SOSYAL BİLİMLER ENSTİTÜSÜ DERGİSİ

Journal of Institute of Social Sciences

Sosyal Bilimler Enstitüsü Dergisi- Journal of Institute of Social Sciences
DOI: https://doi.org/10.54558/jiss.1712551 Araştırma Makalesi/ Research Article

İdarenin Sorumluluğu Çerçevesinde Kişisel Verilerin Korunması: Hukuki ve Etik Boyut

Protection of Personal Data within the Framework of the Administration's Responsibility: Legal and Ethical Dimensions

Murat UZUNPARMAK[1]* İbrahim İRDEM[2]

[1]* Dr., İçişleri Bakanlığı, Mülki İdare Amiri, Ankara, Türkiye.

[2] Doç. Dr., İçişleri Bakanlığı, Emniyet Genel Müdürlüğü, Ankara, Türkiye.

***Sorumlu yazar/ Corresponding author:**
muzunparmak@gmail.com

Başvuru/Submitted: 02.06.2025
Kabul/Accepted: 09.07.2025

Atıf/Cite as:
Uzunparmak, M. & İrdem, İ. (2025). İdarenin sorumluluğu çerçevesinde kişisel verilerin korunması: Hukuki ve etik boyut, *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *16*(2), 494-504.

Öz

Amaç: *Dijitalleşmeyle birlikte kamu hizmetlerinin sunumu sırasında kişisel verilerin toplanması, işlenmesi ve saklanması her geçen gün artmaktadır. Bu durum idarenin kişisel verileri koruma sorumluluğunu derinden etkilemekte ve kritik bir hale getirmektedir. Bu çalışma, idari faaliyetler çerçevesinde idarenin kişisel verilerin korumasına yönelik hukuki ve etik sorumluluğunu tartışmayı amaçlamaktadır.*

Yöntem: *Nitel araştırma yöntemine dayanan çalışmada içerik analizinden ve normatif analiz tekniğinden yararlanılmaktadır. İçerik analizi kapsamında 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verileri Koruma Kurulu kararları, Danıştay ve Anayasa Mahkemesi kararları detaylı bir şekilde incelenmiştir. Bu hukuki metin ve kaynaklardan, idarenin kişisel verilerin korunmasında üzerine düşen sorumluluğu normatif bir çerçevede değerlendirmek için yararlanılmıştır. Normatif analiz kapsamında idarenin özen yükümlülüğüne riayet etme zorunluluğu, yeni teknolojiler karşısında gerekli önlemlerin alınması gerektiği, etik standartlar oluşturularak etik bilincin içselleştirilmesinin önemi vurgulanmıştır.*

Bulgular: *Bilgi iletişim teknolojilerinin ve sunduğu kolaylıkların azami derecede yoğunlaştığı dijital çağ önemli avantajlar sağlamakla birlikte, kişisel ve hassas verilerin giderek daha fazla toplanması ve depolanması, idarenin kişisel verileri koruma yükümlülüğünü kritik hale getirmiştir. İdarenin, idari faaliyetleri çerçevesinde kişisel verilerin korunmasına ilişkin hukuki sorumluluğu kusurlu ve kusursuz sorumluluğa dayanmaktadır. İdare kamu hizmeti sunarken kişisel verileri koruma konusunda hem hukuka hem de etik kaidelere uygun davranmalıdır.*

Sonuç: *Kişisel verileri koruma sorumluluğuna sahip idare özel hayatın gizliliğini ve kişisel hakları güvence altına almak için bu verileri hukuka uygun şekilde toplamak, işlemek ve verilerin güvenliğini sağlamakla yükümlüdür. İdarenin bireysel mahremiyete saygı göstermesi, toplumsal değerleri göz önünde bulundurması ve etik değerlerin idamesinde sorumlu bir tutum sergilemesi elzemdir.*

Özgünlük: *Kişisel verilerin korunması, içinde bulunduğumuz dijital çağda, hem dünyada hem de Türkiye'de en önemli siber güvenlik konularından birisi haline gelmiştir. İdarenin bu alandaki sorumluluğunu hukuk ve etik boyutlarıyla ele almak hem kamu yararı açısından hem de konunun güncel tartışmaların odağına yer alması açısından mevcut literatüre özgün bir katkı sunmaktadır. Disiplinler arası niteliğiyle öne çıkan çalışma, idarenin sorumluluğunu kamu yönetimi ve idare hukuku disiplinleri bağlamında incelemekte, hukuki içtihatlarla teoriyi harmanlamaktadır.*

Anahtar Kelimeler: *Etik, hukuk, idarenin sorumluluğu, kişisel veri, veri güvenliği.*

Abstract

Aim: *The collection, processing and storage of personal data during the provision of public services is increasing day by day with digitalization. This situation deeply affects the responsibility of the administration to protect personal data and makes it critical. This study aims to examine the legal and ethical responsibility of the administration regarding the protection of personal data within the framework of administrative activities.*

Method: *In the article based on qualitative research method, content analysis and normative analysis techniques are employed. Within the scope of content analysis, the Law No. 6698 on the Protection of Personal Data, the decisions of the Personal Data Protection Board, the decisions of the Council of State and the Constitutional Court were examined in detail. These legal texts and sources were used to evaluate the responsibility of the administration in the protection of personal data within a normative framework. Within the scope of normative analysis, the obligation of the administration to comply with the duty of care, the need to take necessary precautions against new technologies, and the importance of internalizing ethical awareness by establishing ethical standards were emphasized.*

