Doç. Dr. Duygu HATİPOĞLU AYDIN*

KİŞİSEL VERİLERİN KORUNMASINDA HUKUKUN SINIRLARI

THE LIMITS OF THE LAW IN PERSONAL DATA PROTECTION

ÖZET

Kişisel verilerin korunması mevzuatı, uluslararası, bölgesel, ulusal düzeyde hukuksal düzenlemeler, idari kararlar ve çeşitli yaptırımlarla korunmanın çerçevesini çizmektedir. Çalışmanın amacı, kişisel verilerin korunmasında hukuktan kaynaklanan sınırlar hakkında sosyo-hukuki bir değerlendirme sunmaktır. Hukuk içi kısıtlamalar, siber alanda hiper düzenleme eğiliminin yarattığı çelişkiler, yargı yetkisi kapsamı hakkındaki ihtilaflar, kişisel verilerin korunmasını işlevsizleştiren düzenleme eksiklikleridir. Korumanın bireye indirgenmiş ve rızaya sıkışmış olması ve mahremiyet öz yönetiminin etkisizliği uygulamadan kaynaklanan kısıtlamalardır. Hukuk ve teknoloji ilişkisi, sermaye lehine hareket eğilimi ve kişisel verilerle güvenlik amacıyla veri toplama ilişkisi hukukun yapısal özelliklerinden kaynaklanan sınırlılıkları oluşturmaktadır. Sosyal kısıtlamalar, bireylerin mahremiyete verdikleri anlamlardaki değişim ve gözetimin sıradanlaşmasında izlenebilir.

Anahtar Kelimeler: Kişisel verilerin korunması, GDPR, mahremiyet hukuku, gözetim, hukuksal korumanın sınırları.

ABSTRACT

The legislation on the protection of personal data draws the framework with international, regional, and national legal regulations, decisions of data protection authorities, and various sanctions. The study aims to present a socio-legal review of some limitations of the protection of personal data law. Besides the values and legislation, some structural and social factors affect the protection. One is the internal limitations of law as hyper-regulation tendency in cyberspace, jurisdiction disputes, and legal gaps that make the protection dysfunctional, besides the law practice that reduces the privacy protection to the individual and stuck to consent and the ineffectiveness of privacy self-management. The relationship between technology and law, the growing influence of companies on the law, and contradictions between privacy and surveillance arise from structural features of the law. Social limits are the change in people's privacy meanings and the law's contribution to the normalization of surveillance.

Keywords: Protection of personal data, GDPR, privacy law, surveillance, the limits of law's protection.

Araştırma Makalesi
Makale Geliş Tarihi: 06.07.2023 **Kabul Tarihi:** 28.08.2023
* **ORCID ID:** https://orcid.org/0000-0002-3153-5310
Hacettepe Üni. Hukuk Fakültesi, Hukuk Felsefesi ve Sosyolojisi Anabilim Dalı,
duyguhatipoglu@hacettepe.edu.tr, duygu.hatipoglu@gmail.com

GİRİŞ

Hukuk düzenleri dijital çağda ve siber alanda kişisel verilerin korunmasıyla ilgili pek çok tasarrufta bulunmaktadır. Uluslararası, bölgesel, ulusal düzeyde hukuksal düzenlemeler, veri koruma otoritelerinin kararları, çeşitli yaptırımlar ve teknolojik düzenlemelerle kişisel verilerin anlamının, neden korunması gerektiğinin ve nasıl korunacağının çerçevesini çizmektedir. Kişisel verilerin hukuk aracılığıyla korunması konusunda çeşitli aksiyonlar ve çokça heves olsa da hukukun, koruma konusunda çeşitli bariyerlere takıldığını söylemek mümkündür.

Bu makalede, kişisel verilerin korunması konusunda çeşitli hukuki engeller sosyolojik bir perspektiften ele alınmıştır. Çalışmada kişisel verilerin hukukla korunmasının tarihine, mevzuata ve hukuksal düzenlemelerin lafzından hareketle korumaya egemen ilkelere değinilmemiştir. Öte yandan veri koruması uygulamada çeşitli hukuksal ve sosyal etki ve kısıtlamalarla şekillenmektedir ve gerçek hayattaki karşılığı mevzuatın öngördüğünden farklı olabilmektedir. Çalışmanın amacı, kişisel verilerin korunması mevzuatını tekrar etmek yerine, somut pratiklere odaklanarak, kişisel verilerin korunmasında ya da korunamamasında genel olarak hukuktan kaynaklanan kısıtlamalar hakkında sosyo-hukuki bir değerlendirme sunmaktır. Mevzuatın öngördüğünün ötesinde, hukuksal düzenleme ve uygulamanın bu anlamda sosyolojik değerlendirmesini yapmak, gerçek bir korumanın ilkelerini ortaya koymak için gerekli bir adımdır. Dolayısıyla çalışmada, veri koruma mevzuatı ve koruma pratiği tekil ve bağımsız bir varlık olarak ele alınmamış, mevzuat ve uygulamanın, hukukun yapısal özellikleri ve politik ve ekonomik gelişmelerle bağlantılı olarak toplumsal ilişkilerde ne anlama geldiği açıklanmaya çalışılmıştır.

Kişisel veriler özelinde hukuksal korumanın sınırlılıklarını tartışırken, hakkında konuştuğumuz konunun çok boyutlu ve karmaşık olduğunu özellikle vurgulamak gerekir. Genel olarak veri korumasının önündeki engeller düşünüldüğünde, hukukun ve sağladığı korumanın bunun yalnızca bir parçası olduğunu kabul etmek önemlidir. “Büyük

Veri" terimi, büyük ve karmaşık veri kümelerini tanımlamak için kullanılır. Sağlık hizmeti verilerinden sosyal medya metriklerine kadar, günümüz teknolojisi, yapılandırılmış veya yapılandırılmamış büyük veri kümelerinin neredeyse gerçek zamanlı olarak toplanabilmesine olanak tanır. Gerçekten Büyük Veri çağında, veri gözden kaçırılmayacak bir hızda genişlemektedir. Her saniye artan bu veri havuzunda, şirketler, devletler, kuruluşlar, yalnızca kişisel verileri değil, hassas verileri de toplayıp işleyebilmektedir. Korumanın da verinin üretilmesi, toplanması ve işlenmesi kadar kapsamlı ve hızlı olması gerekir. Büyük verinin hacmi, ihlallerin artışından veri analizi yöntemlerinin geliştirilmesine, verilerin tüketilmesinden depolanmasına kadar pek çok alanı da etkilemektedir. Ayrıca birbirinden farklı aktörlerin Büyük Veri ekosisteminde önemli kararlar alabildiğini, bunun da veri koruma dinamiklerini etkilediğini belirtmek gerekir.

Çalışma boyunca kullanılan veri koruması ve gizlilik/ mahremiyet kavramlarına da değinmek gerekir. Mahremiyet ya da gizlilik, veri koruma bağlamında yaygın olarak tartışılmaktadır. Gizlilik ve veri koruması eşanlamlı olmasa da büyük ölçüde örtüşürler. Her iki terim de özellikle Avrupa hukuku kapsamında köklü temel insan haklarından kaynaklandığından, aynı olmasalar da birbiriyle yakından ilişkili kavramlardır. Ancak iki farklı değeri ve iki farklı temel hakkı temsil ederler[1]. Kişisel bilgilerin hem özel hem de ticari değeri vardır ve genellikle verileri ticari değer olarak kullanmak, mahremiyette ve hatta bazen genel olarak sosyal refahta bir azalmayı beraberinde getirir. Aksi belirtilmediği takdirde, gizlilik sorunlarının çoğu, aslında aynı madalyonun iki yüzü olan iki farklı pazardan, kişisel bilgi pazarından ve gizlilik pazarından kaynaklanmaktadır[2]. Hukuksal açıdan baktığımızda, mahremiyet, bireylerin ve toplumun çıkarlarının korunmasını ve desteklenmesini sağlamak için oluşturulan maddi bir hak olarak tanımlanırken, veri koruma bir usul olarak, maddi hakların etkin bir şekilde uygulandığı ve korunduğu yön-

[1] Eugenia Politou vd., "Privacy and Personal Data Protection", içinde *Privacy and Data Protection Challenges in the Distributed Era*, ed. Eugenia Politou vd., Learning and Analytics in Intelligent Systems (Cham: Springer International Publishing, 2022), s. 7-12.

[2] Age s. 8.

tem ve koşulları belirleyen kurallar düzeyinde işler[3]. Bu farklılıklar ve örtüşmeleri de göz önünde bulundurduğumuzda çalışmanın merkezi kişisel verilerin korunmasındaki kısıtlamalar olsa da belirli tartışmalarda kişisel verilerin yanında Büyük Veri kapsamında veri korumasından da söz edilmektedir.

Nasıl ki, bir kimse hakkında, onun kendisi için taşıdığı düşüncelere dayanılarak bir yargıya varılamazsa, hukuksal düzenlemeler hakkında bir değerlendirme yapılırken de yalnızca hukukun kendisi hakkında varsaydığı iddialarla yetinmek, meselenin çok boyutluluğunun gözden kaçırılmasına sebep olur. Kişisel verilerin korunmasında mevzuatın temelinde yatan değerler, iddialar ve uygulama kadar, bu toplamı etkileyen hukukla ilgili diğer yapısal ve sosyal faktörlere de bakılması gerekir. Bu anlamda kişisel verilerin korunmasında hukukun sınırlılıkları üç başlıkta ele alınabilir. Hukuk içi kısıtlamalar, siber alanda hiper düzenleme eğiliminin yarattığı çelişkiler, yargı yetkisi kapsamı hakkındaki ihtilaflar, kişisel verilerin korunmasını olanaksızlaştıran ya da işlevsizleştiren düzenleme eksiklikleridir. Bunların yanında korumanın bireye indirgenmiş ve rıza/ onaya sıkışmış olması ve mahremiyet öz yönetiminin etkisizliği uygulamadan kaynaklanan ve koruma kararlarının ve mekanizmalarının işlevsizliğini ortaya koyan olgulardır. Hukukun teknolojik gelişmelerin gerisinde kalma eğilimi, makro düzeyde sermaye lehine hareketi ve veri toplama faaliyetinin yaygınlığının ve çok yönlülüğünün neticesinde kişisel verilerin korunması ideali ile güvenlik amacıyla gözetimde verileri toplanan ve işlenen bireylerin mahremiyetlerini sağlamak arasındaki dengenin bozulması hukukun yapısal özelliklerinden kaynaklanan sınırlılıkları oluşturmaktadır. Sosyal sınırlılıklar ise, hukuksal korumanın bireylerin mahremiyete verdikleri anlamlardaki değişiklikte ve Büyük Veri çağında korumanın olanaksızlığında, gözetimin sıradanlaşmasına hukukun katkısında izlenebilir.

Bir diğer açıdan, bahsedilen sınırlılıklar hukukun doğrudan ve dolaylı sınırları olarak da kategorize edilebilir. Doğrudan sınırlar konuyla

[3] Age s. 9-10.

ilgili mevzuatı, hukuk uygulamasını ve düzenleme eksikliklerini ifade ederken, dolaylı sınırlar, hukuksal düzenlemelerin politik anlamlarını ve bunun çeşitli sonuçları ile mahremiyete ilişkin sosyal sınırlılıkları belirtir.

I. HUKUK İÇİ KISITLAMALAR

Hukuk içi sınırlılıklar başlığı altında, devletlerin kabul ettiği veya devletlerin bir araya gelerek üzerinde uzlaştıkları metinler ve bunların hukuk düzeni içindeki mahkeme kararları, idari tedbirler gibi uygulamalara odaklanılmıştır. Hukuki pozitivist bir bakış açısıyla hukuku ele aldığımızda, kişisel verilerin korunmasıyla ilgili belli başlı uluslararası düzenlemeler ve bunların ulusal hukuk düzenlerindeki yansımaları ve uygulamalarının çeşitli kısıtlamalar içerdiği görülebilir. Kişisel verilerin korunmasında Türkiye'nin takip ettiği ve dünya çapında en ileri hükümlere sahip metin Genel Veri Koruma Tüzüğü *(General Data Protection Regulation- GDPR)*'dür. Bu nedenle, küresel ölçekte farklı örneklerden yararlanılmaya çalışılsa da hukuksal düzenlemeler ve uygulama tartışmalarının merkezinde genellikle GDPR almaktadır. Bunun yanında, 1960'lardan itibaren başlayan tartışmalar, bugün pek çok anayasada kişisel verilerin korunmasının bir hak olarak ifade edilmesiyle neticelenmiştir. Bu temel hakkın uygulanması için, teknolojik gelişimle bağlantılı olarak, korumaya dair mevzuattaki değişiklikler ve içeriği de öngörmeye çalışan pek çok yasa, yönetmelik ve benzeri düzenleme yürürlüktedir. Bu başlık altında ileri sürülecek kısıtlamaların bazıları da pozitif hukuk kurallarının uygulanmasından kaynaklanmaktadır. Öte yandan, hukuku yalnızca devlet kaynaklı düzenlemelerle sınırlamadığımızda, siber alanın küresellik ve çok hukukluluk özellikleri, mevzuat yanında, devlet dışı farklı kural koyucuların müdahalelerini beraberinde getirmekte ve mevzuatın öngördüğü korumanın kısmen de olsa işlevsiz kalmasına yol açmaktadır. Siber alandaki hiper-düzenleme eğilimi, çelişkili kararlar ya da düzenlemeler, yargı yetkisinden kaynaklanan sorunlar, düzenleme boşlukları ve hukuk kurallarının uygulamaya yansıması başlıkları çerçevesinde hukuk içi sınırlılıklar görülebilir.

A) HİPER-DÜZENLEME VE ÇELİŞKİLİ UYGULAMALAR

Siber alan bir hiper düzenleme alanıdır. Bireyler siber alandaki faaliyetleri sebebiyle pek çok kuralla muhatap olmak zorunda kalırlar. Konu kişisel veriler olduğunda da bu değişmemektedir. Bir iletinin bireyleri hangi hukuk düzenleri ile ilişkilendirdiğini ayrıntılı bir şekilde incelediğimizde, bulunduğumuz ülkelerin yasaları, vatandaşlık bağımız olan devletin yasaları, sosyal medya platformlarının yerleşik olduğu ülke yasaları, iletinin ilgili olduğu kişinin tabi olduğu mevzuat, bulutta saklanan veriler açısından sunucuların yer aldığı ülkelerin yasaları gibi, birbirine benzeyen ya da benzemeyen pek çok yargılama yetkisine tabi olduğumuz bir gerçektir[4]. Sosyal medya kullanıcısı olma örneğinde, hukuk sistemlerindeki kuralların örtüşmesi kadar çatışması da olasıdır. Özellikle birbiriyle doğrudan çelişen yasa kurallarının nasıl uygulanacağı hukukçular tarafından çözülmeyi bekleyen bir sorun alanıdır. Kullanıcılar açısından, bireysel düzeyde hangi mevzuata uyacakları ya da hangisini/hangilerini görmezden gelecekleri problemi neredeyse çözümsüzdür.

