# GÖZETİM VE MAHREMİYET TOPLUMU

***Av. Baturalp YAVUZ****

**ÖZET**

Gözetim ve mahremiyetinin toplumsal ve hukuksal zeminin incelendiği bu çalışmada öncelikle "Gözetim Toplumu" ve "Mahremiyet Toplumu" kavramları üzerinde durulmuştur. Bu kavramların teorik incelemesinin ardından ise toplumsal anlamda yarattığı sorunsalın üzerinde durulmuştur. Konunun hukuksal çerçevesinin çizildiği ikinci başlıkta; Anayasal, Kişisel Verilerin Korunması Kanunu, diğer kanunlar ve uluslararası düzlemde gerekli inceleme yapılmıştır. Ayrıca kişisel verilerin korunmasına yönelik oluşturulan kurum da kurumsal bir çerçevede dile getirilmiştir. Son olarak ise ilgili inceleme içtihat zemininde mercek altına alınmış ve Anayasa Mahkemesi, Yargıtay ve Avrupa İnsan Hakları Mahkemesi kararlarından birkaç örnek ile somutlaştırılmıştır.

**Anahtar Kelimeler:** Gözetim, Mahremiyet, Kişisel Verilerin Korunması, Kanun, İçtihat.

# SURVEILLANCE AND PRIVACY SOCIETY

**ABSTRACT**

When the social and legal grounds of surveillance and privacy are examined, this learning primarily focuses on the concepts of "Surveillance Society" and "Privacy Society". After the theoretical examination of these concepts, the problematic they create in the social sense is emphasized. In the second heading in which the legal framework of the subject is drawn; Constitutional, Personal Data Protection, other laws and necessary scrutiny at the international level. In addition, the institution regarding the documents for personal use has been expressed in an institutional framework. Finally, the relevant review has been scrutinized on the basis of case law and has been concretized with a few examples from the Constitutional Court, the Court of Cassation and the European Court of Human Rights.

**Keywords:** Surveillance, Privacy, Protection Of Personal Data, Law, Case Law

* İstanbul Barosu, T.C. İstanbul Aydın Üniversitesi Kamu Hukuku Yüksek Lisans Programı, baturalpyavuz@stu.aydin.edu.tr, ORCID ID: 0000-0001-8711-2547.

## I. GİRİŞ

Küreselleşmeyle başlayan süreçte modern toplumların ortaya çıkması, 21. yüzyıla gelirken internet kullanımı başta olmak üzere bilgi ve teknoloji alanında yaşanan gelişmeler toplumsal anlamda çok farklı kavramların tartışılmasına sebep olmuştur. Özellikle dijitalleşmeyle birlikte insanların birbirlerinden ve dünya üzerindeki gelişmelerden daha hızlı haber almaları zaman ve mekan algısının yıkılmasına, toplumların hem kendi içlerinde hem de kendi aralarında daha fazla yakınlaşmasına sebep olmuştur.

Dijitalleşmenin ortaya çıkardığı en önemli zemin ise, insanların sosyal medya mecraları başta olmak üzere, inovasyon temelli kurulan dijital platformlar aracılığıyla birçok alanda kendi hayatlarıyla alakalı bilgi ve verileri paylaşabilmesi veya başka kişiler hakkında bilgi ve verileri kullanabilmesi olmuştur. Bu durum toplumun her üyesinin dokunulmaz kılınmış haklarını korumakla yükümlü olan devlet aygıtının da birtakım düzenlemeler yapmasına yol açmıştır.

İnternet başta olmak üzere iletişim ve medya teknolojilerindeki gelişmelerle yayılan ve derinleşen dijitalleşmenin yarattığı ortamda toplumun ve onun üyelerinin kişisel bilgilerini korumak noktasında en büyük görev ve sorumluluk da devlete düşmektedir. Bu da kendini devlet aygıtının şiddet tekelinden ziyade onun elinde bulundurduğu daha üstün güç olan hukuk çerçevesinde ortaya çıkmaktadır. Öyle ki devletler egemen birer güç olarak hem idarelerindeki toplumların bu haklarını korurken hem de bu korumanın tam olarak sağlanması için aynı toplumu meydana getiren üyelerin yani vatandaşların kişisel verilerine ulaşma, bu verileri saklama noktasında kendi yetki sınırlarını belirlemiştir. Dolayısıyla bu durum ortaya devletin sorumluluğu ve yetkisi noktasında iki kavramın tartışılmasını ortaya çıkarmıştır.

Özellikle vurgulamak gerekir ki hukuki ve demokratik bir anlayışla yönetilen her devletin egemenlik sınırları içinde yaşayan vatandaşlarının Anayasa ve kanunla belirlenmiş bilgi ve verilerine ulaşma hakkı vardır. Bu en başta devlet işleyişinin sağlanması, kamu düzeninin korunması ve toplum güvenliğinin sağlanması için gereklidir. Söz konusu durumun ortaya çıkardığı kavram ise bu noktada devletin vatandaşlarını kanunlar çerçevesinde gözetleyebilmesi olarak karşımıza çıkmaktadır. Dolayısıyla ilk olarak tartışılması gereken kavram "gözetim" kavramıdır. Devletin kanunlar çerçevesinde olsa da vatandaşları üzerinde gözetim yetkilerinin olması ve ek olarak daha önce bahsedilen teknolojik gelişmeler sonucu toplumun da kendi içinde birçok zeminde bilgi ve verileri paylaşabilmesi bu gözetimin sınırlarının ne olacağı noktasında bir tartışmayı da beraberinde getirmektedir. Zira bu her ne

kadar kanunlarla düzenlense de sınırlamaların nedeni hem uluslararası hem de ulus içi hukuk sistemlerinde çokça atıf yapılan "mahremiyet" kavramında kendini belli etmektedir.

Bakıldığında "gözetim" ve "mahremiyet" kavramlarının bir arada düşünülmesi, bu kavramlar arasında bir sorunsal yaratırken, söz konusu sorunsalın çözüm merkezi yine hukuk ve hukuki zeminde yapılan düzenlemeler, alınan kararlar olmaktadır. Bu kapsamda mercek altına alınması gereken şey gözetim ve mahremiyet kavramlarının açıklanması ve bu kavramların yarattığı sorunsal noktasında yapılan en önemli düzenlemelerden biri olan Kişisel Verilerin Korunması Kanunu başta olmak üzere diğer düzenlemelerin belirtilmesi ve son olarak içtihat çerçevesinin incelenmesi değerli olacaktır.

## II. KAVRAMSAL ÇERÇEVE

### A. GÖZETİM TOPLUMU

Modernitenin ana unsurlarından sayılan gözetimin

[1] iki temel özelliğinden ilki, toplumsal yani katı olanın artık çabucak çözünmesi ve gözetimin artık elastikiyetinin artmasıdır[2]. Staples'a göre, bu durum ana unsuru kültürel açıdan parçalanma ve belirsizliğe yatkın olanlarda yaşanmaktadır[3]. Bilginin güç olduğu hatta bilginin egemenliğinin iktidarın egemenliği sayıldığı[4] günümüz toplumlarında ise Sanayi Devrimi sayesinde iktidar ve bilgi ilişkisi artmıştır. Buradan hareketle, bireyler hakkında bilgi de değer kazanmış ve bu da gözetimi önemli bir unsur hâline getirmiştir. Gözetimin bir mesele hâline gelişi salt gelişen teknoloji ve dijitalleşme ile ilgili olmasa da, zaman içinde bu unsurların insan yaşamının önemli bir parçası olması üzerine sınırlarını genişletmesiyle mümkün olmuştur. Böylece, devlet ve toplumun hudutları belirginliğini yitirmiştir. Her ne kadar bireyler şahsi tercihleri sonucu yaşamlarını herkesin görebileceği bir şekilde paylaşıma sunsa da, bu tercih dijital alanı bütünleştirici bir yan etkisi de vardır. Bu meselenin çekirdeğini oluşturan ise, insanlık tarihinin birikimleriyle olgunlaşmış içinde bulunduğumuz çağın medeniyeti ile bebeklik çağını yaşayan dijital bir medeniyetin girift uzlaşmazlığıdır. Söz konusu uzlaşmazlık hâlinin meydana gelişi de bu yeni haberleşme teknolojilerine bireyler tarafından gösterilen uyumun yetersiz kalması sebebiyledir. Zira dijitalleşme birtakım değerlerden feragat etmeyi gerektirmektedir. Özellikle mahremiyet olgusunun dijital alana taşınması lazım gelmektedir.

