and storage of data in these digital environments within the scope of privacy and security breaches is an important threat to individuals. Data security breaches, malicious software, phishing attacks and social engineering are among these factors (cited in: Altıntaş, Barkuş, 2023, p.50, Çetin 2014, 5).

Data security breaches are a factor that seriously threatens personal data security in digital environments. These breaches occur when malicious people or hackers break into systems and access personal data. For example, as a result of a database hacking attack, users' personal data can be stolen, disclosed or altered. Such breaches can lead to the misuse of sensitive personal data such as financial information, health data, social security numbers. Similarly, malicious software is another important factor that threatens personal data security in digital environments. Malicious software such as viruses, trojans, worms, spyware and ransomware can infiltrate users' computers or other digital devices, leading to the interception and misuse of personal data. This malware often works without users being aware of it. Thus, there are cases of tracking, stealing or manipulating data. Phishing is an attack method that threatens personal data security in digital environments. Attackers aim to obtain personal data by misleading users through fake websites, emails or messages (Bhavsar, vd., 2018; Tchakounté et al. 2020). For example, users may be directed to a fake website to enter their bank account details or login credentials. As a result of such attacks, users can expose their personal data and be exposed to fraudsters. Another threat factor is social engineering. In social engineering, attackers aim to access personal data by manipulating people. Social engineering attacks usually include methods such as phone fraud, requesting personal information over the phone or face-to-face (Akca 2016). Attackers use psychological manipulation, misleading stories or fraud techniques to gain trust or distract people (Altıntaş, Barkuş, 2023, p.50).

The transformation and proliferation of information and communication technologies is a major factor in bringing the concept of surveillance back to

the agenda. Continuous innovative developments in the age of communication technologies have an important place in the repositioning of all individual activities. New communication technologies cause the problems of violation and exposure of private life in social life to deepen. The technological dimension of communication, the speed and mobility in the use of mobile networks emphasize two dimensions of the protection of personal data, rights and freedoms in general: The legislative dimension and the data subject dimension. The former is mentioned above. However, the latter is more important than the former in the protection of rights and freedoms. This is because most of the time, if the individual protects himself or herself, the danger of harm is either eliminated from the outset or is eliminated before the protection provided by legislation.

On social networking platforms, where we create a new life for ourselves instead of sharing our real lives, the lives, relationships, reactions, expectations and likes that we maintain digitally in the new world that we are increasingly closed and shut off from, guide us as users. "In these environments where we are closed in areas where even our most basic physiological and biological differences are erased, we are either spying or being spied on (Avcı, 2015, p.264)". This new social structure, in which individual differences lose their sovereignty, makes us the same and infiltrates our lives more and more day by day by blurring bodies and minds. Social media and these uniform relationships mutually create and continuously transform each other. For this reason, "Social media breaks down social relations on the one hand, but on the other hand, it creates new groups and creates new living spaces where privacy is lost (Avcı, 2015, p.210)".

The protection of personal data has become an issue that is addressed by the legal regulations of many countries and with increasing awareness around the world. In the information and communication age, digital privacy is becoming increasingly complex and important in protecting individuals' personal data and ensuring their privacy. Rapid developments and technological advances in digital environments have led individuals to move their daily lives to digital platforms to a large extent. This has led to the collection, storage and sharing of personal data, increasing digital privacy risks. The key concepts of digital, information, privacy, personal data and confidentiality discussed in this paper shed light on the challenges individuals face in the digital world and emphasized the importance of these concepts. In the future, addressing the current challenges related to digital privacy and developing effective solutions will help individuals to be more secure and in control in the digital world. In this process, the combination of various factors such as legal regulations, technological security measures and increasing digital literacy of individuals will play a critical role in protecting digital privacy.

Based on the results obtained in the study, some recommendations are as follows; In order to increase individuals' perceptions and awareness of the privacy and confidentiality of their personal data, information and awareness campaigns should be organized on the internet regarding personal data and the protection of this data. In addition, it is recommended that the content that will increase the awareness of information professional candidates who may provide information services in the future on the concept of privacy, violation of privacy, privacy of personal data, processing conditions of personal data and problems that may arise from direct and / or secondary use should be emphasized more effectively in courses, digital and printed resources, digital platforms, public spaces and seminars while planning these services. Informative activities should be carried out regarding the area of duty and authority determined by the Personal Data Protection Board, as this institution is legally recognized as responsible for personal data.

In terms of solutions, the need for legal regulations and encouraging the development of subjective sensitivities on communication technologies represent the conclusions that can be drawn from this study.

Yazar Bilgileri

Author details

1- (Sorumlu Yazar **Corresponding Author**)Öğr. Gör., Başkent Üniversitesi İletişim Fakültesi, syagci.tan@gmail.com

2-Dr. Öğr. Üyesi, Başkent Üniversitesi İletişim Fakültesi, sbal@baskent.edu.tr

Destekleyen Kurum/Kuruluşlar

Supporting-Sponsor Institutions or Organizations:

Herhangi bir kurum/kuruluştan destek alınmamıştır. None

Katkı Oranı

Author Contribution Percentage

Birinci yazar % First Author %	50
İkinci yazar % Second Author %	50

Çıkar Çatışması

Conflict of Interest

Herhangi bir çıkar çatışması bulunmamaktadır. None

Kaynak Göstermek İçin

To Cite This Article

Tanışık, S. ve Bal, S. (2024). Dijital Mahremiyet ve Kurumsal Sorumluluk: Kişisel Verilerin Korunmasında İletişim Teknolojilerinin Kamusal Rolü *Yeni Medya*, *(16)*, 268-285, https://doi.org/10.55609/yenimedya.1424182