Hiper düzenlemenin kişisel verilerin korumasında yarattığı kısıtlama sorunu belki *"bütün mahremiyet korumasına hükmedecek tek bir yasa"* ile çözülebilir ancak böyle bir yasal düzenlemenin hukuk sistemlerindeki farklılıklar, farklı bölgelerde farklı mahremiyet algılarına bağlı olan hukuk kültürleri çeşitliliği ve yarışan politik çıkarlar sebebiyle hayata geçmesi olanaklı değildir. Bilindiği gibi kişisel verilerin korunmasında genel itibariyle AB ve ABD, iki farklı yaklaşım olarak, mahremiyetin tanımından korunmasına, hukuksal açıdan öne çıkan sistemlerdir[5]. GDPR karşısında ABD'nin veri korumada hukuksal yaklaşımını değerlendiren Hartzog ve Richards, GDPR'ın bulunduğumuz yerden bağımsız olarak küresel veri ticaretinde iş yapmak isteyenler üzerindeki önemli etkile-

4 Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford; New York: Oxford University Press, 2017), s. 105-6.

5 Fred H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States", *Indiana Law Review* 33, sy 1 (1999): 173-232; Matthew Humerick, "The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?", *Catholic University Journal of Law and Technology* 27, sy 1 (2018): 77-125.

rine değinirler.[6] Öte yandan ABD, AB'nin veri koruma çabasını henüz tam olarak benimsememiştir. AB'nin veri korumaya yönelik çok yönlü yaklaşımı, veriler üzerindeki bireysel haklara, ayrıntılı kurallara, veri işlemeye ilişkin varsayılan bir yasağa ve adil bilgi uygulamalarına gayretle bağlı kalmaya dayanmaktadır. Buna karşılık, ABD'nin *patchwork* yaklaşımı daha müsamahakâr, belirsiz ve insanların şirketlerle olan ticari ilişkilerindeki kırılganlıklarına dayanmaktadır. Bu farklılık yasal düzenlemelerde somutlaştığında[7], farklı ülke örneklerinde uluslararası düzeydeki hukuksal düzenlemelerin öngördüğü ilkelerin yerel kültürlerle karşılaştığında farklı sonuçlara yol açtığı da görülmektedir[8].

B) YARGI YETKİSİNİN KAPSAMINDAN KAYNAKLANAN KISITLAMALAR

Kişisel verilerin korunmasının küresel bir fenomen olması ile koruma hakkındaki yasal düzenlemelerin coğrafi kapsamı arasındaki örtüşmezlik, yani yargı yetkisinin sınırları, hukukun iç kısıtlamalardan bir diğerini oluşturur. Yargı yetkisi sınırlarının kapsamı, şahsa bağlı yargı yetkisine ve konu bakımından yargılama yetkisine sahip bir mahkeme tarafından verilen kararların uygun coğrafi kapsamı ile ilgilidir[9]. Kişisel verilerin korunması, küresel bir olgu olmakla birlikte, koruma mekanizmaları ulusal, bölgesel ve uluslararası düzeyde çeşitlenmektedir. Elbette her düzeyde yargı yetkisiyle ilgili çeşitli yaklaşımlar ve tanımlamalar vardır. Ancak bu düzenlemeler, ortada kalan sorun yumağının kaynağıdır ve çözümü olma iddiasından da uzaktadır.

6 Woodrow Hartzog ve Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection", *Boston College Law Review* 61, sy 5 (2020): 1687-1762.

7 L. Bygrave, "Privacy Protection in a Global Context- A Comparative Overview.", *Scandinavian Studies in Law*, 2004, s. 319-48.

8 Yohko Orito ve Kiyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value" (ETHICOMP 2005, Linköping University, Sweden, 2005), https://rcvest.southernct.edu/ethicomp2005-linkaping-sweden/.

9 Mülki yargı yetkisinin tarihsel süreçte nasıl kurulduğuna ve siyasi ve sosyal kimlikler ürettiğine dair bir tartışma için bkz. Richard T. Ford, "Law's Territory (A History of Jurisdiction)", *Stanford Law School* 97 (1999): 843-930.

Bölgesellik büyük ölçüde yargı yetkisine dair iddiaların gerçekleştiği alanın sınırlarını çizer. Bir devlet, kendi topraklarında meydana gelen her şeyi, kendi topraklarında meydana geldiği basit nedenden ötürü düzenleme hakkına sahiptir. Bununla birlikte, yargı yetkisi iddialarının temeli olarak bölgesellik, iki işlevi yerine getirmeyi amaçlar. Birincisi yargı yetkisinin yasal olarak ne kadar uzağa ulaşabileceğine dair tanımlamaları ifade etmek içindir. İkincisi bölgeselliğin, aynı zamanda bir yargı iddiasının ne zaman çok ileri gittiğini gösteren ve böylece diğer ülkelerin yargı bölgelerine gayri meşru müdahaleyi önleyen bir uyarı ışığı olarak çalışması amaçlanmıştır[10]. Bölgesellik, yargı yetkisi açısından konumu odağına alırken, siber alanda konumları çevrimiçi olarak değiştirmek oldukça kolaydır[11]. Ayrıca siber alanın çalışma biçimiyle birlikte bölgeselliğin, yürürlükteki bazı yasalar veya yargı yetkisi için odaklanmak istediğimiz bir nokta bulmaya çalışırken odağı çeşitli yerlere yönlendirebilmesi de mümkündür. Svantesson, yargı yetkisinin hukuksal temeli olarak görülen bölgesellikten daha iyi bir rejime geçme ve uluslararası hukukun yargı yetkisine nasıl yaklaştığı konusunda daha mantıklı bir tutarlılık elde etme anlamında ilerleme kaydedene kadar, bölgesel yargı yetkisinin, hiper düzenlemeyle birlikte internetle ilgili düzenlemeler açısından sorun olmaya devam ettiğini belirtir[12].

Uluslararası hukuk kapsamındaki teamül ve yargılamaya dair kurallar açısından da benzer bir sonuç ortaya çıkar. Bu kurallar hangi devletin, diğer devletler karşısında, hangi ulusötesi olayı düzenleme, yani yasalarını yapma, yürütme ve uygulama hakkına sahip olduğu sorusuyla ilgilenir. Burada konu edilen çetrefilli meselelerin yani hakaret, mahremiyet, sözleşme ve fikri mülkiyet hukuku, müstehcenlik, ilaç ruhsatı ve kumar yasaları gibi meselelerin yalnızca bir kısmını kişisel verilerin ko-

10 Dan Jerker B Svantesson, "Are we Stuck in an Era of Jurisdictional Hyper-regulation", içinde *50 Years of Law and IT*, ed. Peter Wahlgren, Scandinavian Studies in Law (Stockholm Institute for Scandinavian Law, 2018), s. 153.

11 Mülki yargı yetkisi, siber alanın bir mekân olarak anlaşılmasında da etkili olmuştur. Gerçek dünyada dair kavram setlerinin ve yerselleştirme ölçeklerinin siber alana taşınması, siber alanda yer metaforuyla karşılanmıştır. Bu metaforun tanımı ve yöneltilen eleştiriler için bkz. Duygu Hatıpoğlu Aydın, *Siber Alan ve Hukuk* (İstanbul: On İki Levha Yayıncılık, 2022), s. 39-54.

12 Svantesson, "Are we Stuck in an Era of Jurisdictional Hyper-regulation", s. 154.

runması oluşturmaktadır. Ancak bu alanların çevrimiçi düzenlenmesi, çeşitli yaptırımlara bağlanması, aslında düzenleyici denetimin geleneksel konum merkezli tahsisine meydan okumaktadır[13]. Bu çekişmenin en önemli sebeplerinden birisi, devletlerin kendi sınırları içinde egemenlik haklarını ve buna bağlı olarak ulusal hukuklarını işaret etmesidir.

Uzunca bir süredir, içeriğin tek bir devletin yasalarına aykırı olması nedeniyle, küresel olarak engellenmesi/yaptırımla karşılanması örneklerine rastlanmaktadır. Yerel yasaları tartışmalı bir şekilde ihlal eden içeriğe yanıt olarak küresel olarak içeriği engellemelerini veya kaldırmalarını emreden mahkemelerin giderek daha fazla örneğini bulmak mümkündür. Hiper düzenleme sorunu ile bağlantılı olan bu gelişme, veri korumasını bir noktada işlevsiz kılmaktadır. Daha önce *Yahoo* vs. Fransa davası[14] ya da *gigapedia*'nın Münih'te bir mahkeme tarafından kapatılması gibi hukuki süreçlerde görüldüğü gibi, yargı yetkisinin sınırları problemi henüz çözülememiştir. Hem kişisel verilerin korunması hakkında hem de güncel olması sebebiyle *OpenAI* hakkındaki karara değinmek gerekir. İtalyan veri koruma otoritesi, *OpenAI*'nin kullanıcılardan yasadışı bir şekilde kişisel veri topladığını ve reşit olmayanların yasadışı materyale maruz kalmasını önlemek için bir yaş doğrulama sistemine sahip olmadığını söyleyerek *ChatGPT*'yi coğrafi olarak engelleme yönünde karar almıştır[15]. Hükümetlerin yasalarını kendi yetki alanları dışındaki devlet ve kuruluşlara dayatmaları önünde çeşitli engeller vardır. Bu nedenle, kişisel veriler başka bir ülkede veya yabancı bir kuruluş tarafından işlendiğinde, yasal koruma eksik veya yetersiz olabilir. GDPR sistemi, bu zorlukları aşmak üzere ve sınır ötesi veri korumasını teşvik etmek için bir bölgesel kapsam tanımlaması yapmıştır. Bu anlamda İtalyan Veri Koruma Otoritesi'nin kararı, kişisel verilerin korunması ilkelerine ve GDPR'ın 3. maddesinde düzenlenen bölgesel kapsama uygun olsa da bu ve benzeri bölgesel düzeyde engellemeler, bu kez de *VPN* gibi çeşitli teknolojik araçlarla bertaraf edilebilmektedir.

13 Uta Kohl, "Jurisdiction in Network Society", içinde *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias ve Russell Buchan (UK: Edward Elgar Publishing Limited, 2021), s. 69-96.

14 Joel Reidenberg, "Technology and Internet Jurisdiction", *University of Pennsylvania Law Review* 153 (2005): 1951-74.

15 Adam Satariano, "ChatGPT Is Banned in Italy Over Privacy Concerns", *The New York Times*, 31 Mart 2023, blm. Technology, https://www.nytimes.com/2023/03/31/technology/chatgpt-italy-ban.html.

Veri korumadaki yargılama yetkileri arasındaki çekişmenin en önemli sebeplerden biri olan uyumlu bir yasal çerçevenin olmamasının nedeni genellikle farklı ülkelerin farklı veri koruma yasaları, düzenlemeleri ve politikalarını benimsemeleridir. Bu, kişisel verilerin sınırlar ötesinde korunmasında çatışmalar ve tutarsızlıklar yaratır. Farklı mevzuatların farklı veri koruma otoriteleri eliyle koruma sağladığı da açıktır. Bu farklılık, uygulamada da yeknesaklaşmayı zorlaştırmaktadır.

Ek olarak, standart bir uygulama aracının olmaması, yabancı kuruluşların veri ihlallerinden veya gizlilik haklarının ihlallerinden sorumlu tutulmasını zorlaştırmaktadır. Siber suçlar ve siber güvenlik gibi belirli konularda uluslararası hukuk öznelerinin uzlaşma sağladığını gösteren düzenlemeler ya da genel itibariyle ceza hukuku açısından iş birliği[16], hatta kişisel verilerin ulusal sınırlar ötesine akışına dair çeşitli hukuksal girişimler mevcut olsa da kişisel verilerin korunmasında yargı yetkisinin sınırları, üzerinde tartışılan bir mesele olmaya devam etmektedir.

C) DÜZENLENMEYEN ALANLAR (~~HUKUK~~ DÜZENLEME BOŞLUKLARI)

Hukuk düzenlerinin teknolojik gelişmeleri karşılama ve ihtiyaçlara cevap verme konusundaki hızıyla teknolojik gelişmeleri hızı arasındaki fark, kişisel verilerin korunması konusunda hukukun iç kısıtlamalardan birini oluşturur. Bununla bağlantılı olarak kişisel verilerin elde edilmesi ya da işlenmesi süreçlerinin tamamının mevzuat aracılığıyla düzenlenmesinden söz edilememektedir.

Bir norm sisteminde daima boşlukların bulunması, toplumsal yaşamın değişim hızının hukukun değişiminden daima daha fazla olmasından kaynaklanmaktadır. Bazen de yasa koyucu, sorunu öngördüğü

16 Ceza adaleti konularındaki iş birliklerini politik ve yasal açıdan veri koruma hukuku için değerlendiren bir çalışma için bkz. Paul De Hert ve Auke Willems, "Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters?", içinde *Enforcing privacy: lessons from current implementations and perspectives for the future*, ed. Paul De Hert, Dariusz Kloza, ve Pawel Makowski (Wydawnictwo Sejmowe, 2015), s. 49-76.

halde belirli gerekçelerle çözüm getirecek kuralları koymamış olabilir[17]. Kişisel verilerin korunmasında hukukun sınırlarından birini oluşturan düzenlenmeyen alanlar/konular, bu açıdan teknolojik gelişmelerin hızıyla da bağlantılıdır. Elbette herhangi bir alanda düzenleme yapılması süreci, hukuk kültürü, ulusal, bölgesel ve uluslararası düzeyde yasama faaliyetlerinin ve norm oluşumunun farklı dinamikleri gibi sebeplerden etkilenebilmektedir.

Kişisel verilerin korunmasıyla ilgili bazı konularda düzenleme boşluklarının olduğundan söz edilebilir. Biyometrik veriler, güvenlik amaçlı kamusal gözetim, algoritmik profilleme[18] hakkında kişisel verilerin korunması mevzuatı ya yoktur ya da olan koruma oldukça yetersizdir. Ayrıca bulut bilişim[19], nesnelerin interneti gibi uygulamaların yaygınlaşması hem yargı yetkisinin sınırları hem de sorumluluğun üstlenilmesi açısından boşluklar yaratmaktadır.

Örneğin, nesnelerin interneti (IoT), mahremiyet yasalarının değişimindeki gerekliliği gösteren önemli bir olgudur. Akıllı ev asistanları ve giyilebilir teknoloji gibi IoT cihazları, gözetim amacıyla kullanılabilecek çok miktarda kişisel veriyi toplayabilmektedir. Bu kapasite geleneksel mahremiyet anlayışına önemli zorluklar getirmektedir. Veri toplama uygulamaları hakkında şifreleme ve şeffaflık gibi hesap verilebilirlik önlemleri bireylerin gizlilik haklarının korunmasında yardımcı olabilecektir[20]. Giderek daha bağlantılı bir dünyada bireylerin gizlilik haklarını korumak için yeni yaklaşımlara duyulan ihtiyacın vurgulaması açısından nesnelerin internetinin yaygınlaşması kişisel verilerin korunmasına dair düzenlemelerle doğrudan ilgilidir. Nesnelerin interneti, GDPR'la

17 Yasemin Işıktaç ve Sevtap Metin, *Hukuk Metodolojisi* (İstanbul: Filiz Kitabevi, 2019), s. 222.

18 Monique Mann ve Tobias Matzner, "Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination", *Big Data & Society* 6, sy 2 (01 Temmuz 2019).

19 Kevin McGillivray, ed., "Data Privacy and Data Protection Issues in Cloud Computing", içinde *Government Cloud Procurement: Contracts, Data Protection, and the Quest for Compliance* (Cambridge: Cambridge University Press, 2021), s. 91-156.