[1] **Lyon, David/ Bauman, Zygmunt**: Akışkan Gözetim, Ayrıntı Yayınları, İstanbul, 2013, s.13.
[2] A.g.e.
[3] **Staples, William G**: Everyday Surveillance: Vigilance and Visibility in Postmodern Life, Second Edition, 2008, s.9
[4] **Foucault, Michel:** Deliliğin Tarihi, İmge Yayınları, Ankara, 1995, s.58.

Haberleşmenin sanal dünyaya aktarılarak değerler bakımından revize edilmesi, birey düzeyinde toplumlar için bir temel ihtiyaç hâlini alan dijital teknoloji ve sosyal medyanın gözetleme ve mahremiyet sorunsalına hız vermesiyle zaruri hâle gelmiştir. Her geçen gün artan dijitalleşme gözetleme teknolojileri, hukuki reformlar aracılığıyla devletleri bu doğrultuda eylem almaya zorlamaktadır. Zira tüm önlemleri teknolojik haberleşme sağlayıcı firmaların insafına bırakmak da pek rasyonel bir seçim gibi görünmemektedir. Firmaların gözetim toplumunun oluşmasındaki rolü, günbegün ortaya çıkan skandal niteliğindeki haberlerle de anlaşılacağı üzere kilit önemdedir. Gözetleme ve mahremiyet denildiğinde belki de ilk akla gelen İngiliz toplum kuramcısı Jeremy Bentham'ın panoptikon modeli[5], firmalar ve bireyler arasındaki gözetleme ve mahremiyet sorunsalının fiziki bir aynası gibidir. Elbette bu halkanın öteki ayağını da bu yöndeki çalışmalarıyla Foucault'nun[6] bağdaştırdığı üzere devlet ve otorite oluşturmaktadır. Yazılım açıklarıyla ortaya çıkan kişisel verilerin güvenliksizleşmesi ve teknoloji firmalarının kendilerine emanet edilen kişisel verileri kullanma yönünde inisiyatif ortaya koymasının yanı sıra; devletlerin özellikle 11 Eylül terör saldırıları sonrası ulusal güvenlik gerekçesiyle kişisel verileri kendi içlerinde kullanması ve birbirleriyle paylaşması gibi sonuçların doğmasıyla uluslararası toplum iki taraflı kıskaçlar arasında sıkışarak bir gözetim toplumu dönüşmüştür. Dolayısıyla günümüz koşullarındaki bu dönüşüm tek başına dijital haberleşmenin suçu olmamakla beraber onsuz da gerçekleşmesi olasılık dâhilinde değildir.

Gözetim toplumu olmanın bir sebebi de bireylerin sanal dünyada bıraktıkları izlerin tam olarak nerede olduklarını bilememesinden kaynaklanır. Yani gözetim hangi konumda ve ne şekilde yaşanmakta sorusu cevapsızdır. Dolayısıyla bilgi eksikliği ve erişimin sınırlılığı gözetimi daha da kolaylaştıran bir unsur hâline gelir. Otorite bu zafiyetten yararlanarak denetleme mekanizmasını hayata geçirir. Kişisel verilerin otorite gücünden kaynaklanan meşruiyet ve güven zemini üzerinde elde edilmesi ve arşivlenmesi ile de bir araç hâlini alır. Haberleşme teknolojilerini üreten şirketlerin de zaman içinde meşruiyet kazanması bireylerin kişisel verilerini paylaşırken sorgulama safhasını atlamasıyla sonuçlanır. Bu sayede, devamlı gözetleme altında olarak gözetim toplumu durumuna geçiş gerçekleşir. Yeni kamusal yaşamın meşru bir parçası hâline gelen bu haberleşme teknolojisi, sosyal medyanın da yaygınlaşmasıyla teşhir unsurunu hem bilinçli hem bilinçsiz şekilde denkleme sokar. Gözetim toplumu bu hâliyle çok sayıda gözetim alanını da meydana getirir. Herkes kameralar aracılığıyla gözetlenip kontrol altında tutulabilirdir. Bir tehdit unsuru hâline gelişi de bu sayede mümkün olur. Zira, firmalar

[5] **Bentham, Jeremy:** The Panopticon Writings, edited by Miran Bozovic, Radikal Thinkers, 1995, s. 11-12.
[6] **Lyon/Bauman**: s.16.

dijital ayak izinizi takip ederek yapay zeka teknolojisinin yardımıyla bireylere ürün satışı da yapmaya çalışır; devlet kamera ve kredi kartı hareketlerinden cep telefonu sinyallerinize kadar her şeyi kontrol altında tutarak her adımınızdan haberdar da olur. Kişisel alan ve kamusal alan arasındaki farkın ortadan kalkması da gözetim toplumunda bu şekilde zuhur eder. Bilinçli olarak yaşamını teşhir ettiğini sanırken bireyler, bilinçsizce güvenlik ve mahremiyetlerini tehlikeye atmaktadır. Zira göz önünde bulundurulmayan bir diğer konu güvenliksizleşen dijital iletişimin kişinin hem can hem de mal güvenliğinin ihlal edilebilmesine de ön ayak olunmasıdır. Bu sebepledir ki, günümüzde kimlik ve kredi kartı hırsızlıkları da çok ciddi ve giderek artan suç konularından biri olmaktadır. Dolayısıyla bireylerin sanal dünyaya bağlanmanın getireceği faydalar için fiziksel dünyada değer taşıyan mahremiyet, güvenlik, kişisel veri gibi bilgilerinden kendi tercihleriyle vazgeçmeleri[7] hukuki sonuçlar da doğurmaktadır. Sonuç olarak, ereğinden bağımsız olarak, gözetim mahremiyetin yokluğudur; ihlalidir. Ancak ironik bir biçimde bireyler gözetimsizlik hâlini, görünür olmamaktan duyulan kaygıyla ilişkilendirmektedir. Bauman'ın "iktidara teslimiyet" şeklinde ifade ettiği bu durum, esasında bireylerdeki bilinçsizlik düzeyinin de bir kanıtıdır.

## B. MAHREMİYET HAKKI

Mahremiyete ilişkin literatürde çeşitli tanımlamalarla karşılaşılmaktadır. Örneğin, Westin, bireyin kendi hayatıyla ilgili hangi bilgiyi, ne zaman ve ne kadar başkalarıyla paylaşacağını belirleme hakkına sahip olması olarak tanımlar[8]. Altman ise, bireyin kendisine veya grubuna ulaşma çabası üzerindeki seçici kontrolü olarak[9] Bu tanımlardan hareketle, mahremiyet hakkı, kendimize ilişkin bilgileri düzeyi ve zamanı ve miktarı üzerinde mutlak kontrole sahip şekilde seçici olarak paylaşmaya yönelik bir haktır. Fried mahremiyet hakkını sosyal ilişkilerin kurulabilmesi için zaruri kabul eder; zira ona göre, panoptikon benzeri, bir toplumda dostluk, samimiyet ve güven ilişkileri gelişemez ve mahremiyetin yitimi, en esas değerlere yönelik bir tehdittir[10].

## C. GÖZETİM VE MAHREMİYET SORUNSALI

Otoriteler, bireylerin yaşamlarını kontrol mekanizmalarıyla gözetim altında alırken gözetim ve mahremiyet sorunsalı ortaya çıkar. Giddens'a göre, gözetim modern toplumun

[7] **Schmidt, Eric/Cohen, Jared:** Yeni Dijital Çağ, Optimist Yayınları, İstanbul, 2014, s.8.
[8] **Westin, Alan**: "Privacy and Freedom", Washington and Lee Law Review, 1968 25(1), s.166
[9] **Gifford, Robert:** Environmental Psychology (Boston: Allyn and Bucon), 1997, s.173-175.
[10] **Johnson, Deborah G**: Computer Ethics, Prentice-Hall, Inc., 2001, s.121.

kurumsallaşmasının bir unsurudur[11]. Bu kurumsal unsurlardan biri olan gözetim, internet aracılığı ile mahremiyet ihlallerine sebep olmaktadır. Bireylerin toplumsal kontrol ve gözetime karşı koyabilme gücü, mahremiyet ihlâlleri sorunsalını da doğurmaktadır.