20 Steven I. Friedland, "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy", *West Virginia Law Review* 119, sy 3 (2017): 891-914.

ilişkisi bakımından *lex specialis* sayılabilecek AB'nin E-Gizlilik Direktifi bağlamında ele alınmakla birlikte, küresel düzeyde etkili bir korumayı sağlayacak hukuksal düzenleme mevcut değildir. Düzenleme boşluklarına dair Türkiye'den bir örnek, kamusal alanlarda İdarece yürütülen video kameralı kayıtlar hakkında kişisel verilerin korunması bağlamında bir düzenleme olmayışıdır[21]. Benzer bir şekilde, Türkiye'de son dönemde seçim güvenliği konusunda da gündeme gelen, bir yandan kullanımı yaygınlaşan bir yandan kolaylaşan derin sahte *(deepfake)* teknolojisiyle yaratılan içerikler hakkında kapsayıcı ve etkili bir düzenleme olmayışı, hızlı teknolojik gelişmeler karşısında hukuk eliyle kişisel verilerin korunmasını kısıtlayabilmektedir.

Dijital devrimin yol açtığı önemli bir sorun alanı, özellikle parmak izleri, retina kalıpları, yüz özellikleri, ses kalıpları ve DNA gibi insanların bedenlerinden türetilen biyometrik verilerdir. Biyolojik ve biyometrik verilerin yaygın olarak toplanması ve kullanılması gizlilik sorunlarını beraberinde getirmektedir. Biyometrik verilerin nasıl toplanacağı ve hangi amaçlarla kullanılacağı konusunda da bir düzenleme boşluğundan söz edilebilir[22]. Yine GDPR kapsamında biyometrik veriler ele alınmışsa da dünyada pek çok ülkede biyometrik verilerin toplanması, işlenmesi ve kullanılması konusunda yasal düzenlemeler mevcut değildir. Burada özellikle yüz tanıma teknolojilerine değinmek gereklidir çünkü yüz tanıma teknolojilerinin kullanılmasının veri koruması açısından yarattığı dezavantajlar, mevcut koruma düzenlemelerinin temelinde yer alan ilkelerin de altını oymaktadır. Genel itibariyle, yüz tanımanın farklı ırklardan insanlar ve diğer azınlıklar ve dezavantajlı gruplar üzerindeki orantısız etkisi, gizliliğin ortadan kaldırılmasını normalleştirilmesi, gözetim kapitalizmin güçlenmesi gibi etkileri, yüz tanıma teknolojilerinin

21 Ezgi Turgut Bilgiç, "Kamusal Alanda İdarenin Video Gözetiminin Kişisel Verilerin Korunması Hukuku Bağlamında Değerlendirilmesi" (Yüksek Lisans, Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2023).

22 *AIAct* olarak bilinen ve yapay zeka temelli teknolojilerin gündelik kullanımına dair kapsamlı hukuksal düzenleme, 11 Mayıs 2023'te Avrupa Parlamentosu'nda büyük bir çoğunlukla kabul edildi. Yüz tanıma, tahmine dayalı polislik, gözetim teknolojilerinin insan haklarıyla bağdaştırılması, yapay zeka kullanımında şeffaflık gibi pek çok konuyu ele alan düzenleme Haziran ayında Genel Kurul'da oylanarak kabul edilmiştir.

suistimaline örnekler olarak verilebilir[23]. Yüz tanıma teknolojileri vasıtasıyla kişisel verilerin toplanmasında en büyük problemlerden biri rıza eksikliğidir. Veri gizliliğine ilişkin düzenlemelerin temel ilkelerinden biri, veri toplayan kuruluşların, verileri toplanan kişilere hangi biyometrik verileri topladıklarını bildirme ve bunu yapmak için onaylarını alma zorunluluğudur. Her ne kadar aşağıda tartışıldığı gibi rıza kavramının kendisi sorunlu olsa da yüz tanıma teknolojilerinin bireylerin rızası olmadan toplanması, yani gerçek zamanlı kamu gözetimi gibi uygulamaların kullanılması veya yasal olarak oluşturulmamış veri tabanlarının kullanılması bireylerin rızasını ortadan kaldırmaktadır. Ayrıca yüzlerin şifrelenmesi mümkün değildir. Yüz tanıma verilerini içeren veri ihlalleri, kimlik hırsızlığı, taciz ihtimalini artırmaktadır çünkü şifreler ya da kart bilgilerinin aksine yüzlerimizi değiştirmek olanaklı değildir. Şeffaflığın tam anlamıyla sağlanamaması da kişisel verilerin korunmasında problem yaratmaktadır. Örneğin, parmak izi gibi diğer biyometrik verilerin aksine yüz tanımanın uzaktan, gizlice ve kolay bir şekilde yapılabilmesi şeffaflığı ortadan kaldırmaktadır. Yüz tanıma teknolojileriyle toplanan verilerin, derin sahte temelli uygulamalarla yayılması oldukça kolaydır. Bu da verinin hiç akla gelmeyecek kötü kullanımlarına yol açabilir. Ayrıca toplanan yüz verileriyle yapılan eşleştirmelerde yanlışlık yapılma ihtimali, pek çok hak ihlaline davetiye çıkarabilir.

Siber alanda ve onunla ilgili meselelerde de hukukun teknolojik gelişmelerle ilişkisi, özelde kişisel verilerin korunmasında hukuk içi kısıtlamalardan biri olan düzenlenmeyen alanların varlığını artırmaktadır. Elbette hukukun toplumsal hayatın her alanını ayrıntılı şekilde düzenleme olanağı yoktur. Ancak hızlı ve etkili hareket kabiliyetini kısıtlayan ve aşağıda değinilecek yapısal kısıtlarla birleştiğinde, hukukun hareket tarzının kendisi, gözle görünür bir kısıtlama yaratmaktadır.

Hukuk ve teknolojinin gelişim hızı arasındaki uyumsuzluğun yarattığı olumsuz sonuçların boyunu kavramak için, hukuksal düzenleme-

23 Woodrow Hartzog, "Facial Recognition Is the Perfect Tool for Oppression", *Medium* (blog), 02 Ağustos 2018, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

lerin oluşturulma süreçleri yanında teknolojik gelişmelere de bakmak gerekir. Büyük Veri denilen ve içinde kişisel verileri de barındıran veri paketi, gerçekten büyük ve yaygındır. Varlığı da verilerin serbestçe dolaşmasına bağlıdır. Dolayısıyla siber alanla internet, dijital uygulamalar, elektronik nesneler ya da diğer biçimlerle ilişkilenen kullanıcıların verilerinin üretilmesi ve yayılması sistemin sürmesi için elzemdir. Teknolojik açıdan büyük verinin doğası ile veri korumanın hukuksal düzenlemeleri arasında bir uyumsuzluğa yapısal kısıtlamalar başlığında ayrıca değinilecektir.

D) HUKUK UYGULAMASINDAN KAYNAKLANAN KISITLAMALAR

Hukuk düzeni, yalnızca hukuksal düzenlemelerin değil, mevcut düzenlemelerin de uygulanmasıyla inşa edilir. Hiper regülasyon, yargı yetkisi konusundaki problemler ve düzenlenmeyen alanlarla birlikte, mevcut hukuk kurallarının işleyişi veri korumasında hukuk için kısıtlamalardan bir diğerini oluşturur.

Kişisel verilerin korunması mevzuatındaki çeşitlilik ve alanın yasalarla düzenlenmesine yönelik istek bir yana, koruma rejimlerinde koruma sorumluluğunu bireysel denetime sıkıştıran çözümler öne çıkmaktadır. Bir anlamda kişisel veri korumasının veri sahiplerinin öz yönetimine bırakıldığı bir süreçten söz etmek mümkündür. Veri öznelerinin ürettiği verilerin toplanması ve işlenmesinde "rıza" koruyucu bir araç olması gerekirken, veri toplamayı veri özneleri aleyhine meşrulaştıran bir araca dönüşebilmektedir. Rıza probleminin başlangıç noktası, bireylerin verileri üzerinde kontrol sahibi olabileceği düşüncesidir. Eğer veri özneleri ürettikleri veriler üzerinde söz sahibi iseler, bu verilerin toplanması, işlenmesi ve büyük veri havuzunda bir biçimde yer alması konusunda da söz sahibi olabilirler. O halde mahremiyete yapılan müdahalede bireylerin razısı varsa, bu müdahale hukuk düzeni tarafından meşru sayılacaktır.

Mahremiyetin korunmasında bireylerin rızasının alınmasına dair beklenti, esas olarak "mahremiyet öz yönetimine" dayanmaktadır. Hu-

kuk düzeni bu süreçte, bireyleri, haklarındaki bilgilerin toplanması, kullanılması ya da açıklanmasında fayda-zarar hesabı yapabilmelerine olanak tanıyan bir dizi hakla donatmıştır. Bireylerin rızası, kişisel verilerin neredeyse her biçimde toplanmasını, kullanılmasını ve ifşa edilmesini meşrulaştıran bir güç haline gelmiştir. Öte yandan bireyler bir dizi sorun sebebiyle, mahremiyetlerini uygun şekilde yönetemezler[24]. Bireylerin mahremiyetlerini gerçek bir irade hürriyeti çerçevesinde yönetememelerinin en önemli sebepleri, sürecin teknik özelliklerinden kaynaklanmaktadır. Her şeyden önce veri toplayan pek çok kurum, kuruluş ve kişi vardır. Bunlar arasındaki ilişkiler ve açık ya da kapalı veri alışverişi[25], bireylerin verileri üzerinde kontrol sahibi olmalarını imkansızlaştırmaktadır. Bir diğer sebep, toplanan verilerin çok çeşitli amaçlarla kullanılmasından[26] kaynaklanan kontrol sorunlarıdır. Siber alanda yapılan her işlemde veri toplanması, akıllı şehirler, kameralı gözetim, nesnelerin interneti gibi uygulamalar göz önüne alındığında veri toplama noktalarının yaygınlığı ve karmaşık veri kümeleri oluşması, bireylerin kişisel verilerinin kullanılması ya da kullanılmamasında rasyonel karar vermelerini imkânsız kılan teknolojik olgulardandır.

Hukuksal düzenlemeler açısından bireylerin rızalarının varlığının ifade edilmesi için bildirim ve onay şartı en yaygın uygulamalardır. Özellikle GDPR uygulamasının baskısıyla uygulaması yaygınlaşan çerezler *(cookies)*, kişisel verilerin toplanması ve işlenmesinde rızanın ortaya konulduğu önemli araçlardan biridir. Çeşitli çalışmalarda çerezlerin yönetimi usulüyle ihlallerin engellenemediği[27], hatta mevcut çerez uygula-

24 Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review* 126 (2013): 1880-1904.

25 Wolfie Christl, "Digital Profiling in the Online Gambling Industry. A report on marketing and risk surveillance by the UK gambling firm Sky Betting and Gaming, TransUnion, Adobe, Google, Facebook, Microsoft and other data companies" (Vienna-Essex: Cracked Labs- CleanUp Gambling, 2022).

26 Jacob Leon Kröger, Milagros Miceli, ve Florian Müller, "How Data Can Be Used Against People: A Classification of Personal Data Misuses", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 30 Aralık 2021).

27 Celestin Matte, Nataliia Bielova, ve Cristiana Santos, "Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework", içinde *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, s. 791-809.

malarının yasanın öngördüğü usullere aykırı olarak tasarlandığı[28] ortaya konmuştur.

Kişisel verilerin toplanması ve işlenmesindeki hukuk direktifli uygulamalar da rızanın sakatlanmasına sebep olabilmektedir. Örneğin, verilerin toplanması ve işlenmesi için rıza verilememesinin bedeli olarak hizmetten faydalanamamak, rıza zorunluluğunun bireylerin aleyhine dönmesine sebep olabilmektedir. Üstelik rıza verilmediğinde dahi, bireyler hakkındaki veriler toplanabilmektedir. Benzer şekilde siber alandaki çeşitli hizmetlerden faydalanmak için bireylerin rızası alınırken, uzun açıklama metinlerinin sonucundaki "onay" kutucuklarının işaretlenmesi, rızanın varlığı için yeterli sayılmaktadır. Bu uzun, küçük yazılı ve okunması genelde zaman kaybı olarak görülen metinler[29], şirketler açısından yasal sorumluluğu bertaraf eder gibidir[30]. Kutucukların işaretlenmesiyle kabul edilen metinlerin içerikleri, bireyler tarafından genelde bilinmez. Verilerin toplanması için bu metinlerin onaylanması ve böylece veri toplamanın yasal hale gelmesi sürecinde, edimlerin tarafları arasında açık bir eşitsizlik olması çok muhtemeldir. Mahremiyet öz yönetimi açısından bireyin, her türlü bilgisel donanıma sahip, dijital okuryazarlığı üst düzeyde, teknolojik farkındalığı yüksek, verilerinin toplanmasının ve işlenmesinin anlamını bilen ve gelecekteki ihtimalleri öngörebilen bir kişi olarak tanımlanması, siber alanda etkileşime geçen veri öznelerinin çok küçük bir kısmına tekabül etmektedir.

Mahremiyetin kolektif sosyal boyutunu kabul etmek, piyasa verimliliğinin "bireysel" mahremiyet kaygılarını aştığı piyasa temelli baskın mahremiyet koruma modellerinin varsayımlarına meydan okuma ve bireysel direniş eylemlerinin ve kolektif ölçekte kitlesel duyarlılığa dönüş-

28 Alexander Hanff, "The problem with Consent Management Platforms is they are unlawful by design", *linkedin.com* (blog), Aralık 2021, https://www.linkedin.com/pulse/problem-consent-management-platforms-unlawful-design-alexander/.

29 Florian Schaub vd., "A Design Space for Effective Privacy Notices", içinde *The Cambridge Handbook of Consumer Privacy*, ed. Evan Selinger, Jules Polonetsky, ve Omer Tene, Cambridge Law Handbooks (Cambridge: Cambridge University Press, 2018), s. 365-93.

30 Ari Ezra Waldman, "How Big Tech Turns Privacy Laws Into Privacy Theater", *Slate*, 02 Aralık 2021, https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html.

mesi potansiyeline sahiptir[31]. Düzenleyici girişimler bireysel mahremiyet okuryazarlığına ve öz yönetime odaklanırken, mahremiyetin kolektif bir değer ve sosyal bir fenomen olduğunu gözden kaçırmakta ve bu da düzenlemelerin etkisizliğiyle sonuçlanmaktadır.

Uygulamada bir başka sınır, dijital çağın ortaya çıkardığı eşitsizliklerin[32] izlenebildiği bir alan olarak, hukuksal korumadan faydalanabilenlerin özelliklerinde ve yargısal süreçlerde görünürlüklerinde ortaya çıkmaktadır. Fransız Veri Koruma Otoritesi (*CNIL*) tarafından yapılan yakın tarihli bir araştırmada, kişisel verilerinin ihlal edildiği iddiasıyla başvuru yapanların çoğunlukla erkek (%62), 30-49 yaşları arasında (%54,2) ve yüksek lisans veya üzeri bir eğitim derecesine sahip olduğu (%48,6) tespit edilmiştir. Toplumsal cinsiyet, yaş ve eğitim kaynaklı eşitsizliklerin izlenebildiği bu araştırmaya göre, başvurucu kadınların oranı, bilgisayarlara ve dijital teknolojilere aşinalıklarıyla ilişkilendirilmiştir. Öte yandan kadınların çevrimiçi şiddetin daha çok hedefinde olmasına rağmen, bunları bertaraf etmek ve mahremiyetlerini korumak için farklı stratejiler geliştirmiş olabileceklerine de değinilmiştir[33]. Kısaca değinilen bu bulguların, adalete erişim süreçlerinde yaşanan sorunlarla benzeşmesi tesadüf değildir. Kişisel verilerin korunması düzenlemelerinin merkezinde yer alan hak sahipleri bireysel düzeyde mahremiyetlerini korumaya çalışırken, hukuk sistemlerinin diğer yapısal sorunlarından da etkilenmektedir.

GDPR'ın *Cambridge Analytica* skandalındaki muhtemel uygulamasını değerlendiren bir çalışmada[34], GDPR hükümlerinin 2016 ABD Başkanlık seçimlerinde uygulanması halinde ihlalleri engellemek için çok az şey yapabileceği öne sürülmüştür. GDPR hükümleri yalnızca

31 Lemi Baruh ve Mihaela Popescu, "Big data analytics and the limits of privacy self-management", *New Media & Society* 19, sy 4 (2017): 592.

32 Mustafa Berkay Aydın, "Dijital Sosyoloji Üzerine Notlar", içinde *Dijital Sosyoloji Çalışmaları*, ed. Aslıhan Zinderen (Ankara: Nobel Bilimsel Eserler, 2021), s. 8-10.

33 Antonie Courmont, "Le plaignant type ? Un homme, diplômé et cadre | LINC", linc.cnil.fr, ubat 2023, https://linc.cnil.fr/fr/le-plaignant-type-un-homme-diplome-et-cadre.

34 Alexis Ward, "The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?", *Trinity College Law Review* 25 (2022): 221-42.

kişisel verilerin kullanımı için geçerli olduğundan, *Cambridge Analytica* GDPR hükümlerini tamamen anonimleştirme teknikleriyle ortadan kaldırabilirdi. Böylece kişisel tanımlayıcı bilgileri kullanmadan da tüm veri kümeleriyle aynı amaçlara ulaşabilirdi. Anonimleştirme olmasa bile, *Cambridge Analytica*, veri sahiplerinin gerekli rızasıyla verileri yasal olarak işleyebileceğinden, GDPR koruması çok da etkili olmayacaktı. Sürekli onaydan bıkmış kullanıcıların önündeki karmaşık onay koşulları, *Cambridge Analytica* gibi karmaşık denetleyicilerin bu güçlü veri kümelerini oluşturmak için gereken onayı almaları için boşluk yaratabilecekti. Üstelik *Cambridge Analytica*, şirketinin meşru menfaatlerinin veri sahiplerinin menfaatlerinden daha ağır bastığını iddia ederse ve bu bir biçimde kabul görürse, verilerin toplanması için onaya dahi ihtiyaç duymayacaktı. Ayrıca GDPR hükümleri uyarınca veri sahiplerine verilen haklar, muhtemelen *Cambridge Analytica*'nın müdahalesini önlemek için de yeterli olmayacaktı. *Cambridge Analytica*, ancak silme veya işlemeyi kısıtlama haklarını ileri süren veri öznelerinin kalabalık bir şekilde hareket etmesi halinde durdurulabilirdi. Üstelik, veri kümesinden bir model oluşturulduktan sonra silme hakkının ileri sürülmüş olması müdahaleyi engellemeyecekti. Ayrıca bu bireysel haklar, bireyleri daha sonra şirketin hedefi haline gelmekten koruyamazdı[35]. Bu tespitler, ileri düzey koruma sağladığı iddia edilen GDPR düzenlemesinin, pratikte ne kadar işe yaracağını ortaya koyması açısından önem taşımaktadır.

II. HUKUKUN YAPISAL ÖZELLİKLERİNDEN KAYNAKLANAN KISITLAMALAR

A) HUKUK VE TEKNOLOJİ İLİŞKİSİ

Siber alan ve ilgili meselelerin yapısal, teknik ve fiziksel özellikleri, geleneksel hukuksal sınırları ve anlayışları zorlamaktadır. Ağ toplumunda hukuk, çeşitli sorun alanlarıyla muhatap olmak zorunda kalmıştır. Yeni teknolojilerin hukuka neden ve hangi biçimlerde meydan okuduğunu maddeleştiren Van Dijk, yeni toplumun ağ yapısının mevcut

35 Age s. 240-41.

hukuk düzenleriyle karşılanamadığını vurgular[36]. Gerçekten ağlardaki enformasyon ve iletişimin soyut, coğrafi olarak sürekli değişen bir niteliğe sahip olması, yapılan düzenlemelerin uygulanması konusundaki problemler, ağ teknolojisinin sınır ötesi niteliği, hukuksal düzenlemelerin temelinde endüstri devrimi ve hatta endüstri öncesi zanaat ve ticaretin maddi gerçeklerinin yer alması, hukuksal düzenlemelerin, önceki dönem ekonomik gelişmelerin aşamalarına bağlı olması, mevzuatın hızla eskiyen teknolojilerle çerçevelenmesi ve hukuksal düzenlemelerin parçalılığı ve birbiriyle çelişmesi sebepleri bu meydan okumanın başlıca sebepleridir.

Kişisel verilerin korunması konusunda, hukuk ve teknoloji ilişkisine dair bazı temel tespitler yapılabilir[37]. Öncelikle hukuk, teknolojik gelişmelerin gerisinde kalmaya meyillidir. Siber alandaki gelişmeler hukuka sürekli meydan okurken, hukuksal tartışmalara önceki dönemlerin kavram setleriyle karşılık verme çabası baskındır. Bu karşılık genelde tutucu ve tepkiseldir. Hukuk kurallarının konusu hakkında uzlaşma, politik ve ekonomik durum, hukuk kurallarının yürürlüğe girme süreçlerindeki aktörler ve faktörler, ayrıca küresel bir fenomen hakkında konuşuyor olmamız bu eğilimi beslemektedir. Üstelik teknolojik gelişme hızı, siber alanın klasik sınırlarının ve merkezinin olmayışı, teknolojik gerçeklik ile sosyal gerçeklik arasındaki boşluk, bu eğilimi beslemektedir.

Büyük Verinin hukukla ilişkisini GDPR örneği üzerinden ele alan Pagallo, koruma mekanizmalarının ana vurgusunun, yukarıda hukuk içi kısıtlamalar başlığında tartışılan ve GDPR'da belirtilen bireysel rıza ve verilerin en aza indirilmesi, doğruluk ve amaç sınırlaması, bütünlük ve gizlilik ile yasallık, adalet ve şeffaflık ilkelerine ilişkin birincil normlar olduğunu belirtir[38]. Öte yandan teknolojik yeniliğin hızı ve daha genel anlamda düzenleyici sistemler arasındaki rekabet, veri korumada parçalanma risklerine üstün gelmesi gereken koordinasyon çabaları, bu

36 Jan Van Dijk, *Ağ Toplumu* (İstanbul: Kafka Yayınları, 2018), s. 195-97.

37 Duygu Hatıpoğlu Aydın, *Siber Alan ve Hukuk* (İstanbul: On İki Levha Yayıncılık, 2022), s. 137-70.

38 Ugo Pagallo, "The Legal Challenges of Big Data":, *European Data Protection Law Review* 3, sy 1 (2017): 36-46.

alanda teknolojik araştırma ve yeniliğe engel olmaması gereken yasal hakların korunması konularında birincil normlara meydan okumaktadır. Bunun çözümü GDPR'nin Büyük Verinin zorluklarıyla başa çıkmak için bir esneklik payı sağlayan ikincil kuralları aracılığıyla belirli konularda makul bir uzlaşma sağlanmasıdır. Özellikle teknolojinin tarafsızlığı ve deneysel federalizm ilkeleri, GDPR'ı teknolojik yenilik sürecini yönetecek kadar esnek hale getirebilir. Yasal koordinasyon mekanizmaları, yetki devri mekanizmalarını dengeleyebilir. Kişisel verilere dair önleyici koruma usulleri ve yeni kolektif haklarla harekete geçecek hukuksal yollar, alandaki araştırma ve geliştirmeyi kısıtlamadan, Büyük Verinin hukuk alanındaki kısıtlarına cevap olabilir[39].

Ayrıca teknoloji alanında, insan davranışlarını düzenleyen tek kurallar sistemi hukuk değildir[40]. Farklı kural koyucular, siber alanda faaliyetlerini sürdürmektedir ve insan davranışlarını düzenleme kapasitesine sahiptir. Alanın yalnızca hukuk kurallarıyla düzenlenmemesi, kodların, kullanıcı eğilimlerinin, teknik standartların ve şirketlerin kâr odaklı yaklaşımlarının ortaya çıkardığı çelişkiler, siber alanın farklı çıkar grupları arasında bir mücadele alanı olarak işlediğini gösterirken, bütün bu vaziyet, kişisel verilerin korunmasında hukuka dair yapısal bir kısıtlama olarak görülebilir.

B) HUKUK VE SERMAYE İLİŞKİSİ

Hukukun politik karakteri, eleştirel hukukçular tarafından dile getirilen bir olgudur. Siber alanla ilgili meselelerde ve özellikle kişisel verilerin korunmasında, ana aktörlerden biri olan şirketlerin gücü, hukukun sermaye ile ilişkisinin izlenebildiği alanlardandır. Yasa yapıcı güçleriyle devletler ve teknolojiyi üreten, yaygınlaştıran ve bu sayede varlığını sürdürüp büyütebilen şirketler arasındaki ilişki, özellikle ulus devletlerin klasik rollerini değiştirmiştir. Bununla birlikte şirketlerin de rollerinin

39 Age, s 46.

40 Lawrence Lessig, "The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation", *CommLaw Conspectus: Journal of Communications Law and Technology Policy (1993-2015)* 5, sy 2 (1997): 181-92; Lawrence Lessig, "Code Is Law", Harvard Magazine, 01 Ocak 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html.

değiştiğini ve devletleşmeye başladıkları söylenebilir. Bu durumu genel olarak kapitalist üretim modelinin neoliberal döneminde geleneksel yapıların dönüşümünün bir parçası olarak görmek gerekir.

Büyük teknoloji şirketlerinin kişisel veriler mevzuatını çekiştirerek, baskıyla ya da ona uyum sağlamaya zorlanarak etkilediği konusunda şüphe yoktur ve bunun tam tersi de geçerlidir[41]. Gerçekten büyük teknoloji şirketleri gündelik hayatta siber alanla ilişkimizi ve elbette yaşadığımız dönemi belirleme gücüne sahiptir. Özellikle büyük teknoloji şirketlerinin en büyük avantajı olan mevcut müşteri ağları ve iş kolları tarafından üretilen veriyi toplayabilme ve işleyebilme güçleri[42], Büyük Veri çağında onları kuralları belirleyen bir pozisyona sokmuştur. Platformlar ya da *Big Tech* olarak bu büyük şirketler sadece veri toplayarak değil, sunulan seçenekleri belirlemek ve algoritmik yapılandırmalarıyla toplumu derin bir biçimde etkileyebilmekte ve şekillendirebilmektedir[43].

Şirketlerin çeşitli finansal hedeflerine ulaşmalarında etkili araçlardan biri mevcut hukuksal kurumları ve araçları harekete geçirme kabiliyetleridir. Bu, normal ekonomik faaliyetinin kapsamını ve devletin bu ekonomik faaliyetlerdeki pozisyonunu belirlerken, ki bu genellikle çekişmelere dayanır, bu çekişmeler içinde yasal kurumlar değişikliğe uğramaya başlar[44]. Böylelikle şirket mantığının hukuksal kurum ve düzenlemelere sirayet ettiği ve özel mülkiyetin kutsallığı gibi kapitalist değerlerin siber alan kadar, kişisel verilerin korunmasını etkilediği görülebilir. Makro düzeyde kuralsızlık, deregülasyon, özel mülkiyetin korunmasında kullanıcılar ve müşterekler aleyhine düzenlemeler sermayenin kural koyucu rolünün güçlenmesinin örnekleridir. Kişisel verilerin korunması

41 Yakın dönemde İtalyan Veri Koruma Otoritesi'nin OpenAI ürünü ChatGPT hakkında verdiği yasaklama kararı, şirketi, mahremiyet politikalarını yeniden düzenlemeye ve GDPR ilkelerine uymaya zorlayan bir etki yaratmıştır.

42 Wolfie Christl, "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions" (Vienna: Cracked Labs, 2017).

43 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Reprint edition (Cambridge, Massachusetts London, England: Harvard University Press, 2016).

44 Simon Deakin vd., "Legal Institutionalism: Capitalism and the Constitutive Role of Law", *Journal of Comparative Economics* 45 (2015): 188.

alanına baktığımızda, yukarıda tartışılan rıza ve onay araçları, tercihlerinde özgür rasyonel birey tanımlamasına dayanırken, bu mahremiyete verilen değerin ve mahremiyetin hukuki korumasının toplumsaldan bireysele kaymasının bir göstergesidir. Cohen[45], bununla ilişkili olarak mahremiyetin hukuk teorisindeki yerinin, liberal benlik için bir korumayı kavramsallaştırıldığını vurgular.

Kişisel verilerin büyük veri kümesinin bir parçası olması ve hukuksal korumanın özellikle kişisel verilere yönelik olması, şirketlerce toplanan çeşitli verinin, mahremiyetin korunması bağlamında yeterince denetlenememesi sonucunu doğurabilir. Dijital kişisel veriler, yeni bir malvarlığı sınıfını temsil ederek, ekonomide daha fazla önem kazanmaktadır. Bu veri varlıkları üzerindeki kontrol, *Apple*, *Microsoft*, *Amazon*, *Google/Alphabet* ve *Facebook*'tan oluşan (GAFAM) ve *Big Tech* denen şirketlerin ortaya çıkışını ve hakimiyetini açıklar. Büyük teknoloji şirketlerinin kişisel veriler üzerindeki mülkiyet ve kontrol haklarını kendi başlarına genişletmek yerine, kullanıcı ölçümlerinin (örneğin, kullanıcı sayıları, kullanıcı katılımı) performatif ölçümü, yönetişimi ve değerlemesi yoluyla *"kullanıcıları"* ve *"kullanıcı katılımını"* mal varlıklarına dönüştürmesi söz konusudur. Bu sayede *Big Tech*, kullanıcıları ve kullanıcı katılımını (yani kullanıcı verilerini) abonelik veya satış erişimi gibi ölçülebilir, okunaklı ve para kazanılabilir hale getirerek değerlendirebilir. Artık doğrudan kişisel verinin toplanmasına gerek yoktur. Şirketlerin gücü, kişisel verilerin mülkiyetinden ziyade kullanıcıları değerlendirme sürecinden kaynaklanmaktadır. Mevcut düzenlemeler çerçevesinde, şirketlerin kullanıcılar üzerindeki kontrolü, kişisel verileri toplamak ve kullanmak için sözleşmeden doğan haklara bağlıdır. *Big Tech*, kullanıcı verilerinin toplanmasını ve para kazanılmasını artırdıkça, bu sözleşmelerdeki yasal değişiklikler yoluyla sürekli sözleşme kapsamını genişletebilirler[46].

45 Julie E. Cohen, "What Privacy is for", *Harvard Law Review* 126, sy 7 (2013): 1905.

46 Kean Birch, D Cochrane, ve Callum Ward, "Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech", *Big Data & Society* 8, sy 1 (16 Mayıs 2021): 1-15.