Geçmişte toplumu denetleme mekanizmasının bir parçası olan çeşitli gözetim metotları, bilgi teknolojilerinin de yayılmasıyla çağımızın sıradan bir rutini hâline gelmiş ve hepimizi çepeçevre sarmıştır. Bunun sonucu olarak da gözetim, sosyal yaşamda mahremiyet sorunsalının akademik dünyada da ilgisini çekmiş ve konu tartışılmaya başlanmıştır. Örneğin Sartori, bilgi çağının bittiğini ve bireylerin gözetim altına alındığı yeni bir çağın başlangıcını duyurmaktadır. Dolayısıyla günümüzde bebekler dünyaya gözlerini açtıkları andan itibaren gözetleme çağının kapıları onlar için aralanıyor. Bilgi teknolojisiyle çeşitlenen gözetim metotları, mahremiyeti ortadan kaldırıyor ve yaşamı transparan bir görünüme kavuşturuyor. Gözetimin sıradanlaşması, güvenlik gerekçe gösterilerek kişilerin yaşamlarının otorite erkini elinde tutanlarca gözetim altına alınmasıyla sona ermiştir[12]. Mahremiyetin ihlali sorunsalı halkı zaman zaman terörize edecek boyutlara bile ulaşabilir. Bu hâliyle de aynı zamanda güvenliksizlik durumu ortaya çıkabilmektedir. Zira uluslararası toplumun devletlere duydukları güven zaman içinde azalmaktadır. Buna karşılık devletler siber suçlara yönelik hukuki önlemler almayı uygun görmüşlerdir. Örneğin bir güvenlik şirketinin[13] çok yüksek meblağda maliyet açıklaması bu konuya ilgileri çekmiştir. Enformasyon çağı sonsuz bir bağımsızlık teklif ederken mahremiyeti ihlal edip uluslararası toplumda büyük bir hayal kırıklığına da sebebiyet vermiştir.

Gözetim artık bir sosyal kontrol, biyo-politika mekanizması olmuştur ve yaşamımıza önce Orta Çağ'daki salgınlar esnasında "kapatılma" yolu ile girmiştir. Moderniteyle beraber Bentham'ın Panoptikon adı verilen modeli gözetimin fiziki bir görünümünü sergilemekteydi. Nihayetinde gözetim, modern yaşamın adeta tek boynuzlu sosyal kontrol mekanizmasıdır. Yarattığı mahremiyet ihlalleri ile birlikte çok sayıda sorunsalı içinde barındırmakta ve böyle giderse bilgi teknolojileri ve gözetim ile beraber otoriteleri bilgi oburluğuna yönlendirerek, mutlak bir güce dönüştürmeye; mahremiyeti tarumar etmeye ve güvensizlik hissinin toplumsal yaşamın bir parçası hâline gelmesine sebep olacaktır.

[11] **Giddens, Anthony:** "Ulus Devlet ve Şiddet", Kalkedon Yayınları, (Çev. C. Atay) İstanbul, 2008, s.197.
[12] **Dolgun, Uğur**: Enformasyon Toplumundan Gözetim Toplumuna, Ekim Basım Yayın, Bursa, 2006, s.16.
[13] http://www.nortoninternetsecurity.cc/2011/09/norton-study-calculates-cost-of-global.html (Erişim Tarihi: 19.05.2021)

## III. HUKUKSAL ÇERÇEVE

Devletin vatandaşları üzerindeki gözetim ve gözetim sonucu elde ettiği bilgi ve verileri kaydetme yetkisinin, toplumun mahremiyetiyle alakalı bir çerçeveyi ihlal etmeyerek yürütülmesi için hukuki zeminde birçok düzenleme yapılmıştır. Bu düzenlemeler en başta Anayasal düzeyde olmak üzere kanunlar ve uluslararası hukuk alanında kendini göstermektedir. Bu çalışmanın ana omurgası gereği 6698 sayılı Kişisel Verilerin Korunması Kanunu merkez alınacak olsa da diğer hukuki kaynaklarında incelenmesi yerinde olacaktır. Tabii ki de her ne olursa olsun toplumsal gözetim ve mahremiyet ile ilgili en önemli omurga 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur. Dolayısıyla bu çalışmada da söz konusu kavramlarla ilgili yapılacak içtihat incelemesinde merkeze Kişisel Verilerin Korunması Kanunu alınacaktır.

### A. ANAYASAL ZEMİN

Temel kanun olarak da kabul edilecek Türkiye Cumhuriyeti Anayasasında, toplumun gözetim ve mahremiyetiyle ilgili öne çıkan hükümlerin başında kişinin dokunulmazlığı ile maddi ve manevi varlığının vurgulandığı 17. madde gelmektedir. Bu maddeye göre herkesin yaşama hakkının olduğu belirtilirken yine herkesin maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu vurgulanmaktadır. Bu noktada açık bir şekilde kişinin mahremiyeti üzerinde bir düzenleme ortaya konulurken bunun bir hak olduğu vurgulanarak devlete de sorumluluk yüklenmektedir.

Toplumun mahremiyetiyle alakalı en net düzenlemenin yapıldığı Anayasal madde olarak karşımıza çıkan ve özel hayatın gizliliğini öne çıkaran hükümlerin yapıldığı 20. Maddede herkesin özel hayatına saygı gösterilmesi gerektiği, herkesin kendi mahremiyle alakalı bilgi ve verilerin korunmasını talep edebileceği ve isterse aynı bilgi ve verilerin silinmesini isteyebileceği gibi kapsamlar mevcuttur.

Yine Anayasa'nın 22 numaralı maddesine göre herkesin haberleşme özgürlüğüne sahip olduğu ve söz konusu haberleşmenin gizliliğinin esas teşkil ettiği vurgulanmaktadır.

### B. KİŞİSEL VERİLERİN KORUNMASI KANUNU

Kişilere ilişkin bilgilere gereksinim tarihin eski dönemlerinden beri bir ihtiyaç olarak karşımıza çıkmıştır. Günümüzde ise toplumun bir bireyi olarak insanın günlük hayatı dâhil olmak üzere hayatının her alanına dair bilgileri içeren verilerin toplanması önemli bir olgu olmaktadır. Nitekim bu alanda bilgi toplamak için geliştirilen birçok aracın bulunması teknolojinin de gelişimiyle daha da artmıştır. Dolayısıyla kişisel veriye olan gereksinim gelişen

teknolojinin içerisinde daha kolay ulaşılabilir bir ağ mekanizmasını yaratmıştır. Kişisel verilere olan erişimin kolaylaşması bu verilerin ihlal edilme olasılığını da güçlendirmiştir. Öyle ki gözetleme yöntemiyle alınan kişisel bilgilerin üst düzey kişilere ait olması bu verilerin korunmasını gerektirmiştir. Sadece üst düzey kişilere ait değil sıradan insanlara dair verilerin de korunması özel hayatın gizliliği ilkesi kapsamında hukuki bir çerçevede koruma altına alınması zorunluluğunu getirmiştir. Bu alanda yapılan düzenlemeler ilk olarak 1970'li yıllarda Avrupa'da ortaya çıkmış ve zamanla Dünyaya yayılmıştır[14].

Ülkemizdeki kişisel verilerin korunması üzerine olan çalışmalar uluslararası düzene kıyasla daha geç bir dönemde başlamıştır. Herhangi bir kanunun bulunmaması uluslararası antlaşmalarla belirlenen ilkelerin iç hukukumuza aktarmamamıza neden olmuştur[15]. Nihayet 12 Eylül 2010 tarihinde yapılan referandumla kabul edilen 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile kişisel verilerin korunması açıkça anayasal bir güvenceye kavuşmuştur. Anayasanın 20. maddesine eklenen fıkraya göre, *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişi- sel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* Henüz yeni eklenen bu fıkra sınırlı bir düzenleme getirmesi nedeniyle doktrinde eleştirilere maruz kalmıştır. Zira kişisel verilerin korunmasına dair bağımsız bir organın bulunmaması yeterli bir denetim mekanizması yaratmamıştır. Bu konuda bir başka adım 2016 yılında atılmıştır. Avrupa Konseyi bünyesinde 1985 yılında yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[16] ülkemiz tarafından 1981 yılında imzalanmış olmasına rağmen ancak 2016 yılında kabul edilen 6669 Sayılı Kanun ile onaylanmıştır.

Kişisel verilerin korunmasına yönelik özel bir kanunun olmayışı bu alandaki düzenlemelerin en büyük eksikliği olmuştur. 1989 yılında bu konuya özel bir komisyon kurulmuş ancak herhangi bir ilerleme kaydedilememiştir. İkinci komisyon ise 2000 yılında kurulmuş ve üç yıllık bir çalışma sonucu kanun tasarısı hazırlanmıştır. Ancak bu tasarıda da

[14] **Bogdanor, Vemon**: Blackwell'in Siyaset Bilimi Ansiklopedisi, Ümit Yayıncılık, C.II, (Çev. Erhan Yükselci, Sema Yükselci, Bülent Peker), Ankara, 2003, s. 426

[15] **Korkmaz, İbrahim:** "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", TBB Dergisi, 2016 (124), s.81-152.