Hukuk ve sermaye arasındaki ilişkinin kişisel verilerin korunması mekanizmalarına yansımasının bu bağlamdaki bir başka örneği, verilerin toplanmasındaki amaçlarda belirsizliktir. Kişisel verilerin işlenmesi için hukuka uygun olarak ve açık ve meşru amaçların belirlenmiş olması ve verilerin toplanması aşamalarında da açıkça ifade edilmiş olması gerekir. Uygulamadaki *"pazarlama amacıyla"* ya da *"kullanıcı deneyimini geliştirmek"* gibi yorum ve ifadeler ile şirketlerce öne sürülen *"meşru menfaat"* kişisel veri otoritelerince de[47] tartışılan ve belirsiz bir gerekçedir.

Eşitsizliğin derinleşmesinde haklardan (bir bakıma olması gereken) beklentilerin yüksekliği ile uygulama (olan) arasındaki ilişkiye dikkat çeken Solove, mahremiyet haklarının, çok daha büyük bir mimarinin küçük bir parçası ve en fazla destekleyicisi olduğunu vurgular[48]. Mahremiyetin korunmasında bireye yüklenen misyonun abartılması çeşitli teknolojik araçların bireyin elini kolunu bağlaması yanında, veri toplama ve işlemenin enformasyonel kapitalizmin[49] temel iş modellerinden biri olması, şirketlerin gizliliği korumak için motivasyonlarını kamusal haklardan ya da insan haklarından uzaklaştırmaktadır. *"İnovasyon"* etrafında kümelenen kültürel ve politik söylemler, şirket faaliyetlerinin devlet kontrolünden muafiyetini destekler[50]. Böylece teknolojinin geliştirilmesi gibi *"erdemli ve üretken"* faaliyetler, yine, gizliliğin korunması ile piyasa verimliliği arasındaki gerilimde ikincisini destekler. Bir biçimde veriler üzerinden beslenen şirketler ağı, verileri toplamanın ve işlemenin önündeki hukuksal engelleri aşacak çeşitli teknolojik girişimler de yapabilmektedir. Bu durumda da hizmeti sunan şirketler ve hak sahibi

47 Örneğin Belçika Veri Koruma Otoritesi, IAB Avrupa (Interactive Advertising Bureau Europe) tarafından geliştirilen Şeffaflık ve Rıza Çerçevesi'nin (TCF) GDPR'nin bir takım hükümlerine uymadığını tespit etmiş, ilgili şirkete 250.000 € para cezası vermiş ve şirketin faaliyetlerini IAB Avrupa ile uyumlu hale getirmek için bir eylem planı sunması için iki ay süre tanımıştır. "The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR | Autorité de protection des données
Gegevensbeschermingsautoriteit", Şubat 2022, https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr.

48 Daniel J. Solove, "The Limitations of Privacy Rights", *Notre Dame Law Review* 98, sy 3 (2023): 975-1036.

49 Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York, NY: Oxford University Press, 2019).

50 Julie E. Cohen, "The Regulatory State in the Information Age", *Theoretical Inquiries in Law* 17, sy 2 (27 Temmuz 2016), https://www7.tau.ac.il/ojs/index.php/til/article/view/1425.

kullanıcılar arasındaki yapısal eşitsizlik, son kertede kişisel verileri toplanan kullanıcıların aleyhine derinleşmektedir.

Veri gizliliği ile ilgili yasal gerekliliklere uymak elbette teknolojik ekosistemdeki herhangi bir sorumlu oyuncu yani şirketler için büyük önem taşımalıdır. Bu alandaki kuruluşlar, düzenleyicilere, tüketicilere, ortaklara ve davacılara, veri gizliliği hususlarını teknolojilerine tam olarak yerleştirdiklerini kanıtlayabilmelidir. Ancak piyasa verimliliğinin, gizliliği korumaya karşı baskın hale gelmesi, şirketlerin sorumluluklarını belirsizleştirmektedir. Denetlenmesi gereken pek çok uygulama ve teknolojik aracın varlığı, sermaye lehine politik ve kültürel kabullerle birleştiğinde hukuksal koruma sınırlı bir alana hapsedilmiş olmakta ve neredeyse işlevsizleşmektedir.

C) KİŞİSEL VERİLERİN GÖZETİMLE İLİŞKİSİ

Kişisel verilerin korunmasında hukukun yapısal sınırlarından bir diğeri, verilerin toplanmasında sadece şirketlerin kâr odaklı faaliyetlerinin değil, devlete yüklenmiş en önemli işlevlerden biri olan güvenlik amacının da etkisiyle kişisel verilerin korunmasıyla gözetimin ilişkisidir. Burada, piyasa verimliliği ve mahremiyetin korunması arasındaki gerilime benzer biçimde bir özgürlük-güvenlik ikileminin hukuksal korumanın çerçevesini çizdiği söylenebilir.

Devletler açısından güvenlik amaçlı gözetim, gizliliğin korunması bakımından şirketlerin belirsizliklerle dolu "meşru menfaat" amacıyla benzerdir. Siber güvenlik şemsiyesi altında devletlerin birbirlerine ve farklı grupların devletlere yönelik hareketleriyle çerçevelenen istihbarat faaliyetleri, pratikte gizliliğin korunmasına önemli bir istisna oluşturmaktadır. Gündelik hayatın olağan bir parçası haline gelen akıllı şehir uygulamaları, e-devlet uygulamaları, sınırların kontrolü, devletlerin egemenlik alanlarında gerçekleşen ve egemenliklerine referans veren veri akışlarıdır[51]. Elbette güvenliğin sağlanması açısından gözetimin fayda-

[51] Güvenliğin sağlanması amacıyla verilerin toplanmasının en büyük handikaplarından birisi, verinin büyüklüğü ile veri ihlallerinin artışı arasındaki doğru orantıdır. Güvenliğin sağlanması için veri toplanabilen

ları yadsınamaz. Hatta pek çok elektronik uygulama, çipler, kameralar, kodlar ve benzerleri gündelik hayatı da oldukça kolaylaştırmaktadır. *"Elektronik gözün"* iyi huylu tarafının[52], akıllı profilleme, yapay zekâ/makine öğrenmesinin kullanıldığı aygıtlar, yüz tanıma gibi ileri düzey gözetleme teknolojileri ile adeta görünmez (ve aşağıda değinileceği gibi doğal) hale gelmesiyle, mahremiyete verilen anlam ve önemin denetimle dönüştüğünü göz önünde bulundurmak gerekir. Ayrıca gözetim kapitalizminin[53] yasal araçlarla derinleşerek sürmesi, bir yandan hukuksermaye ilişkisine göz kırparken, öbür tarafta gözetimin temelini oluşturan profilleme, mevzuat boşlukları vasıtasıyla, manipülasyona açık ama baktığımızda "kişisel olmayan" veri kümelerinin toplanmasını olanaklı kılar.

Devletlerin güvenlik amacıyla gözetim olgusunu, eski dönemlerden ayıran önemli bir etki, veri toplamanın başlıca aktörlerinden olan şirketlerin, bu gözetime dolaylı ya da doğrudan, zorla ya da gönüllü[54] destek vermesi olmuştur. Şirketler aracılığıyla toplanan verilerin güvenlik amacıyla el değiştirdiği bir gerçektir. Örneğin, nesnelerin internetinin yaygınlaşması sonucu, kendi kendine gözetim bilgilerinin kitlesel üretimi, mahremiyetin çehresini değiştirmiştir. Nesnelerin interneti özel şirketlere ve dolayısıyla hükümetlere benzeri görülmemiş şekillerde veri aktarımı için kolaylık sağlamaktadır. *IoT* araçlarıyla bir insanın hayatının her alanından toplanabilen veri, bir yandan ticaret akışının bir parçası haline gelirken, hükümetlere de bilgileri, satın alma, istihbarat programları aracılığıyla toplama veya özel şirketlerle ortaklıklar yoluyla elde etme fırsatı

teknolojik araçlar ve altyapılar arttıkça ve etki alanları genişledikçe, veri hırsızlıkları, manipülasyonlar ve güvenlik ihlallerine karşı savunmasız kalma ihtimali artar. Akıllı şehirlerde dört kademede (akıllı nesneler, akıllı mekanlar, akıllı altyapılar ve akıllı vatandaşlar) veri kırılganlıklarına değinen bir çalışma için bkz. Daniela Popescul ve Laura-Diana Genete, "Data Security in Smart Cities: Challenges and Solutions", *Informatica Economică* 20, sy 1 (2016): 29-38.

52 David Lyon, *Elektronik Göz: Gözetim Toplumunun Yükselişi*, çev. Dilek Hattatoğlu (İstanbul: Sarmal Yayınevi, 1997), s. 10.

53 David Lyon, *Gözetlenen Toplum- Günlük Hayatı Kontrol Etmek*, çev. Gözde Soykan (İstanbul: Kalkedon Yayınları, 2006); David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique", *Big Data & Society* 1, sy 2 (01 Temmuz 2014); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

54 Amitai Etzioni, *Privacy in a Cyber Age* (New York: Palgrave Macmillan, 2015), s. 93 vd.

vermiştir[55]. *IoT* yanında, sosyal medya platformlarının devletlerle ilişkilerini düşündüğümüzde, devletin elektronik gözünden saklanmak adeta olanaksız hale gelmiştir.

Gizlilik ve güvenlik ilişkisindeki en büyük handikaplardan biri, gizliliğin güvenliğe karşı çoğunlukla yenilmesidir, çünkü yaşam ve uzuv tehlikede iken, mahremiyet hakları daha soyut ve belirsiz kalır. Birçok insan daha güvenli olmak için mahremiyetlerinden vazgeçmeleri gerektiğine inanır. Tartışmanın güvenlik tarafındakiler, insanları bu uzlaşmayı kabul etmeye teşvik etmek için güçlü argümanlar öne sürerler. Bunlardan en bilineni "gizleyecek bir şeyim yok" argümanıdır. Buna göre, gizleyecek bir şeyi olmayan insanların gözetlenmekten korkmaları ya da gözetime karşı çıkmaları için hiçbir sebep yoktur. Solove bu argümanların, mahremiyeti korumanın ne anlama geldiğine ve bunu yapmanın maliyet ve faydalarına ilişkin yanlış görüşlere dayandığını ileri sürer[56]. Ona göre, gizlilik ve güvenlik arasındaki tartışma yanlış çerçevelenmiştir ve bu değerler arasındaki değiş tokuş ya hep ya hiç önerisi olarak anlaşılmıştır. Ayrıca Solove, güçlü güvenlik önlemlerine sahip olmanın ve gizliliği korumanın birlikte mümkün olduğunu da belirtir. Güvenliğin sağlanmasıyla gizliliğin korunması arasında bir denge kurulmasının olanaklılığı bir yana, ikisi arasındaki çekişmede kişisel verilerin korunmasının değerinin düşmesi, bu çalışma için bir sınırlılığı ifade etmektedir. Bu dengenin oluşturulacaksa, güvenliğin sağlanması için veri toplama faaliyetinin yalnızca devletler yoluyla gerçekleşmediğini, büyük gözetim ağında şirketler gibi farklı aktörlerin de devreye girdiğini görmek gerekir. Yasadışı gözetim ya da devletlerin yetki aşımı gibi olaylarda vatandaşları koruyan çeşitli hukuksal düzenlemelerin ve koruma mekanizmalarının, şirketlerin doğrudan kişisel verileri ya da profillemeye yarayan ikincil verileri toplamasında işe yaramaması da bu dengede kişisel verilerin korunmasını kısıtlamaktadır. Dolayısıyla kişisel verilerin korunmasıyla güvenlik amacıyla gözetim, teknolojik araçların kapasitesiyle, siber alandaki ak-

55 Friedland, "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy", s. 912.

56 Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, Illustrated edition (New Haven London: Yale University Press, 2013).

törlerle ve korunan değerlere verilen önemin toplumsal inşasıyla birlikte düşünülmelidir.

GDPR düzenlemesini gözetim bağlamında değerlendiren Andrew ve Baker, Büyük Veriyi kontrol etme çabasının, veri korumasında genel bir iyileştirmeden ziyade risklerin dengelenmesini sağladığını iddia etmektedir[57]. Bu iddialarını siber yasaların yeni "altın standardını" tartışmalı bir şekilde somutlaştırdığını söyledikleri GDPR ilkeleri çerçevesinde sınarlar. Sonucunda ise, aslında yasaların koruma altına aldığı çeşitli güvencelerin, anonimleştirme ve takma adların, gizlilik kaygılarını bertaraf etmekte etkili karşı önlemleri temsil ettiğini, öte yandan aynı korumanın davranışsal ve diğer tanımlanmamış veri biçimlerinin kullanımını, toplanmasını ve ticaretini de teşvik ettiğini iddia edeler. Esasen burada mahremiyetin ve gözetimin kavramsallaştırılmasındaki farklılıklara dikkat çekmek gerekir. Özünde mahremiyet, bireylerin şahsi bilgilerinin görünürlüğü üzerinde kontrol sahibi olma haklarıyla ilgilenir, ancak aynı zamanda fiziksel bedenlerimize, duygularımıza, kişisel ilişkilerimize, politik görüşlerimize ve seçimlerimize ilişkin hakları da içerir. Daha ayrıntılı ve daha kişisel verilerin toplanmasıyla mahremiyet ihlallerinin arttığı düşünülür çünkü bu verilerin derinliği bireyleri özne olarak yakından hedeflemek için kullanılabilir. Mahremiyeti gözetimden ayıran en önemli unsurlardan biri çoğunlukla, mahremiyet endişelerinin birey ölçeğinde kavramsallaştırılmasıdır. Gözetime baktığımızda, mahremiyeti koruyan yasaların etkisizliği ortaya çıkar çünkü gözetimde bireylere özel bilgilerin toplanması amacından çok, anonimleştirilmiş veri setlerine erişimi hedeflenir. Gözetimde toplanan veriler, algoritmalar ve analitiklerle hem geçmiş olayları anlamak hem de gelecekteki davranışları tahmin etmek için bireyleri ve grupları zamana ve mekâna yerleştirmek için büyük şirketler ve hükümetler tarafından kullanılır. Böylece klasik tanımıyla kişisel verilere ihtiyaç duymadan bireyler ve topluluklar hakkında bilgi toplamak veya bireyler arasında açık bağlantılar kurmak mümkündür. Gözetimdeki risklerin bu biçimde kavramsallaştırılması, bu riskler hakkındaki anlayışımızı, kişisel verilerin toplanması ve ticare-

57 Jane Andrew ve Max Baker, "The General Data Protection Regulation in the Age of Surveillance Capitalism", *Journal of Business Ethics* 168, sy 3 (2021): 565-78.

tinin daha geniş kontrol ve yönetişim etkilerini içerecek şekilde genişletmektedir[58]. Yazarlara göre, GDPR'nin veri etiğini, özellikle davranışsal verilerle ilgili olarak kodlamaya yönelik çabası sınırlıdır, çünkü düzenlemedeki istisnalar, şirketlerin GDPR kısıtlamalarından kaçabilecekleri bir geçit oluşturur. Böylece GDPR, ticari çıkarları geliştirebilecek davranışsal bir veri pazarı için alan yaratmaktadır[59]. GDPR kapsamında korunan kişisel verilerin dışında kalan sahipsiz veri kümelerinin, algoritmik profillemede ya da örneğin seçimlerin büyük ölçekli değiştirilmesinde potansiyel kullanımı önemli endişeler doğurmaktadır.