[16] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Uygun Bulunduğuna Dair Kanun Gerekçesi, https://www2.tbmm.gov.tr/d26/1/1-0320.pdf (Erişim Tarihi: 19.05.2021

ilerleme kaydedilememiş ve kanun hâline getirilememiştir. 2008 yılına geldiğimizde Adalet Bakanlığı önceden yapılmış bu kanun tasarına ek çalışmalar yaparak Başbakanlık'a göndermiştir. Başbakanlık tarafından TBMM Başkanlığı'na gönderilen tasarı bir dizi komisyon arasında dolaşmış en sonunda 2014 yılında TBMM seçimleri nedeniyle yasal bir sonuca ulaşamadan hükümsüz hâle gelmiştir. Tasarı 18 Ocak 2016 tarihinde tekrar TBMM Başkanlığı'na gönderilmiş ve süreç yeniden başlamıştır. En sonunda 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde TBMM'de kabul edilerek kanun olarak kabul edilmiştir. Son kertede kabul edilen kanun ile kişisel verilerin korunması tartışmaya mahal bırakmayacak bir şekilde kanunlaştırılmış ve yasal bir çerçeveye konulmuştur.

## 1. KANUN KAPSAMINDAKİ KAVRAMLAR

Ülkemizde yasalaşması uzun bir sürecin ardından gerçekleşen Kişisel Verilerin Korunması Kanununun temel dayanaklarını 108 sayılı Avrupa Konseyi Sözleşmesi ve 95/46/AT sayılı Avrupa Birliği Yönergesi gibi uluslararası antlaşmalar oluşturmaktadır. Bu nedenle ilgili kanun incelenirken bu uluslararası antlaşmalar önemli bir kaynak oluşturmaktadır. Kanunun amacına baktığımızda daha ilk maddede görmek mümkündür: *"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir"*[17] Temel haklar ve ödevler başlığı altında Anayasamızın 20. maddesi uyarınca düzenlenen özel hayatın gizliliği kapsamında oluşturulan kişisel verilerin korunması hukuk devleti olmanın bir getirisi olarak karşımıza çıkmaktadır. Nitekim temel haklarımızın korunması devletin idare etme gücünün gösterilmesinde oldukça önemli bir yoldur. Bu açıdan bakıldığında kişisel verilerin korunmasına olan ihtiyaç insanın temel hakları çerçevesinde değerlendirilirken diğer bir yandan devletin gücünü de temsil etmektedir.

Kişisel Verilerin Korunması Kanununun 2. maddesi ile düzenlenen kanunun kapsamı kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişilerdir[18]. Dolayısıyla kanunun kapsamı oldukça geniş tutulmuştur. Kanunun uygulanmasında ise kamu veya özel sektör ayrımı yapılmamıştır. Çünkü kişisel veriler sadece kamuya yönelik bir bilgi kaynağı oluşturmaz özel sektörü de kapsayacak kadar geniş bir bilgi akışını kapsamaktadır. Kişisel verilerin nereden başlayıp nereden biteceğinin belirsizliği bir anlamda bütüncül bir

[17] https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/ (Erişim Tarihi: 19.05.2021).
[18] **Korkmaz,** s.81-152.

yaklaşımı getirmektedir. Uluslararası antlaşmaların bir kısmı kişisel verilerin korunmasında sadece gerçek kişileri kapsarken bir kısmı ise gerçek ve tüzel kişiler olmak üzere her ikisini de kapsamaktadır. Türk mevzuatında her ikisini de koruma altına alan bir düzenleme getirilmiştir. Kişisel verilerin korunması sadece kamu organlarına yönelik değil aynı zamanda özel sektöre karşı da geliştirilmiştir. Esas olarak devlete karşı koruma altına alınan kişisel veriler daha kapsamlı bir koruma alanına ihtiyaç duymuştur. Ayrıca kişisel verilerin korunmasının uygulama alanının belirlenmesinde Türk Hukuku, 95/46/AT sayılı Avrupa Birliği Yönergesinin 3. maddesini baz almıştır[19]. Buna göre kişisel veriler tamamen veya kısmen otomatik olarak işlenmesi söz konusu olduğunda bir dosyalama sistemine kaydedilmiş ya da kaydedilecek kişisel verilerin otomatik olmayan yollarla işlenmesi bu kanun hükümlerinin uygulama alanı bulmasını sağlamaktadır.

Kanunun 3. maddesi kişisel verilerin ne olduğuna dair bir açıklık getirmekle birlikte kişisel veri ile ilgili diğer tanımlara yer vermiştir. Kişisel veri, *kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi*[20] ifade etmektedir. Bu maddeye göre, kişiyi tanımlayan her türlü bilgi kişisel veri olarak görülmelidir. Benzer bir şekilde OECD tarafından yayınlanan Kişisel Verilerin Sınır aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri'nde, 108 sayılı Avrupa Konseyi Sözleşmesi'nde ve 95/46/AT sayılı Avrupa Birliği Konseyi ve Avrupa Parlamentosu Yönergesi'nde kişisel verinin tanımı yapılmıştır. Kişisel veri bir kişiye ait bilinebilecek bütün verileri ifade ederken bu bilgiler belli bir kimsenin kimliği etrafında şekillenen etnik kökeni, fiziksel özellikleri, sağlık, eğitim, istihdam durumu, aile hayatı, ikamet adresi, kredi kartı, kişisel düşünce ve inançları gibi kişiyi belirlenebilir hâle getiren doğrudan ya da dolaylı bütün bilgileri içermektedir[21]. Bir başka tanımlama kişisel verilerin işlenmesi üzerine yapılmıştır. Kişisel verilerin uygulama alanını açıklayan tanımlamaya göre, kişisel verilerin işlenmesi; *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"*[22] ifade etmektedir. Bilgilerin edinilmesinden itibaren başlayan sürecin tamamı bu tanımlama altına girmektedir. Açık rıza kavramı ise ilgili kanunun 3. maddesinde tanımlandığı *şekliyle "belirli*

[19] **Solove, Daniel J/Rotenberg, Marc/Schwartz, Paul M**.: Information Privacy Law, İkinci Baskı, Aspen Publishers, New York, 2006, s. 902

[20] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 19.05.2021).

[21] **Wacks, Raymond:** Personal Information Privacy and the Law, Clarendon Press, Oxford 1993, s. 26

[22] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 19.05.2021).

*bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"*[23] olarak karşımıza çıkmaktadır. Bununla birlikte açık rızanın kişisel verilerin korunması üzerindeki etkisi kişilerin kendi iradeleriyle bu verilerin paylaşılıp paylaşılmaması gerektiğiyle ilgili verecekleri karara bağlı olarak değişmektedir. Dolayısıyla açık rızanın bulunması kişisel verilerin işlenmesinin hatta paylaşılmasının ön koşuludur.

Kişisel verilerin açıkça kime ait olduğunun belirlenmesini önleyen kavram kişisel verilerin anonim hâle getirilmesidir. Bu kavramın önemi kişisel verilerin belirlenmesini engellemek amaçlı kullanılan şifreleme yöntemini ifade etmesidir. Kişisel verilerin datalarda saklanmasını sağlayan şey veri kayıt sistemleridir. Bu sistemlerin oluşturulması elektronik ya da elle yazılacak biçimde olabilmektedir. Hangi yöntemin kullanıldığının önemi olmadan kişisel verilerin saklandığı yerler olarak ayırt edebileceğimiz veri kayıt sistemleri bu verilerin korunmasını sağlayan altyapıyı oluştururlar. Dolayısıyla önemi verilerin gizliliğinin sağlanmasından gelmektedir. Kişisel veriler açık rızamıza dayalı ve anonim hâle getirilerek veri kayıt sistemlerine kaydedildiğinde bu işlemi yapacak sorumlulara ihtiyaç olmaktadır. Bu görevi yerine getiren kişiler veri sorumlusu ya da veri işleyen olarak Kanunda açıkça belirtilmiştir. *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi"*[24] ifade etmektedir. Görüldüğü gibi kişisel verilere dair kavramların Kanunda açıklanmış olması bu verilerin güvence altına alınırken açıklık ilkesi gereğince doğru bir şekilde anlaşılmasını sağlamaktadır.

## 2. KİŞİSEL VERİLERİN İŞLENMESİ VE VERİLERE İLİŞKİN DİĞER HÜKÜMLER

Kişisel veriler işlendiği takdirde bu verilerin korunması için çeşitli ilkeler oluşturulması amaçlanmıştır. Bu amaca uygun olarak belirlenen ilkeler Kişisel Verilerin Korunması Kanunu'nun 4. maddesiyle düzenlenmiştir. Kanunda ve diğer kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebilecek kişisel veriler hukuka uygun olmalıdır. Kişisel verilerin işlenmesine yönelik oluşturulmuş ilkeler Kanunda şu şekilde sayılmıştır; "*hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar korunma"*[25]. Kişisel verilerin hukuka uygun olarak işlenmesi verilerin güvence altında olması için önemlidir. Nitekim kanunsuz bir şekilde işlenecek bir veri ihlal olarak görülecektir. Nitekim kullanıcılar açısından da bir güvenlik

[23] A.g.e.
[24] A.g.e.
[25] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 19.05.2021).

endişesi yaratacak olan bu durum, daha sonradan oluşacak herhangi bir hukuki sorunda kişisel verisi bulunan gerçek veya tüzel kişinin zarar görmesine neden olacaktır.

Kişisel veriler, kanuna uygun bir şekilde işlenmek istendiğinde bazı işlenme şartlarını yerine getirilmesi gerekmektedir. İlgili Kanunun 5. maddesi bu şartları belirlemiştir. 1982 Anayasası'nda da belirtildiği üzere kişisel verilerin işlenmesi kişinin açık rızasıyla mümkün olmaktadır. Anayasal bir nitelik olarak da karşımıza çıkan bu husus açık rızaya verilen önemi de göstermektedir. Ayrıca bu açık rızanın şüphe oluşturmayacak şekilde net olması ve herhangi bir zorlamayla belirtilmemiş olması gerekmektedir. Aksi takdirde açık rıza kabul edilebilirliğini kaybetmektedir. Özellikle internetten yapılan alışverişlerde daha çok karşımıza çıkan kişisel verilerin işlenmesine dair sözleşmelere onay verilmesinin açık rıza olarak kabul edilmektedir. Açık rıza hususunda iki kavram dikkat çekmektedir; opt-in ve opt-out. Opt-out kavramı kişinin hayır dememesi üzerinden kabul edilen rızadır. Opt-in ise doğrudan bir seçenek üzerinden onay verilerek rızanın belirtilmesidir. Kural olarak kişisel verilerin işlenmesi yukarıda anlatıldığı gibi olmaktadır. Ancak kişisel verilerin açık rızayla işlenmesinin bazı istisnaları bulunmaktadır. Bunlardan biri Kanunla düzenlenmesi durumunda kişisel veriler açıkça rıza olmadan da işlenebilmektedir. Rızanın açıklanamadığı veya geçerli olmadığı hâllerde kişilerin hayat ve beden bütünlüklerinin korunması için gerekli olduğu takdirde istisnai olarak bu hüküm uygulanır[26]. . Bunun yanı sıra kişinin bir sözleşmeye taraf olması durumunda verilerinin işlenmesine izin verilmesi de mümkün olmaktadır. Kişinin, kişisel verilerini kendi alenileştirmesi durumunda da benzer bir şekilde rıza olmadan verilerin işlenmesi söz konusudur. 95/46/AT sayılı Avrupa Parlamentosu Yönergesinde de bu istisnai hükümler sayılmış ve bir anlamda Kanunun dayanağı olarak görülmüştür.

Kişisel verilerin işlenmesine yönelik olarak Kanunun 6. maddesinin göstermiş olduğu özel nitelikli kişisel verilerin kişinin açık rızası olmadan işlenmesini olanaksız kılmaktadır. Bu özel kişisel veriler şunlardır; *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"*[27]. Özel nitelikli bu kişisel veriler uluslararası antlaşmalarda özel bir koruma altına alınmamıştır. Kanunun getirmiş olduğu bu özel nitelikli kişisel verilerin korunmasındaki ana amaç bu verilere dair bir ihlalin söz konusu olması durumunda bu verilerin kişilere daha fazla zarar verme olasılıklarının bulunmasıdır. Tıpkı kişisel verilerin işlenmesinde olduğu gibi bu

[26] **Korkmaz, s**.81-152.
[27] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 19.05.2021).

maddenin de istisnası bulunmaktadır. Sağlık ve cinsel hayat dışındaki kişisel veriler kanunlarda öngörülen hâllerde ilgili kişinin açık rızası olmaksızın işlenebilecektir. Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenebilmesi ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi gibi kanunda sayılan diğer durumlarda mümkün olmaktadır. Kişisel verilerin korunmasına yönelik yukarıda sayılan maddeler dışında verileri işlenen kişinin hakları 11. maddede düzenlenmiştir. Buna göre, kişisel verileri işlenen kişi kendisiyle kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgileri talep etme, verilerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme gibi kişisel verilerinin akıbetine dair bilgileri talep etme hakkına sahiptir.

Kişisel verilerin hassas bilgiler içermesi ve herhangi bir veri güvenirliliğinin kaybolması durumunda bu eylemden sorumlu kimselere yönelik cezai yaptırımlar Kişisel Verilerin Korunması Kanunu'nun 17. maddesinde sayılmıştır. İlgili maddede işlenen suçlara yönelik 5237 sayılı Türk Ceza Kanunu'nun 138 ila 140 ıncı madde hükümleri uygulanmaktadır. Burada TCK'ya yapılan göndermenin bulunması bu kanunun özel hayatı koruyucu hükümler içermesidir. Nitekim özel hayatın gizliliğinin ihlal edilmesi durumunda TCK hükümleri geçerli olmaktadır. Kişilere Karşı Suçlar ve Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı bölümlerinde bu ihlallerin cezai şartları belirlenmiştir. TCK'da nelerin kişisel veriler olduğu açıkça belirtilmemiştir ancak kişisel verilerin kaydedilmesi suçunu düzenleyen 135. maddenin gerekçesinde suçun konusunun kişisel veri olarak kabul edilmesi gerektiğini belirtmiştir[28]. Kişisel verilerin korunmasına yönelik yapılan düzenlemelere aykırı davranılması durumunda Kanunun 18. maddesinin öngördüğü idari yaptırımlar uygulanmaktadır. İdari para cezasını hükme bağlayan madde veri sorumlusu olan gerçek kişiler ve özel hukuk tüzel kişilerini sorumluluk altında tutmaktadır. Bununla beraber ilgili maddede kabahat olarak görülecek durumlar tek tek sayılmıştır; aydınlatma, veri güvenliğini sağlama, Kurul kararlarını yerine getirme ve Sicile kayıt ve bildirim yükümlülüklerine aykırı davranılması. Son olarak kişisel verilerin korunmasına yönelik istisnalar Kanunda özel olarak düzenlenmiştir. Bu istisnalar Kanun kapsamı dışında tutulan kişisel verileri içermektedir. Buna göre 28. Maddenin ilk fıkrası Kanun kapsamı dışında olan kesin istisnaları belirlemiştir. İkinci fıkrası ise kısmen Kanun kapsamı dışında tutulan istisnai durumları açıklamıştır[29]. Kısmen kapsam dışında tutulan bu hususlar aslında kanun kapsamındadır. Ancak ilgili maddede belirtilen kanun maddeleri bakımından istisna oluşturmaktadırlar.

[28] **Özen, Muharrem/Hafızoğulları Zeki:** Türk Ceza Hukuku Özel Hükümler, Us-A Yayınları, 2010, s. 267, 268.
[29] **Dülger, Murat Volkan:** Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019, s.259.

İncelemiş olduğumuz Kişisel Verileri Koruma Kanunu Türk hukukundaki büyük bir boşluğun doldurulmasını sağlamıştır. Nitekim kişisel verilerin korunması gelişen teknoloji ortamında güvenirliliğin azalmasıyla birlikte zorunlu hâle gelmiştir. Kanunun getirmiş olduğu hükümler ve bağlayıcılığı kişilerin özel bilgilerinin güvenirliliğinde bir güvence oluşturmaktadır.

## C. DİĞER İLGİLİ KANUNLAR

Muhakkak ki toplumun neredeyse tamamını ilgilendiren gözetim ve mahremiyet konusunun sadece Kişisel Verilerin Korunması Kanunu'nda düzenlenmiş olması mümkün değildir. Dolayısıyla Türk Hukuk Sistemi'nde bu kapsamda birçok kanun da düzenlenmiş bulunmaktadır.

Örnek vermek gerekirse 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanununun 34/A maddesinde yapılan düzenlemeye göre askeri personelin kimlik işlemlerinde ve görev sürecinde askeri teşkilat tarafından alınmış bilgilerin korunması vurgulanmaktadır. Yine 1136 sayılı Avukatlık Kanunu'nun 39. maddesine göre avukatların kendilerine müvekkilleri tarafından verilen bilgi ve verilerin bulunduğu dosyaları saklama görev ve hakkı bulunmaktadır. Her türlü devlet ve özel kurumda konaklama, geçici süreliğine kalma veya bakım görme gibi durumlarda kimlik belirtme zorunluluğunun düzenlendiği 1774 sayılı Kimlik Bildirme Kanunu'na göre de bu tür bilgilerin alıcı kurumlar tarafından saklanmasına yönelik hükümlerin bulunduğu hukuksal zemin bu duruma yine örnek gösterilebilir[30].