Özgürlük ve güvenlik arasında denge kurulması, kişisel verilerin korunması bağlamında somutlaştırıldığında, veri koruma mevzuatının gerektirdiği temel koşulların olmadığı devletler açısından önemli güvenlik ve ihlal sorunları doğacağı da bir gerçektir. Kişisel verilerin korunması mevzuatı asgari bir hukuk devleti ve demokrasi zemininde mümkündür. Bu zemindeki kaymalar, kişisel verilerin korunmasını da doğrudan etkileyebilmektedir. Dolayısıyla gözetimde şeffaflık, hesap verilebilirlik, hukuka uygunluk gibi kriterleri gerçekleştirmekten uzak yönetimler açısından, koruma mevzuatının yapısal sınırlarıyla yeniden karşılaşılır. Konuyla ilgili belirgin örneklerden biri Çin'in pozisyonudur. Çin menşeli pek çok uygulama (TikTok gibi), özellikle ABD tarafından bir biçimde denetim altına alınmaya ya da yasaklanmaya çalışılırken, öne çıkan sebep kişisel verilerin korunması ve ulusal güvenliktir. Bunun yanında demokratik anayasalara sahip olmakla birlikte pratikte hukuk devleti usullerinin işletilmediği çeşitli ülkelerde, vatandaşların güvenlik amacıyla toplandığı iddia edilen verilerinin bu bilgilere erişimi olan üst düzey yetkililer tarafından usulsüz, hukuka aykırı kullanımı, hatta bazı örneklerde yurtdışına transferi gibi güvenlik açıkları söz konusu olabilmektedir.

58 Age, s. 569-70.

59 Age, s. 576.

III. KİŞİSEL VERİLERİN HUKUKSAL KORUMASINDA SOSYAL KISITLAMALAR

Kişisel verilerin hukuksal korumasının sınırlarını çizen, aynı zamanda hukuk uygulamasının da etkisinde biçimlenen bir konu da veri öznelerinin ya da ilgili kişilerin mahremiyetlerine ve verilerinin korunmasına verdikleri anlamlardır. Hukukun mahremiyetin tanımını ne şekilde yaptığıyla bağlı olarak ama hukukun kendisini de etkileyecek biçimde, etkinliği ölçmekte kişilerin gizliliklerinin korunmasındaki hevesleri, istekleri ve hukuksal korumayı harekete geçirebilme motivasyonları önemlidir. Mahremiyet hakkında insanların fikirlerini ve dolaylısıyla hukuksal korumanın sınırlarını belirleyen anlayışlar, hukuksal düzenlemeler kadar veri toplama pratiği ve teknolojik durumdan da etkilenmektedir.

A) MAHREMİYETİN KORUNMAYA DEĞER OLUP OLMAMASI

Mahremiyet nedir, neden önemlidir ve nasıl korunmalıdır sorularının cevapları çeşitlendirilebilir. Hatta bir tanım birliği olmamasının hukuk uygulamasına yansıyan yönleri de vardır. Mahremiyetin korunmasına dair düzenlemeler ve hukuk uygulamasının kendisi de sınırları ve özellikle mahremiyetin tanımına yönelik belirsizlikleriyle, kamusal beklentiler ve gerçeklik arasında uyumsuzluk yaratır[60]. Allen, mahremiyetin çeşitli görünümlerine ve koruma mekanizmalarına değindiği çalışmasında, mahremiyeti koruyan yasal düzenlemelerin referans verdiği popüler gizlilik kadar, çoğunlukla farkında olmadığımız, popüler olmayan mahremiyetin de korunması gerektiğini ifade eder[61]. İnsanların mahremiyetlerinin korunmasının önemli ve değerli olduğuna dair bir varsayımdan yola çıkan hukuksal düzenlemeler, korunmaya değer olanın çerçevesini çizerken, mahremiyete verilen önem ve değerin insanlardaki karşılığı ölçüsünde etkili olabilecektir.

60 Philip Leith, "The socio-legal context of privacy", *International Journal of Law in Context* 2, sy 2 (2006): 105-36.

61 Anita Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press, 2011).

Hukuksal düzenlemeler ve kullanıcıların mahremiyete verdikleri değer ve koruma davranışları, bir açıdan mahremiyetin performatif özelliğine[62] vurgu yapar. Mahremiyetin gerçekleştiği kadar korunduğu iddiasını taşıyan bu yaklaşıma göre, hukuksal düzenlemeler bu performansın bir parçasıdır. Belirli rollerin ve değerlerin sürekli tekrar edilmesi ya da "gerçekleştirilmesi" bu davranışları normalleştirdiği gibi, bir süre sonra bunu bir alışkanlık haline getirir[63]. Yani hukuksal çerçeve, mahremiyetin ne olduğu hakkındaki fikrimizi ve gizliliği korumak için yapabileceklerimizin sınırını çizerek, mahremiyeti sosyal olarak inşa eder. Aynı şekilde çeşitli alışkanlıklar hem mevcut normları hem de alternatif beklentilere dair olanakları belirler. Bu iddiayı, şirketlerin mahremiyet hakkındaki söylem ve girişimleri çerçevesinde değerlendiren Waldman, şirket içi anlatıların ve şirketler hakkındaki şirket çalışanları ve kamuoyu algısının, aynı şirketlerin fiili uygulamalarıyla ters düşen değerleri inşa edebildiğini belirtir[64]. Veri sahibi kullanıcılar açısından mahremiyet, diğer aktörlerle birlikte mahremiyet hakkındaki performanslarını sergiledikleri bir sahneye dönüşecektir.

Mahremiyetin hukuksal korunmasında bireye biçilen bir rol olduğu yukarıda tartışılmıştı. Bu rolün hayali olduğunu belirten Acquisti ve Grossklags[65], insanların, kişisel mahremiyet söz konusu olduğunda ekonomik olarak rasyonel failler olarak hareket edemeyebileceklerini ve gizlilikle ilgili kararların eksik bilgilerden, sınırlı rasyonellikten ve doğrulama önyargısı, hiperbolik indirim[66] gibi psikolojik önyargılardan

62 Ari Ezra Waldman, "Privacy, Practice, and Performance", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 01 Şubat 2021).

63 Garfield Benjamin, "Privacy Norms and Resistances Between the Performative, the Habitual and the Periperformative", *Social Epistemology Review and Reply Collective* 11, sy 1 (2022): 7-13.

64 Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (Cambridge: Cambridge University Press, 2021).

65 Alessandro Acquisti ve Jens Grossklags, "Privacy Attitudes and Privacy Behavior", içinde *Economics of Information Security*, ed. L. Jean Camp ve Stephen Lewis, Advances in Information Security (Boston, MA: Springer US, 2004), s. 165-78.

66 Hiperbolik indirim, insanların gelecekteki ödüllere nazaran acil ödüllere ve tatmine öncelik verdikleri psikolojik bir önyargıdır. Satış ve pazarlamada, tüketicileri kısa vadeli ödül veya anında tatmin temelinde satın almaya teşvik etmek için kullanılır. Ariel Rubinstein, "'Economics and Psychology'? The Case of Hyperbolic Discounting*", *International Economic Review* 44, sy 4 (2003): 1207-16.

etkilendiğini savunmaktadırlar. Bireyler kişisel bilgilerini bir fayda gördüklerinde ifşa edebilirler, ancak aynı zamanda bu bilgilerin işleniş biçiminden önemli ölçüde etkilenirler. Kişisel verilerin ikincil kullanımı konusunda önemli ölçüde endişe duyabilirler ve bu endişeler temkinli bir davranışa yol açabilir. Dolayısıyla, mahremiyetin korunmaya değer olduğu fikriyle siber alandaki faaliyetlerin mutlak şekilde örtüşmesinden söz edilememektedir. "Mahremiyet paradoksu"[67] olarak tarif edilen bu olgu, genel olarak insanların mahremiyetlerini koruma hakkındaki tutum ve davranışları arasındaki çelişkiye işaret eder.

Mahremiyet paradoksunu ölçmeye yönelik çeşitli araştırmalarda bu çelişkinin ortaya çıktığı ama bazılarında da insanların mahremiyetlerine verdikleri değer ölçüsünde koruma davranışı gösterdikleri ortaya konmuştur. Bu araştırmalar arasındaki farkların sebeplerine değinen bir çalışmada[68], bireylerin, belirli bir alıcıya bazı kişisel bilgileri satmaya ve hatta vermeye istekli olabilecekleri, ancak yine de rızaları olmadan aynı verilerin kontrolsüz bir şekilde kullanılmasına şiddetle itiraz ettikleri, bunun bir anlamlandırma meselesi olduğu vurgulanmıştır. Ayrıca mahremiyet davranışı oldukça bağlamsal bir olgudur bu nedenle, bireylerin aynı davranışı farklı bağlamlarda aynı biçimde göstermelerini beklenemez. Bir diğer husus, kişisel bilgilerin somut ve değişmez olmaları, farklı türde kişisel bilgilere bireylerin farklı değerler atfedebilmeleridir[69]. Mahremiyet paradoksu, bilgiye dair duyarlılıkların tam olarak ifade edilmemesinden de kaynaklanabilir. Elbette araştırmaların yapılış biçimleri de böylesi bir farkın ortaya çıkmasına sebep olmaktadır.

Mahremiyetin korunmasında hukuksal düzenlemelerin sınırı bağlamsallık, farklı kültürlerde mahremiyete verilen çeşitli anlamlar ve değerler, bireylerin karmaşık veri kümeleriyle baş etmekte yaşadıkları

67 Susanne Barth ve Menno D. T. de Jong, "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review", *Telematics and Informatics* 34, sy 7 (2017): 1038-58.

68 Spyros Kokolakis, "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon", *Computers & Security* 64 (2017): 122-34.

69 Anya Skatova vd., "Unpacking privacy: Valuation of personal data protection", *PloS one* 18 (03 Mayıs 2023): 1-21.

zorluklar, mahremiyet performanslarının önem ve değere etkisi ve çeşitli sosyal normların benimsenme düzeyleriyle çizilir. Şüpheli görünmemek, gizleyecek bir şeyi olmadığı fikri, mahremiyet ihlallerinin çeşitli hizmetlere ulaşılmasında bir bedel olarak görülmesi gibi, mahremiyetin korunmasını etkileyen çeşitli sosyal normlardan söz edilebilir.

Bilgiye erişimin önündeki engelleri aşmak adına kullanılan teknolojik araçlar, anonimleştirmeyi destekleyen uygulamalar, kullanıcıların kimliklerinin ve faaliyetlerinin gözetimden uzak kalmasına yol açarken, bir açıdan da veri toplayıcılarına açık bir meydan okumaya dönüşebilir. Çünkü anonimleştirme, özellikle devletler açısından pek çok tehdidin tespit edilmesi ve bunların gerçekleşmesinin önlenmesinde engel olarak görünmektedir[70]. Böylece veri toplanmasına rıza göstermemek, bir yandan belirli hizmetlere erişimi olanaksızlaştırırken, diğer yandan kişileri şüpheli bir pozisyona sokabilir. İnsanlar anti-sosyal, ya da suçlu veya şüpheli gözükmemek adına aktif bir korumdan vazgeçebilirler.

Kişiler nezdinde mahremiyete verilen önemi ve hukuksal korumanın önemini belirleyen bir başka husus, mahremiyet-güvenlik ikileminde değinilen "gizleyecek bir şeyim yok" düşüncesidir[71]. Bu iddianın açtığı yolun, sadece saklayacak bir şeyleri olanların mahremiyetlerine değer vereceklerine çıktığını ve tam da bu noktada başarısız olduğunu söyleyen Cofone örneklerini, sağlık sigortası yapmak için işçilerinin genetik verilerini işleyen işverenler ve vergi mahremiyeti açısından tartışmaktadır[72]. Üstelik bu varsayımın kabul görmesi, veri korumasının teknolojik olarak neredeyse olanaksız olduğu gerçeğiyle de birleşince, bu yöndeki fikirlerin bir süre sonra bir norm haline gelmesine sebep olabilir.

Düşüncelerin alışkanlıklara dönüşmesi konusunda bir örnek şirketlerin veri toplama faaliyetlerinin ücretsiz internetin sonunu getirebile-

70 Ross W. Bellaby, "Going Dark: Anonymising Technology in Cyberspace", *Ethics and Information Technology* 20 (2018): 189-204.

71 Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy", *San Diego Law Review* 44 (2007): 745-72.

72 Ignacio Cofone, "Nothing to Hide, but Something to Lose", *University of Toronto Law Journal* 70 (2019): 1-41.

ceği düşüncesidir. Bu fikrin benimsenmesi mahremiyetin korunmaya değer olmaması inancını pekiştirmektedir. Richards, kişisel bilgilere onay verilmesi gerektiği, bunun çevrimiçi hizmetlerden ücretsiz yararlanılabilmesi açısından gerekli olduğu fikrinin mahremiyete dair bir mit olduğunu belirtir[73]. Bu mitin yaygın kabul görmesi neticesinde, bireyler verilerini paylaşmaya teşvik edilmiş olur. Bu teşvik ve arkasındaki büyük varsayım, bir süre sonra kişisel verilerin önemi hakkındaki iddiaların ve bunların değerlerinin altını boşaltır.

Kişisel verilerin korunması mevzuatı açısından mahremiyet, genellikle devlet ve ticari aktörlerin giderek yaygınlaşan gözetimine karşı bireysel bir direniş noktası olarak görülmektedir. Mahremiyetin öz yönetimini destekleyen uygulamalarda da bunu görmek mümkündür. Mahremiyet, bireysel özerkliği teşvik ederek, bireysel düzeyde kendi kaderini tayin gücünü ve en azından bireylerin kendini tanımlama kapasitesini korumaktadır. Büyük Veri çağında ise, gizlilik tartışmaları, gizlilik ihlallerinden kaynaklanan zararı bireysel düzeyde tanımlamanın zorluğu nedeniyle karmaşıktır. Aksine şirketler, kullanıcıların artık çevrimiçi ortamlarının gerçek zamanlı olarak aşırı kişiselleştirilmesini beklediklerini ve karşılığında gizlilikten vazgeçmenin karşılıklı olarak bu tür hizmetlerin varsayılanı olarak anlaşıldığını iddia etmektedir. Bu mantığa göre mahremiyet, bir hak olmak yerine, tüketicilerin, özerk aktörler olarak ele alınmaları için ödemek zorunda oldukları bedel haline gelmektedir[74].

Mahremiyet toplumsal içeriğinden uzaklaşıp, bireysel bir değere indirgendikçe, adeta bir fetiş haline gelir[75]. Kaldı ki hukuksal korumanın hedefi de öncelikle ve tercihen bireydir. Özellikle tarihsel süreçte mahremiyete verilen değer değişimini atlayan, kişisel verileri, büyük veriyle birlikte kapitalist üretim ilişkilerinde bir meta veya hammadde kaynağı

73 Neil M. Richards, "Four Privacy Myth", içinde *A World Without Privacy: What Law Can and Should Do?*, ed. Austin Sarat (Cambridge; New York: Cambridge University Press, 2015), s. 71-74.