Devletin gözetim sürecindeki en önemli güçlerinden biri olan polis teşkilatının bu alandaki görevlerinin düzenlendiği 2559 sayılı Polis Vazife ve Selahiyet Kanunu da bu noktada birçok hüküm getirmektedir. Zira kanun kapsamında polis gücünün 1. maddede belirtilen kişiler üzerinde parmak izi ve fotoğraflarının alınmasına izin veren hüküm dışında, bu verilerin mahremiyete saygı çerçevesinde saklanması vurgulanmaktadır. Örnek olarak önleme araması kapsamında hakim veya mülki amirin uygulamaya izin vermemesi gerekirken, polisin de kendiliğinden PVSK m.4/A'ya dayanarak durdurma ve kimlik sorma faaliyetlerini gerçekleştirememesi gerekir. Bu noktada devletin gözetim ve kamu düzeni gibi kavramları yerine getirirken mahremiyet hakkına da saygı duyması gerekmektedir[31].

---

[30] **Altındere, Murat:** Kişisel Verilerin Korunması Hukuku ve Uygulanması, Adalet Yayınevi, Ankara, 2020, s.43

[31] Nitekim kolluğun bireyleri durdurup kimlik sorabilmesi için en azından umma derecesinde bir şüphenin varlığı gereklidir. Yani kişinin aranan veya suç işleyen bir kişi olduğunun kolluk tarafından en azından umma seviyesinde düşündürecek birtakım verilere gerek vardır. Yoksa durdurma ve kimlik sorma yetkisi kolluğa keyfi uygulamalar yapma imkanı vermez. Ceza muhakemesindeki şüphe derecelerini ve durdurma bakımından varolması gereken

Örnek olarak verilen bu kanunlar dışında Türk hukuk sisteminde bulunan gözetim ve mahremiyet toplumuyla alakalı diğer kanunlar ve söz konusu hükümleri şu şekilde sıralanabilir;

- 2920 sayılı Türk Sivil Havacılık Kanunu 40. madde
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu 3. madde
- 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu 2 sayılı ek madde
- 4721 sayılı Türk Medeni Kanunu 23., 24., 25. maddeler
- 4857 sayılı İş Kanunu 75. madde
- 4904 sayılı Türkiye İş Kurumu ile İlgili Bazı Düzenlemeler Hakkında Kanun 21. madde
- 4982 sayılı Bilgi Edinme Hakkı Kanunu 1., 2., 3., 4., 5., 21., 22., 29. maddeler
- 5070 sayılı Elektronik İmza Kanunu 12. madde
- 5237 sayılı Türk Ceza Kanunu 60., 132., 133., 134., 135., 136., 137., 138., 139. ve 140. maddeler
- 5352 sayılı Adli Sicil Kanunu 11. madde
- 5258 sayılı Aile Hekimliği Kanunu 5. Madde
- 5271 sayılı Ceza Muhakemesi Kanunu 80., 137., 209. Maddeler
- 5411 sayılı Bankacılık Kanunu 42., 73., 159. maddeler
- 5429 sayılı Türkiye İstatistik Kanunu 2., 13., 14. madde
- 5429 sayılı Türkiye İstatistik Kanunu 2., 13., 14. madde
- 5490 sayılı Nüfus Hizmetleri Kanunu 3., 9., 43., 44. ve 45. maddeler
- 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu 8., 23., 31. ve 39. madde
- 5502 sayılı Sosyal Güvenlik Kurumu Kanunu 2. ve 35. Madde
- 5510 sayılı Sosyal Sigortalar ve Sağlık Sigortası Kanunu 78. madde
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun 1., 6., 7., 12. ve 19. maddeler
- 6102 sayılı Ticaret Kanunu 24. ve 780. Maddeler
- 6328 sayılı Kamu Denetçiliği Kurumu Kanunu 19. Madde
- 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu 69., 77. ve 99. maddeler
- 6475 sayılı Polis Hizmetleri Kanunu 7., 12. ve 22. Maddeler
- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun 2., 6., 7., 8. ve 10. maddeler

Sıralanan bu kanunlardan hareketle de görülebilir ki devletin veya özel kurumların toplum üzerindeki gözetim yetkisinin ve mahremiyet korumasının Türk hukuk sistemindeki önemi çok açık bir şekilde ortaya çıkmaktadır[32].

şüphe derecesini gösteren sistematik tablo için bkz. Kunter-Yenisey-Nuhoğlu, a.g.e., s.1579; Önleme aramasının yapılabilmesi için ise Adli ve Önleme Aramaları Yönetmeliğinin 20. maddesinde de vurgulandığı üzere, aramaya ilişkin makul sebepler ve tehlikenin varlığını gösteren belirlemelerin bulunması gerekir.

[32] **Turan, Metin:** Kişisel Verilerin Korunması, Seçkin Yayıncılık, İstanbul, 2020, s.56.

## D. ULUSLARARASI HUKUK ÖZELİ

Toplumsal gözetim ve mahremiyetle ilgili iç hukuktaki en önemli hukuksal kaynağının Kişisel Verilerin Korunması Kanunu olduğu düşünüldüğünde, bu düzlemden hareketle uluslararası alandaki yansımanın Avrupa İnsan Hakları Sözleşmesi'ne vurgu yapılması yerinde olacaktır. Avrupa Birliği'nin yaptığı 95/46 sayılı Veri Koruma Direktif ile sağlanan kişisel verilerin korunması hakkındaki zemini resmi bir hukuksal kaynak olarak kabul edilebilir olsa da asıl vurgulanması gereken AİHS'dir. Zira kişisel verilerin korunmasıyla alakalı ilgili sözleşmede doğrudan bir hüküm bulunmasa da metnin 8. maddesi Avrupa İnsan Hakları Mahkemesi başta olmak üzere taraf ülkelerce konuyla ilgili temel altyapı olarak alınmaktadır. Ayrıca belirtmek gerekir ki AİHM kararları, uluslararası çerçevede kişisel verilerin korunmasına yönelik hukuki zemin için oldukça önemlidir. Bu çalışmanın içtihat bölümünde AİHM kararlarına değinileceğinden bu başlık altında AİHS 8. Maddenin etkinliğinin anahtarı, mahkemenin açık dokulu yasallık ve zorunluluk kavramlarına olan yaklaşımında saklıdır[33]. Sözleşmenin 8. Maddesindeki hüküm *"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."* şeklinde düzenlenmiştir. . Her ne kadar söz konusu madde kişinin kendi ve ailesiyle alakalı mahremiyeti düzenleyen bir zemini oluştursa da hükümdeki terimlerden anlaşılacağı üzere kişisel verilerin korunmasına yönelik bir etki ortaya çıkarmaktadır. Zira bu hükümle birlikte devlet aygıtına kişisel verilerin korunması doğrultusunda belirli eylemlerden uzak durması doğrultusunda negatif bir yükümlülük yüklenmektedir. Aynı zamanda yine devlete anayasal bir yükümlülük olarak kişisel verilerin korunmasına yönelik gerekli tedbirlerin alınmasında temel bir insan hakkı olarak sorumluluk yüklenmektedir[34].

Diğer önemli uluslararası düzenlemelere bakıldığında karşımıza ilk olarak İnsan Hakları Evrensel Belgesi gelmektedir. Zira İHEB'nin 12. maddesine göre kimsenin özel yaşamına, aile konutuna ve haberleşmesine keyfi olarak karışılamayacağı belirtilmekte ve herkesin benzer her türlü müdahaleye karşı korunması gerektiği vurgulanmaktadır. Özel hayata ve mahremiyete

[33] **Nardell, Gordon**: "levelling up: Data Privacy and the European Cour of Human Rights'', Data protection in a Profiled World, ed: Serge gutwirth/yves Poullet/Paul De Hert, Heidelberg, Springer, 2010, S.46.
[34] **Dülger**, s.55.

ilişkin olarak kişisel verilerin aktarılması ve işlenmesi noktasında 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında sınırlı olarak sayılmıştır ve yorum yoluyla genişletilemez[35]. Ayrı bir örnek olarak Medeni Siyasal Haklar Sözleşmesi örnek olarak verilebilir. Öyle ki MSHS'nin "Mahremiyet Hakkı" başlıklı 17. maddesinde İHEB'de geçen hükmün iki ayrı fıkrada aynen düzenlendiği görülmektedir.

Hukuksal bir kaynak olarak görülecek bir diğer metin ise Ekonomik Kalkınma ve İşbirliği Örgütü'nün rehber ilkelerinde kişisel verilerin korunmasına yönelik hüküm bulunmaktadır[36].

## IV. KURUMSAL ÇERÇEVE

Kişisel verilerin ve mahremiyetin korunmasına yönelik uluslararası yasal düzenlemelerden biri, Avrupa Konseyi'nin 1995 tarihli 108 sayılı Sözleşmesi ve Avrupa Parlamentosu'nun 95/46/EC sayılı direktifidir. Kişisel Verileri Koruma Kurulu bahsi geçen sözleşme ve direktife uygun olarak kanunla bağımsız bir kurum olarak 30 Ocak 2017 tarihinde kurulmuştur. 6698 sayılı Kanunun 19. maddesine göre Adalet Bakanlığı'na bağlıdır.

Kişisel Verileri Koruma Kurulu dokuz üyeden oluşur. Üyelerin beşi TBMM, ikisi Cumhurbaşkanı, kalan ikisi de Cumhurbaşkanlığı Kabinesi tarafından seçilir. Üye seçiminde, Kurumun görev alanına giren konularda bilgi ve deneyimi bulunanların çoğulcu bir şekilde temsiline özen gösterilir. TBMM beş Kurul üyesini seçerken, seçim için, siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı kadar aday gösterip Kurul üyelerini bu adaylar arasından her siyasi parti grubuna düşen üye sayısı esas alarak TBMM Genel Kurulunca seçer. Ancak, siyasi parti gruplarında, Meclis'te yapılacak seçimlerde kime oy kullanılacağına dair görüşme yapılamaz ve karar alınamaz. Kurul üyelerinin seçimi, adayların belirlenerek ilanından sonra on gün içinde yapılır. Karar yeter sayısı olmak şartıyla seçimde en çok oyu alan boş üyelik sayısı kadar aday seçilmiş olur. Cumhurbaşkanı ve Cumhurbaşkanlığı Kabinesi ise ikişer Kurul üyesini şu şekilde belirler: Cumhurbaşkanı veya Cumhurbaşkanlığı Kabinesi tarafından seçilen üyelerden birinin görev süresinin bitiminden kırk beş gün önce veya herhangi bir sebeple görevin sona ermesi hâlinde durum, on beş gün içinde Kurum tarafından, Cumhurbaşkanlığına bildirilir. Üyelerin görev süresinin dolmasına bir ay kala yeni üye seçimi yapılır. Kurul üyelerinin görev süresi dört yıldır. Süresi biten üye yeniden seçilebilir. Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçer. Kurulun Başkanı, Kurumun da başkanıdır.

[35] **Baysal, Mustafa:** Kişisel Verilerin Korunması Kanunu El Kitabı, Seçkin Yayınları, İstanbul, 2020, s.32.
[36] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Kanun'un 23. maddesinde Kurul'un çalışma esasları düzenlenmiştir. Kurul, başkan dâhil en az altı üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz. Kurulda görüşülen işler tutanağa bağlanır. Kararlar ve varsa karşı oy gerekçeleri karar tarihinden itibaren en geç 15 gün içinde yazılır. Kurul, gerekli gördüğü kararları kamuoyuna duyurur. Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir. Kişisel Verileri Koruma Kurulu'nun başlıca görevleri: özel nitelikli kişisel verilerin işlenmesinde gerekli ve yeterli önlemlerin alınması (m. 6/4); kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri hâlinde, verilerin ilgili ülkeye aktarılabilmesi için izin vermek (m. 9/2-b); kişisel veriler için yeterli korumanın bulunduğu ülkeleri tespit edip ilan etmek (m. 9/3); işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunca yapılan bildirimleri gerektiğinde kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan etmek. (m.12/5); veri sorumlularına yapılan başvuruların reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde kendisine yapılan şikayetleri incelemek (m.14); şikayet üzerine veya resen harekete geçmek suretiyle tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vermek (m. 15/5); benzer ihlallerin yaygın olarak gerçekleştirildiğinin tespit edilmesi hâlinde ilke kararları almak (m. 15/6); telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar vermek (m. 15/7); başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicilinin gözetimini yapmak (m.16/1); gerekmesi durumunda Veri Sorumluları Siciline kayıt zorunluluğuna istisnalar getirmek (m.16/2); kişisel verilerin korunmasına ilişkin öngörülen yükümlülükleri ihlal eden memurlar hakkında disiplin soruşturması yapılması için ilgili kurumlara bildirim yapmak (m. 18/3); kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak (m.22/1-a); kurumun işleyişine, veri güvenliği ile ilgili yükümlülükleri belirlemeye ve veri sorumlusu ile temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlemleri yapmak (m. 22/1-e,f,g); diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek (m.22/1-h).

## V. İÇTİHAT ÇERÇEVESİ

Türk hukuk sisteminde ve uluslararası hukukta bu denli önemli bir yer teşkil eden toplumsal gözetim ve mahremiyet konusunun ilgili hukuk zeminindeki mahkeme kararlarında da öne çıkması beklenmektedir. Bu kapsamda özellikle Kişisel Verilerin Korunması

Kanunu'nun önemi yadsınamaz derecede fazladır. Dolayısıyla içtihada bakıldığında söz konusu kanuna dayanarak verilen kararlar öne çıkmaktadır.

## A. ANAYASA MAHKEMESİ İÇTİHADI

Toplumsal mahremiyet ve gözetimle ilgili ortaya konulmuş Anayasa Mahkemesi kararlarına bakıldığında ilk olarak Biyometrik Yöntemlerle Kimlik Doğrulama Yapılmasını Öngören Kanunla İlgili Danıştay On beşinci Dairesinin yaptığı itiraz başvurusu örnek verilebilir. Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesine, dava konusu kanunun ilgili maddesiyle eklenen hükmün Anayasa'ya aykırılığı iddiasıyla yapılan başvuru Yüce Mahkeme tarafından yerinde kabul edilmiştir. Zira davaya konu olan "... biyometrik yöntemlerle kimlik doğrulamasının yapılması ve …" hükmünün TBMM tarafından temel bir yasayla çerçevesi çizilmeden ortaya konulduğu ve bu durumun Anayasa'nın 2., 13. ve 20. maddelerine aykırı olduğu mahkeme kararında dile getirilmiştir[37].

AYM'nin diğer bir kararı da 5237 numaralı Türk Ceza Kanunu'nun ve 6526 numaralı Kanun'un 4. maddesiyle değişik 136. maddesinin ilk fıkrasının Anayasa'ya aykırılığı üzerine bir dava üzerine verilmiştir. Söz konusu başvuruda Ceza Mevzuatı'nda herhangi bir sınırlama yapılmamasından ötürü dava konusu olan hükmün Anayasa'nın 38. maddesine aykırı olduğu belirtilmiştir. Ancak bu başvuru Yüce Mahkeme tarafından Anayasa'ya aykırı bulunmamıştır. Mahkeme kararının gerekçesinde kişisel verinin sadece kişinin isim, soyadı, doğum tarihi gibi bilgilerle sınırlı olmadığını vurgulamıştır[38].

Mahkeme'nin bir başka kararı da kurumsal e-posta adresine gelen bilgi ve verilerin işverenler tarafından okunmasıyla ilgili bir karardır. İlgili başvuruda işverenlerin bu bilgilere sahip olduğunda işe iade davası zemininde haksız olarak delil elde edebileceği ve bu durumun Anayasa'nın haberleşmenin gizliliğiyle alakalı hükmüne aykırı olduğu vurgulanmıştır. Ancak Yüce Mahkeme ortaya koyduğu kararda başvuruya konu olan uygulamanın, haberleşmenin gizliliğini ilkesine aykırı olduğuna ve başvurucunun iddiasının yerinde olduğuna; ancak Anayasa'nın 20. ve 22. maddelerinde sırasıyla güvenceye kavuşturulan özel hayata saygı ve haberleşmenin gizliliği hakkının ihlal edilmediğine vurgu yapmıştır[39].

[37] Anayasa Mahkemesi, 2014/180 E. 2015/30 K. 19.3.2015 T. 3.4.2015 tarihli 29315 sayılı Resmî Gazete'de yayımlanmıştır.
[38] Anayasa Mahkemesi, 2015/32 E. 2015/102 K. 12.11.2015 T. 02.12.2015 tarihli 29550 sayılı Resmî Gazete'de yayımlanmıştır.
[39] Ö. K. ve O. Ö. Başvurusu, Başvuru No: 2013/4825, Karar Tarihi: 24/03/2016.