74 Baruh ve Popescu, "Big data analytics and the limits of privacy self-management", s. 591.

75 Christian Fuchs, "Towards an alternative concept of privacy", *Journal of Information, Communication and Ethics in Society* 9, sy 4 (01 Ocak 2011): 220-37.

olarak değerlendirmeyen, mahremiyetin korunması düzenlemelerini kapitalist üretim ilişkilerinde anlamlandırmayan ve mevcut güç eşitsizliklerinin üzerini örten bir yaklaşımın, mahremiyeti fetişleştirdiğini söylemek mümkündür.

Oysaki, Allen'ın vurguladığı gibi genç olduğumuz, meşgul olduğumuz ya da zevk aldığımız gizemli teknolojiyle gelen veri toplama, paylaşma ve depolama risklerine aşina olmadığımız için kendi mahremiyetimize bilinçsizce kayıtsız kalabiliriz. Burada hukuksal düzenlemeler vasıtasıyla, devletin bizi yalnız bırakmasını gerektiren yasalar kadar, başkalarının bizi yalnız bırakmasını sağlamak için devletin bize yardım etmesini gerektiren yasalara da ihtiyaç vardır[76]. Dolayısıyla, mevcut durumda bireylerin mahremiyetlerine verdikleri değeri azaltan ve çeşitli sebeplerle önemsizleştiren anlayışlar karşısında, hukuksal düzenlemelerin sağladığı koruma bulanıklaşmaktadır.

B) BÜYÜK VERİ VE MAHREMİYETİN KORUNMASININ OLANAKLARI

Kişisel verilerin yaygınlığı ve neredeyse siber alandaki her faaliyete saçılmış olması, hukuk uygulaması veri üreticileri olarak bireylerin mahremiyetlerini korumayı değerli bulup bulmamaları yanında bunun olanaklarını da etkilemektedir. Veri toplamanın teknik kolaylıkları ile bireylerin bu teknik okuryazarlığa sahip olmaması, ayrıca birey düzeyinde bağımsız bir korumanın mümkün olmaması korumayı sınırlamaktadır. Bu konuda bir başka dikkat çekici husus, hukuk uygulamasının bireylerin anlayışlarında ve teknik kapasitede yarattığı sınırlardır. Sürekli olarak izleniyor olma hali, hukukun çeşitli sebeplerle ve küçük de olsa izlenmeyi hem meşru hem de yasal kılması, mahremiyetin korunmasını zorlaştırmaktadır.

Siber alanın ağ yapısından kaynaklı, verilerin dolaşımı bir ağda gerçekleşir ve bireysel faaliyetler doğrudan ya da dolaylı olarak diğer kullanıcıları etkileyebilir. Kişisel verilerin korunması açısından bireyler kendi

76 Allen, *Unpopular Privacy: What Must We Hide?*, s. 196.

mahremiyetlerini korumak adına ne kadar özenli davranırlarsa davransınlar, başkalarının verilerinin de dolaşımda ve verilerin birbirleriyle etkileşimde olması sebebiyle, diğerlerinin ağlarının dışında kalamazlar ve böylece kendi mahremiyetleri de dolaylı da olsa tehdit altında olabilir[77]. Dolayısıyla birbirine bağlı bir mahremiyet olgusundan bahsetmek mümkündür. Bir çalışmada bireylerin kişisel bilgilerinin başkaları aracılığıyla açıklanmasının, özellikle çevrimiçi platformlar bağlamında gizliliği giderek daha fazla tehdit ettiğine değinilmiştir[78]. Yazarlar, kullanıcıların çevrimiçi platformlarla etkileşimde bulunurken başkalarının gizliliğini neden ve nasıl korumaya veya ihlal etmeye karar verdiğinin daha derin bir şekilde anlaşılması ve etkili çözüm yollarının araştırılması problemiminden hareketle çeşitli sonuçlara ulaşmışlardır. Buna göre, GDPR gibi mevcut düzenlemeler, birbirine bağlı gizlilik ihlallerini yeterince dikkate almamaktadır. Bu, çevrimiçi platform sağlayıcılarının bireylerin gizlilik haklarını akranları aracılığıyla ihlal etmeleri için bir boşluk sunar. Çevrimiçi platformlar, başkalarının bilgilerini paylaşırken kullanıcıdan onayını isterken (örneğin, "Erişime İzin Ver"), veri aktarımına dahil olan çok sayıda veri, sahibine ne bildirilir ne de vazgeçme imkânı verilir[79]. Gizlilik açısından ideal bir dünyada, kullanıcıların ortak sahiplerinin rızası olmadan başkalarının kişisel verilerini paylaşmalarına izin verilmeyecek olsa da günümüzün birbirine bağlı ortamında bu mümkün değildir. Bununla birlikte, kullanıcıların başkalarının kişisel bilgilerinin açıklanması konusunda bilinçli bir karar vermelerini sağlamanın, birbirine bağlı gizlilik ihlallerini önemli ölçüde azaltabileceği iddia edilmektedir. Her ne kadar kişinin kendi bilgilerine erişim sağlarken zorunlu katılım mekanizmaları talep eden GDPR'ın yürürlüğe girişiyle, kuruluşların gizlilik politikalarının şeffaflığı ve görsel temsili iyileşmiş olsa da yeni düzenlemelerin başkalarının verilerini açıklarken zorunlu ve bilgilendirici katılım mekanizmalarını içermesi gerekmektedir. Kullanıcıların gizlilik endişeleri, çevrimiçi platformlardaki tercihlerini ve davranışlarını bireysel düzeyde

77 Solove, "The Limitations of Privacy Rights".

78 Anjuli Franz ve Alexander Benlian, "Exploring Interdependent Privacy – Empirical Insights into Users' Protection of Others' Privacy on Online Platforms", *Electronic Markets* 32, sy 4 (01 Aralık 2022): 2293-2309.

79 Age, s. 2304.

etkileyebilmekle birlikte, birbirine bağlı gizlilikle ilgili bilinçli kararlar alınabilecek kullanıcı arayüzlerinin tasarımı önerilmektedir[80].

Mahremiyete verilen değerle bağlantılı olarak şunu da vurgulamak gerekir ki, kültürel farklılıklar her zaman mevcuttur. Farklı kültürlerde mahremiyete verilen değerin, ya da hangi verinin korunmaya değer olduğu konusundaki yaklaşımların çeşitliliği, hukuksal korumayı zayıflatmaktadır. Bilgi çağında mahremiyete dair insan davranışlarında belirsizlik ve bağlam bağımlılığı, insanların mahremiyeti içeren karmaşık takaslarda kendi çıkarları doğrultusunda hareket etmelerine her zaman güvenilemeyeceği anlamına gelir. İnsanlar genellikle paylaştıkları bilgilerin farkında değildirler, bu bilgilerin nasıl kullanılabileceğinin farkında değildirler ve paylaşmanın sonuçları hakkında tam bilgiye sahip oldukları nadir durumlarda bile kendi tercihleri konusunda belirsizdirler. Değişen koşullara uyum sağlama yetisi, sırayla, insanların neyi ve ne kadar ifşa ettikleri konusunda kolayca etkilenmelerine sebep olur. Dahası, paylaştıkları şey, bireyler, tüketiciler ve vatandaşlar olarak yaşamlarının birçok alanında duygularını, düşüncelerini ve davranışlarını etkilemek için kullanılabilir. Bu tür bir etki her zaman veya zorunlu olarak kötü niyetli veya tehlikeli olmasa da kişinin kişisel verileri ve gizliliği üzerindeki kontrolünden vazgeçmesi, verileri elinde tutanlar ile bu verilere tabi olanlar arasındaki güç dengesini değiştirir. Verilerin olağanüstü bir hızla üretildiği ve toplanabildiği teknolojik ortamda, yalnızca bireyi bilgilendirmeye veya güçlendirmeye dayanan politika yaklaşımları, son bilgi teknolojilerinin yarattığı risklere karşı yeterli koruma sağlama olasılığının düşük olduğunu göstermektedir. Gerçekten gizliliğin korunması için gerekli koşullar olarak tasarlanan iki ilke olan şeffaflık ve kontrolün, verilerin akışkan büyümesindeki etkisi sınırlı olabilmektedir[81].

80 Age, s. 2305.

81 Alessandro Acquisti, Laura Brandimarte, ve George Loewenstein, "Privacy and Human Behavior in the Age of Information", *Science* 347, sy 6221 (2015): 509-14.

Belirli bir amaçlar toplanan verinin başka amaçlarla kullanılması[82] ve kişilerin haberleri dahi olmadan (örneğin nesnelerin interneti aracılığıyla) toplanan pek çok "yapılandırılmamış" verinin anlamlı içeriklere dönüştürülebilmesi üzerine kurulu Büyük Veri sistemi, gözetim olgusunun, yalnızca devletlerle sınırlandırılamayacak biçimde[83] gündelik yaşamın tüm alanlarında hâkim hale gelmesine yol açmıştır. Sürekli gözetleniyor olmak ve bundan kaçışın olmaması hali, hukukun izin verdiği gözetim, veri toplama ve üstü çeşitli sebeplerle örtülmüş veri ihlalleriyle pekişmektedir. Hartzog, Selingen ve Gunawan insanların çok çeşitli araçlarla ve sürekli gözetlenmesi eğiliminin, mahremiyeti koruyan yasalar her zamankinden daha sağlam hale gelse bile, devam edeceğini iddia etmektedir[84]. Bunun nedeni, mahremiyet yasalarının insanların gözetimin sınırlarını belirleme beklentilerine bakıyor oluşudur. İnsanların izlenmeye alışmaları, yani gözetime maruz kalmaya duyarsızlaşmaları, makul gözetim önlemlerini ve adil uzlaşmaları nasıl gördüklerini etkilemektedir. "Mahremiyet çentikleri" teorisine göre yasa yapıcılar ya da yorumcular daha büyük ve daha ciddi mahremiyet ihlallerini hedefleme eğilimindedir, örneğin zarar eşiği karşılanıyor mu? Bu, daha zayıf, küçük, daha sık ve sıradan mahremiyet ihlallerini göz ardı ederek gözetimi sistematik olarak normalleştirmektedir. Yasa, normlara ve insanların gizlilik ihlali olarak kabul ettikleri için eşikler belirleme beklentilerine baktığı için, çentiklerin normalleştirilmesi, gizlilik standartlarının dezavantajlı bir biçimde sürekli olarak yeniden müzakere edilmesine neden olmaktadır. Mahremiyeti koruyan yasalar, bir süre sonra insanların tahammül edebileceği her şeye izin verir hale gelir. Mahremiyet çentikleri, kapı zilleri, gözlükler ve saatler üzerindeki kameraların ve biyometrik sensörlerin çoğalmasının yanı sıra gözetim ve veri analizinin seyahat, egzersiz

82 Örneğin çeşitli sağlık verilerinin toplanıyor olması, insanların belirli sağlık hizmetlerin ulaşımını kısıtlayabilir. Bu verilerin kimin tarafından, ne şekilde değerlendirileceğine ilişkin uygulamadaki belirsizlikler sebebiyle misal iş hayatında karşısına çıkmaması için pek çok insan psikolojik sağlık hizmetlerine erişimden çekinebilmektedir.

83 Şirketler aracılığıyla toplanan çeşitli verilerin şirketler ve devletler arasında nasıl değiş tokuş edildiğine dair ayrıntılı bir inceleme için bkz. Wolfie Christl, "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions" (Vienna: Cracked Labs, 2017).

84 Woodrow Hartzog, Evan Selinger, ve Johanna Gunawan, "Privacy Nicks: How the Law Normalizes Surveillance", *Washington University Law Review* 101 (2023): 1-77.

ve sosyal toplantılar gibi hayatımızın yeni alanlarına sürüklenmesiyle etkinleştirilir. Hayatın her alanına yayılan ve denetlenmeyen mahremiyet ihlallerinin sonucu yavaş yavaş izlenmeye şartlandırılmış bir toplumdur. Hukuk aracılığıyla bireylerin "makul gizlilik beklentilerinin" düşmesi sonucu gözetim kapasitesinin genişlemesi ve mahremiyetin azalması, kişisel verilerin korunmasında hukukun sınırlarından biri haline gelir.

SONUÇ

Kişisel verilerin korunması mevzuatı, kâğıt üzerinde oldukça güçlüdür. Dijital olarak bağlantılı bir dünyada insanların mahremiyet ihtiyaçlarına belirli değerler çerçevesinde cevap veren mevzuatın etkisi ve gücü yadsınamaz. Bu çalışma, kişisel verilerin korunması hukukunun kuralları, prensipleri, hedeflerinden ziyade, farklı açılardan hukukun gücünü ve etkisini sınırlandıran olgulara odaklanmıştır. Hukukun öngördüğü korumayı sınırlandıran sebepler hukukun iç kısıtlamaları, hukukun yapısal sınırları ve sosyal kısıtlamalar olarak üç ana başlıkta değerlendirilmiştir.

Siber alanın hukuksal atmosferini belirleyen küresellik ve çok hukukluluk özellikleri, hiper regülasyona da yansır. Gerçekten siber alandaki çok taraflı ve katmanlı regülasyon eğilimi, normlar dolayısıyla değerler ve uygulama arasında çelişkilere yol açmaktadır. Ayrıca etkili bir korumanın hayata geçirilmesinde yargı yetkisinin kapsamından kaynaklanan problemler, hukuk içi bir başka sınırlılığı oluşturur. Üstelik teknolojik gelişmelerin hukukun değişimine yansımasındaki gecikmeler sonucunda nesnelerin interneti, yüz tanıma teknolojileri başta olmak üzere biyometrik veriler, kamusal alanda kameralı idari gözetim gibi alanlarda hiç hukuksal düzenleme olmayışı, yani düzenleme boşlukları korumayı zayıflatmaktadır. Nihayet, özellikle GDPR kapsamında hukuk uygulamasını da değerlendirmek gerekir. Kişisel verilerin korunmasının veri sahiplerinin öz yönetimine bırakılmış olması, yasanın korumadan ziyade veri toplamasını yasallaştıran, rızaya sıkıştırılmış hukuk pratiğinin merkezini oluşturmaktadır. Bildirim ve onay aşamalarında verisi toplanan bireylerin aydınlatılmış rızalarının alınmasının önünde, uzun gizlilik sözleşmeleri, hizmetten faydalanmak için onayların zorunlu tu-

tulması gibi kurnazlıklar çıkmaktadır. Bütün bunların toplamı hukukun iç kısıtlamaları oluşturur.

Hukukun teknolojiyle ilişkisi, hukuk-sermaye ilişkisinin kişisel verilerin korunmasına yansıyan kısımları ve kişisel verilerin korunmasının gözetimle ilişkisi, yapısal sınırları oluşturur. Hukukun teknolojik gelişmeler karşısındaki tutucu ve tepkisel tavrı, her iki olgunun oluşma süreçleriyle karşılaştırılmalıdır. Siber alanın özelliklerinden kaynaklanan etkiler, farklı kural koyucuların müdahaleleriyle birleştiğinde, hukukun yapısından kaynaklanan kısıtlar belirginleşir. Ayrıca hukuk-sermaye ilişkisi, neoliberal dönemde geleneksel olanı dönüştürürken, kişisel verilerin korunmasının payına, bir biçimde kayırılan sermaye temsilcileri, korumayı tüketicilere indirgeyen yasal yaklaşımlar ve mahremiyetin korunması aleyhine öne çıkan piyasa verimliliği düşmektedir. Kişisel verilerin, devletin güvenlik amacıyla gözetimi sonucunda topladığı verilerle örtüşmesi, hatta alelade, ham, kişisel ya da hassas veriler arasında herhangi bir ayrım yapmaya gerek bırakmayan kitlesel gözetimin olağanüstü artışı ve yaygınlaşması, gözetim alanında devlet ve şirketlerin dirsek temasları, hukukun bir başka yapısal sınırlılığını oluşturmaktadır.