## B. YARGITAY İÇTİHADI

Yargıtay içtihadına bakıldığında da yine kişisel verilerle alakalı bir zeminin öne çıktığı görülmektedir. Bu kararlar arasından örnek olarak verilebilecek dava, 2014 yılında alınmıştır. Bilinmektedir ki TCK'nın 136. maddesinin 1. fıkrasına göre bir kişinin bulunduğu makam ve konumun yararıyla, başka birinin kişisel verilerine ulaşması ceza artırıcı bir sebep olmaktadır. Yargıtay On İkinci Ceza Dairesi'nin verdiği söz konusu kararda da "kişisel verinin" kişinin isim, soyadı, telefon numarası gibi bilgileri kapsayan bir kavram olsa da 136. Hüküm nezdinde, herkes tarafından bilinebilecek bu tür bilgilerin maddedeki kişisel veri kavramıyla düşünülemeyeceği belirtilmiştir. Öyle ki bu durumun hukuksal işleyişte sınırları belirsiz bir uygulama ortaya çıkaracağı vurgulanmıştır[40].

Yargıtay'ın verdiği bir diğer karar ise, toplumda çok sık tartışılan; kişisel veri olarak kabul edilen telefon numarasının kişinin rızası dışında paylaşılmasıyla ilgili verdiği karardır. Yargıtay On İkinci Dairesi'nin ilgili kararında bu durumun Anayasa'ya aykırı olduğuna ve başvuruya konu olan dava kararının bozulmasına hükmetmiştir[41].

Yargıtay Dokuzuncu Dairesi'nin aldığı kararda ise özel bir kurumda çalışan bir personelin gizli yazışmalarının bulunduğu bir özlük dosyasının yeni işverene, personelin rızası olmadan aktarılmasının manevi tazminat sebebi sayıldığı vurgulanmıştır. İlgili kararda bunun manevi tazminat talebinin ilgili mahkemelerce reddinin ise hukuken hatalı olduğu belirtilmiştir[42].

Yargıtay On ikinci dairesinin aldığı bir diğer davada ise yine toplumda oldukça fazla tartışılan bir husus ortaya konulmaktadır. Zira Daire'ye getirilen başvuru dosyası üzerinden verilen kararda sosyal medya mecralarında yapılan paylaşımlardan ötürü mağdur olmuş kişinin fotoğraflarının rıza alınmadan paylaşılmaya devam edilmesinin verileri hukuka aykırı şekilde yayma ve bu verileri aynı yöntemle ele geçirme suçu teşkil edeceği belirtilmiştir[43].

## C. AİHM İÇTİHADI

AİHM içtihadıyla alakalı bir inceleme yapıldığında da birçok karar da konuyla ilgili dava bulunmaktadır. Örneğin Leander adlı kişinin İsveç'e karşı açtığı davada AİHM, Leander'in hakkındaki güvenlik soruşturması nedeniyle askeri bir deniz üssü yakınındaki

[40] Yargıtay 12. Ceza Dairesinin 13.01.2014 tarih ve 2013/9043 Esas ve 2014/151 karar sayısı ile verdiği kararı.
[41] Yargıtay 12. Ceza Dairesinin 7.7.2014 tarih ve 2014/607 Esas ve 2014/607 Karar sayısı ile verdiği kararı.
[42] Yargıtay 9. Hukuk Dairesinin 14.04.2016 tarih ve 2014/37215 Esas ve 2016/9418 Karar sayısı ile verdiği kararı.
[43] Yargıtay 12. Ceza Dairesinin 12.04.2017 tarih ve 2015/13582 Esas ve 2017/3109 Karar sayısı ile verdiği kararı.

müzedeki işine son verilmesi üzerine kendisine ilişkin güvenlik kayıtlarına erişmesine izin verilmemesini ve kişisel verilerin ulusal güvenlik gerekçesiyle gizli olarak tutulmasını" özel yaşama müdahale kabul ederek ihlal kararı vermiştir[44].

AİHM'nin başka bir kararı da Birleşik Krallık'a karşı açılan davada verilmiştir. Mahkeme ilgili başvuruda bakımevi kurumunda kalan çocuğun geçmişini merak ederek öğrenmek istemesine karşın, gizli bilgi içerdiği gerekçesiyle istenilen verilerin verilmemesini AİHS'nin 8. maddesine aykırı bulmuştur[45].

Slovakya'ya karşı açılan bir başka kararda ise başvuruyu yapan çiftin, çocuk sahibi olamamalarından ötürü kaldıkları hastanede kısırlaştırıldıklarını öne sürmeleri ve talep ettikleri belgelerin gizli olduğu gerekçesiyle hastane tarafından verilmemesi yine AİHS'nin aynı hükmüne aykırı bulunmuştur[46].

**SONUÇ**

Görülmektedir ki küreselleşme ile başlayan süreçte dijitalleşmenin toplumun her noktasına ulaşması gözetim ve mahremiyet zemininde toplumları etkilerden, toplumların üstünde bir egemen güç olan devlet aygıtının da bu noktada yetkiler ve sorumluluklar almasına, hukuki düzenlemeler yapmasına yol açmıştır.

Söz konusu hukuki düzenlemelerin incelemesi yapıldığında da özellikle Kişisel Verileri Koruma Kanunu'nun özellikle öne çıkan bir etkisinin olduğu görülmektedir. Çalışmada da bunun hukuksal zemini detaylı bir şekilde incelenmiştir. Ancak önemle belirtmek gerekir ki teorik ve hukuksal düzenlemelerde bu konu ne kadar kapsamlı şekilde düzenlenmiş olsa da yaşanan aksaklıkların ve kişisel verilerin korunmasına yönelik toplumda yerleşmiş olan kaygıların gösterdiği şekliyle uygulamadaki durumun çok da olumlu olmadığı ortaya çıkmaktadır. Bu durumda hukukun uygulanması noktasında kamuyu tatmin etmemeye yol açmaktadır.

[44] B. No: 9248/81, T. 26.03.1987, Leander v. İsviçre.
[45] B. No: 10454/83, T. 07.07.1989, Gaskin v. Birleşik Krallık.
[46] B. No: 32881/04, T. 06.11.2009, K.H. ve Diğerleri v. Slovakya, para. 58.

## KAYNAKÇA

**Altındere, Murat**: Kişisel Verilerin Korunması Hukuku ve Uygulanması, 1. Baskı, Adalet Yayınevi, Ankara, 2020.

**Baysal, Mustafa**: Kişisel Verilerin Korunması Kanunu El Kitabı, 2. Baskı, Seçkin Yayınları, İstanbul, 2020.

**Bogdanor:** Blackwell'in Siyaset Bilimi Ansiklopedisi, C.II, Çev. Erhan Yükselci, Sema Yükselci, Bülent Peker, Ankara, Ümit Yayıncılık, 2003, s. 426.

**Dolgun, Uğur**: Enformasyon Toplumundan Gözetim Toplumuna, 1. Baskı, Ekin Basım Yayın, Bursa, 2005.

**Dülger, Murat Volkan:** Kişisel Verilerin Korunması Hukuku, 2. Baskı, Hukuk Akademisi, İstanbul, 2019.

**Hafızoğulları, Zeki / Özen, Muharrem:** Türk Ceza Hukuku Özel Hükümler – Kişilere Karşı Suçlar, 1. Baskı, Us- A Yayıncılık, 2010.

**Korkmaz, İbrahim:** Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBB Dergisi, sayı 124, 2016, ss. 81-152**.**

**Nardell, Gordon:** levelling up: Data Privacy and the European Cour of Human Rights'', Data protection in a Profiled World, ed: Serge gutwirth/yves Poullet/Paul De Hert, Heidelberg, Springer, 2010.

**Solove, Daniel/Rotenberg, Marc /Schwartz, Paul:** Information Privacy Law, 2. Baskı, Aspen Publishers, New York, 2006.

**Turan, Metin:** Kişisel Verilerin Korunması, 3. Baskı, Seçkin Yayıncılık, İstanbul, 2020**.**

**Wacks, Raymond**: Personal Information Privacy and the Law, 1. Baskı, Clarendon Press, Oxford, 1993.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Uygun Bulunduğuna Dair Kanun Gerekçesi, https://www2.tbmm.gov.tr/d26/1/1-0320.pdf (Erişim Tarihi: 19.05.2021).

https://www.kisiselverilerinkorunmasi.org/kanunu-6698-sayili/ (Erişim Tarihi: 19.05.2021).

https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 19.05.2021).

KVKK Rehberi. https://kvkk.gov.tr/Icerik/2030/Rehberler?&page=3 19.05.2021 tarihinde erişilmiştir.

Dolar Annually, http://www.nortoninternetsecurity.cc/2011/09/norton-study-calculates-cost-of-global.html (Erişim Tarihi: 19.05.2021).