Son olarak, kişisel verilerin korunması hukukunun uygulamasını belirleyen sosyal kısıtlamalar mevcuttur. Bireylerin mahremiyete verdikleri anlamın kültürlere göre değişmesinin yanında, hukukun mahremiyete dair çizdiği çerçeve de mahremiyetin korunmaya değer olup olmadığını belirler. Bireyleri, mahremiyetlerini korumaya değer olmadığına motive eden, böylece yasal korumayı etkileyen başka olgular da vardır. Hukukun öngördüğü birey bazlı ve bağımsız korumanın, bireylerin mahremiyetlerinin birbirine bağlı olması sebebiyle etkisiz kalması söz konusu olabilmektedir. Gözetimin olağanüstü yaygınlaşması ve sıradanlaşması da korumanın düzeyini etkilediği gibi, bir noktada insanlar bunun imkânsız olduğuna ikna olabilir ya da ikna edilebilirler. Ayrıca bireylerin yasada tanımlanan haliyle kişisel verilerini toplamadan da kullanıcı verileriyle kendileri hakkında bir profil çıkarılabilmesi ve hedefin bu olması, mevzuatı etkisizleştirmektedir. Üstelik yasaların büyük ve görünür veri ihlalleriyle meşgul olmaya eğilimli olmaları ve bunları

parlatmaları, mahremiyet çentiklerini artırarak, küçük, yaygın, sıradan ve gündelik ihlalleri önemsizleşmektedir. Böylece yasal düzenlemeler gözetimin sıradanlaştırılmasına mahremiyetin değerinin düşmesine yol açmaktadır.

Kişisel verilerin kâğıt üzerinde güçlü korumasının önündeki engeller daha da ayrıntılandırılabileceği gibi, her bir başlık ayrıca ele alınmaya değerdir. Bundan sonrası için kişisel verilerin korunmasında hukukun bahsedilen sınırlarının farkında olunması, küresel bir fenomenin farklı biçimlerde ele alınarak, kamusal menfaatlerin korunmasının özel menfaatler karşısında güçlendiği, kolektif, gerçek ve etkili bir korumanın yolunu açabilecektir.

KAYNAKÇA

"The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR | Autorité de protection des données
Gegevensbeschermingsauto riteit", Şubat 2022. https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr. (E.T. 25.04.2023)

Acquisti, Alessandro, Laura Brandimarte, ve George Loewenstein. "Privacy and Human Behavior in the Age of Information". *Science* 347, sy 6221 (2015): 509-14.

Acquisti, Alessandro, ve Jens Grossklags. "Privacy Attitudes and Privacy Behavior". Içinde *Economics of Information Security*, editör L. Jean Camp ve Stephen Lewis, 165-78. Advances in Information Security. Boston, MA: Springer US, 2004. https://doi.org/10.1007/1-4020-8090-5_13.

Allen, Anita. *Unpopular Privacy: What Must We Hide?* Oxford University Press, 2011. https://doi.org/10.1093/acprof:oso/9780195141375.001.0001.

Andrew, Jane, ve Max Baker. "The General Data Protection Regulation in the Age of Surveillance Capitalism". *Journal of Business Ethics* 168, sy 3 (2021): 565-78. https://doi.org/10.1007/s10551-019-04239-z.

Aydın, Mustafa Berkay. "Dijital Sosyoloji Üzerine Notlar". İçinde *Dijital Sosyoloji Çalışmaları*, editör Aslıhan Zinderen, 1-18. Ankara: Nobel Bilimsel Eserler, 2021.

Barth, Susanne, ve Menno D. T. de Jong. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review". *Telematics*

and Informatics 34, sy 7 (2017): 1038-58. https://doi.org/10.1016/j.tele.2017.04.013.

Baruh, Lemi, ve Mihaela Popescu. "Big data analytics and the limits of privacy self-management". *New Media & Society* 19, sy 4 (2017): 579-96.

Bellaby, Ross W. "Going Dark: Anonymising Technology in Cyberspace". *Ethics and Information Technology* 20 (2018): 189-204.

Benjamin, Garfield. "Privacy Norms and Resistances Between the Performative, the Habitual and the Periperformative". *Social Epistemology Review and Reply Collective* 11, sy 1 (2022): 7-13.

Birch, Kean, D Cochrane, ve Callum Ward. "Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech". *Big Data & Society* 8, sy 1 (16 Mayıs 2021): 1-15. https://doi.org/10.1177/20539517211017308.

Bygrave, Lee. "Privacy Protection in a Global Context- A Comparative Overview." *Scandinavian Studies in Law*, 2004, 319-48.

Cate, Fred H. "The Changing Face of Privacy Protection in the European Union and the United States". *Indiana Law Review* 33, sy 1 (1999): 173-232.

Christl, Wolfie. "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions". Vienna: Cracked Labs, 2017.

———. "Digital Profiling in the Online Gambling Industry. A report on marketing and risk surveillance by the UK gambling firm Sky Betting and Gaming, TransUnion, Adobe, Google, Facebook, Microsoft and other data companies". Vienna-Essex: Cracked Labs- CleanUp Gambling, 2022.

Cofone, Ignacio. "Nothing to Hide, but Something to Lose". *University of Toronto Law Journal* 70 (2019): 1-41.

Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, NY: Oxford University Press, 2019.

———**.** "The Regulatory State in the Information Age". *Theoretical Inquiries in Law* 17, sy 2 (27 Temmuz 2016). https://www7.tau.ac.il/ojs/index.php/til/article/view/1425.

———**.** "What Privacy is for". *Harvard Law Review* 126, sy 7 (2013): 1904-33.

Courmont, Antonie. "Le plaignant type ? Un homme, diplômé et cadre | LINC". linc.cnil.fr, Şubat 2023. https://linc.cnil.fr/fr/le-plaignant-type-un-homme-diplome-et-cadre. (E.T. 28.04.2023)

De Hert, Paul, ve Auke Willems. "Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters?" İçinde *Enforcing privacy: lessons from current implementations and perspectives for the future*, editör Paul De Hert, Dariusz Kloza, ve Pawel Makowski, 49-76. Wydawnictwo Sejmowe, 2015.

Deakin, Simon, David Gindis, Geoffrey Hodgson, Kainan Huang, ve Katharina Pistor. "Legal Institutionalism: Capitalism and the Constitutive Role of Law". *Journal of Comparative Economics* 45 (2015): 188.

Etzioni, Amitai. *Privacy in a Cyber Age*. New York: Palgrave Macmillan, 2015.

Ford, Richard T. "Law's Territory (A History of Jurisdiction)". *Stanford Law School* 97 (1999): 843-930.

Franz, Anjuli, ve Alexander Benlian. "Exploring Interdependent Privacy – Empirical Insights into Users' Protection of Others' Privacy on Online Platforms". *Electronic Markets* 32, sy 4 (01 Aralık 2022): 2293-2309. https://doi.org/10.1007/s12525-022-00566-8.

Friedland, Steven I. "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy". *West Virginia Law Review* 119, sy 3 (2017): 891-914.

Fuchs, Christian. "Towards an alternative concept of privacy". *Journal of Information, Communication and Ethics in Society* 9, sy 4 (01 Ocak 2011): 220-37. https://doi.org/10.1108/14779961111191039.

Hanff, Alexander. "The problem with Consent Management Platforms is they are unlawful by design". *linkedin.com* (blog), Aralık 2021. https://www.linkedin.com/pulse/problem-consent-management-platforms-unlawful-design-alexander/. (E.T. 05.05.2023).

Hartzog, Woodrow. "Facial Recognition Is the Perfect Tool for Oppression". *Medium* (blog), 02 Ağustos 2018. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66. (E.T. 04.05.2023).

Hartzog, Woodrow, ve Neil Richards. "Privacy's Constitutional Moment and the Limits of Data Protection". *Boston College Law Review* 61, sy 5 (2020): 1687-1762.

Hartzog, Woodrow, Evan Selinger, ve Johanna Gunawan. "Privacy Nicks: How the Law Normalizes Surveillance". *Washington University Law Review* 101 (2023): 1-77.

Hatıpoğlu Aydın, Duygu. *Siber Alan ve Hukuk*. İstanbul: On İki Levha Yayıncılık, 2022.

Humerick, Matthew. "The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?" *Catholic University Journal of Law and Technology* 27, sy 1 (2018): 77-125.

Işıktaç, Yasemin, ve Sevtap Metin. *Hukuk Metodolojisi*. İstanbul: Filiz Kitabevi, 2019.

Kohl, Uta. "Jurisdiction in Network Society". İçinde *Research Handbook on International Law and Cyberspace*, editör Nicholas Tsagourias ve Russell Buchan, 69-96. UK: Edward Elgar Publishing Limited, 2021.

Kokolakis, Spyros. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon". *Computers & Security* 64 (2017): 122-34.

Kröger, Jacob Leon, Milagros Miceli, ve Florian Müller. "How Data Can Be Used Against People: A Classification of Personal Data Misuses". SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 30 Aralık 2021. https://doi.org/10.2139/ssrn.3887097.

Leith, Philip. "The socio-legal context of privacy". *International Journal of Law in Context* 2, sy 2 (2006): 105-36.

Lessig, Lawrence. "Code Is Law". Harvard Magazine, 01 Ocak 2000. https://www.harvardmagazine.com/2000/01/code-is-law-html. (E.T. 06.03.2023).

———**.** "The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation". *CommLaw Conspectus: Journal of Communications Law and Technology Policy (1993-2015)* 5, sy 2 (1997): 181-92.

Lyon, David. *Elektronik Göz: Gözetim Toplumunun Yükselişi*. Çeviren Dilek Hattatoğlu. İstanbul: Sarmal Yayınevi, 1997.

———. *Gözetlenen Toplum- Günlük Hayatı Kontrol Etmek*. Çeviren Gözde Soykan. İstanbul: Kalkedon Yayınları, 2006.

———. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique". *Big Data & Society* 1, sy 2 (01 Temmuz 2014): 2053951714541861. https://doi.org/10.1177/2053951714541861.

Mann, Monique, ve Tobias Matzner. "Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination". *Big Data & Society* 6, sy 2 (01 Temmuz 2019): 2053951719895805. https://doi.org/10.1177/2053951719895805.

Matte, Celestin, Nataliia Bielova, ve Cristiana Santos. "Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework". İçinde *2020 IEEE Symposium on Security and Privacy (SP)*, 791-809, 2020.

McGillivray, Kevin, ed. "Data Privacy and Data Protection Issues in Cloud Computing". İçinde *Government Cloud Procurement: Contracts, Data Protection, and the Quest for Compliance*, 91-156. Cambridge: Cambridge University Press, 2021. https://doi.org/10.1017/9781108942485.006.

Orito, Yohko, ve Kiyoshi Murata. "Privacy Protection in Japan: Cultural Influence on the Universal Value". Linköping University, Sweden, 2005. https://rcvest.southernct.edu/ethicomp2005-linkaping-sweden/.

Pagallo, Ugo. "The Legal Challenges of Big Data": *European Data Protection Law Review* 3, sy 1 (2017): 36-46. https://doi.org/10.21552/edpl/2017/1/7.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Reprint edition. Cambridge, Massachusetts London, England: Harvard University Press, 2016.

Politou, Eugenia, Efthimios Alepis, Maria Virvou, ve Constantinos Patsakis. "Privacy and Personal Data Protection". Içinde *Privacy and Data Protection Challenges in the Distributed Era*, editör Eugenia Politou, Efthimios Alepis, Maria Virvou, ve Constantinos Patsakis, 7-12. Learning and Analytics in Intelligent Systems. Cham: Springer International Publishing, 2022.

Popescul, Daniela, ve Laura-Diana Genete. "Data Security in Smart Cities: Challenges and Solutions". *Informatica Economică* 20, sy 1 (2016): 29-38.

Reidenberg, Joel. "Technology and Internet Jurisdiction". *University of Pennsylvania Law Review* 153 (2005): 1951-74.

Richards, Neil M. "Four Privacy Myth". İçinde *A World Without Privacy: What Law Can and Should Do?*, editör Austin Sarat, 33-82. Cambridge; New York: Cambridge University Press, 2015.

Rubinstein, Ariel. "'Economics and Psychology'? The Case of Hyperbolic Discounting*". *International Economic Review* 44, sy 4 (2003): 1207-16.

Satariano, Adam. "ChatGPT Is Banned in Italy Over Privacy Concerns". *The New York Times*, 31 Mart 2023, blm. Technology. https://www.nytimes.com/2023/03/31/technology/chatgpt-italy-ban.html. (E.T. 29.04.2023).

Schaub, Florian, Rebecca Balebako, Adam L. Durity, ve Lorrie Faith Cranor. "A Design Space for Effective Privacy Notices". İçinde *The Cambridge Handbook of Consumer Privacy*, editör Evan Selinger, Jules Polonetsky, ve Omer Tene, 365-93. Cambridge Law Handbo-

oks. Cambridge: Cambridge University Press, 2018. https://doi.org/10.1017/9781316831960.021.

Skatova, Anya, Rebecca McDonald, Sinong Ma, ve Carsten Maple. "Unpacking privacy: Valuation of personal data protection". *PloS one* 18 (03 Mayıs 2023): 1-21. https://doi.org/10.1371/journal.pone.0284581.

Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". *San Diego Law Review* 44 (2007): 745-72.

———**.** *Nothing to Hide: The False Tradeoff between Privacy and Security*. Illustrated edition. New Haven London: Yale University Press, 2013.

———**.** "Privacy Self-Management and the Consent Dilemma". *Harvard Law Review* 126 (2013): 1880-1904.

———**.** "The Limitations of Privacy Rights". *Notre Dame Law Review* 98, sy 3 (2023): 975-1036.

Svantesson, Dan Jerker B. "Are we Stuck in an Era of Jurisdictional Hyper-regulation". İçinde *50 Years of Law and IT*, editör Peter Wahlgren, 143-58. Scandinavian Studies in Law. Stockholm Institute for Scandinavian Law, 2018.

———**.** *Solving the Internet Jurisdiction Puzzle*. Oxford; New York: Oxford University Press, 2017.

Turgut Bilgiç, Ezgi. "Kamusal Alanda İdarenin Video Gözetiminin Kişisel Verilerin Korunması Hukuku Bağlamında Değerlendirilmesi". Yüksek Lisans, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2023.

Van Dijk, Jan. *Ağ Toplumu*. İstanbul: Kafka Yayınları, 2018.

Waldman, Ari Ezra. "How Big Tech Turns Privacy Laws Into Privacy Theater". *Slate,* 02 Aralık 2021. https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html. (E.T. 05.04.2023).

———**.** *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge: Cambridge University Press, 2021.

———. "Privacy, Practice, and Performance". SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 01 Şubat 2021. https://doi.org/10.2139/ssrn.3784667.

Ward, Alexis. "The Oldest Trick in the Facebook: Would the General Data Protection Regulation Have Stopped the Cambridge Analytica Scandal?" *Trinity College Law Review* 25 (2022): 221-42.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.