Results: *The digital age, where information communication technologies and the conveniences they offer have intensified to the maximum, provides significant advantages, but the increasing collection and storage of personal and sensitive data has made the administration's obligation to protect personal data critical. The administration's legal responsibility for the protection of personal data within the framework of its administrative activities is based on defect and strict liability. While providing public services, the administration must act in accordance with both the law and ethical principles in protecting personal data.*

Conclusion: *The administration responsible for protecting personal data is obliged to collect, process and ensure the security of these data in accordance with the law in order to secure the privacy of private life and personal rights. The administration must respect individual privacy, take social values into account and display a responsible attitude in maintaining ethical values.*

Originality: *The protection of personal data has become one of the most important cybersecurity issues in the digital age we live in, both in the world and in Turkey. Addressing the responsibility of the administration in this area with its legal and ethical dimensions offers an original contribution to the existing literature, both in terms of public interest and in terms of placing the subject at the center of current discussions. The study, which stands out with its interdisciplinary character, examines the responsibility of the administration in the context of public administration and administrative law disciplines and blends theory with legal precedents.*

Key Words: *Ethics, law, responsibility of the administration, personal data, data security.*

Giriş

Bilgi iletişim teknolojilerinin ve dijitalleşmenin ivme kazandığı günümüz post-modern toplumlarında bireylerin ve devletlerin karşı karşıya kaldığı en önemli meselelerden birisi hiç şüphesiz kişisel verilerin korunmasıdır. Bireylerin çevrim içi ve çevrim dışı kimliklerinin özünü oluşturan kişisel veriler bireylerin kimlik bilgilerinden inançlarına, alışkanlıklarından özel hayatlarına, sağlık durumlarından mali kazançlarına kadar çok sayıda bilgiyi içermektedir. Bireylerin haklarını, özgürlüklerini ve meşru menfaatlerini korumakla yükümlü olan devletin yürütme gücünün somut tezahürü olan idare, kişisel verileri koruma yükümlülüğü kapsamında hem hukuki sorumluluklarını yerine getirmeli hem de etik ilkelere riayet etmelidir.

İdare kamu hizmetini yerine getirirken kişisel verilerin korunması kapsamında hem kusurlu sorumluluğa hem de kusursuz sorumluluğa sahiptir. İdarenin kusur sorumluluğu hukuka aykırı eylemlerden, kişisel verilere ilişkin yasal düzenlemelere ve idari yükümlülüklere uyulmamasından, veri güvenliğini sağlamada gerekli özenin gösterilmeyip yetersiz kalınmasından kaynaklanmaktadır. İdarenin kusursuz sorumluluğu ise kamu hizmetinin yürütülmesi sırasında idare, hukuka uygun bir şekilde hareket etse bile, kusuru olmaksızın gerçekleşen faaliyetlerinden ortaya çıkmaktadır. Kusursuz sorumluluk halinde de idare bireylerin uğradığı zararı tazmin ve telafi etmek zorundadır.

İdari mercilerce veri sorumluları tarafından işlenen kişisel veriler hukuka ve meşru amaçlara uygun olmalı, iyi bir şekilde muhafaza edilmeli, veri güvenliğini sağlayacak her türlü teknik ve idari önlemleri içermelidir. Kişisel verilerin korunması konusunda idare tarafından gerekli denetimler yapılmalı ve yaptırılmalıdır. İdare kişisel verileri korurken nasıl hukuka uygun davranıyorsa etik normlara da o derece uygun davranmalıdır. Bireylerin özel hayatına saygı gösterilmeli, veri toplama ve işleme süreçleri bu hakkı ihlal etmeyecek şekilde gerçekleşmelidir. Kişisel verilerin hangi amaçlara dayanarak toplandığı, nasıl işlendiği ve kimlerle paylaşıldığı konusunda şeffaflığa dikkat edilmeli, veri güvenliği konusunda toplumsal farkındalık oluşturulmalıdır. İdare, yapay zekânın içinde bulunduğumuz zaman dilimini ve toplumların geleceğini hızla etkilediği süreçte algoritmaların denetlenebilirliğine yönelik güçlendirilmiş uygulamalara yer vermeli, iyi eğitilmiş veri setleri kullanmalı, ayrımcılık riskini elimine etmek için veriler üzerinde kullanıcıların kontrolünü güçlendirecek mekanizmalar geliştirmelidir.

Bu çalışmada kişisel verilerin korunmasında idarenin sorumluluğu kapsamlı bir şekilde ele alınmakta, yalnızca hukuki boyutla sınırlı kalınmayarak, etik boyuta da yer verilmektedir. İdarenin kamu hizmetlerinin yerine getirilmesi sürecinde kişisel verileri korumaya yönelik faaliyetlerinin hem hukukla hem de etik ilkelerle tam bir uyum içinde yürütülmesi gerektiği vurgulanmaktadır.

Dijitalleşme ve Güvenlik

Bilgi çağı olarak adlandırılan içinde bulunduğumuz 21. yüzyılda etkisini hızlı bir şekilde artıran küreselleşmenin doğrudan etki ettiği alanlardan birisi hiç şüphesiz güvenlik olmuştur. Güvenlik en yalın şekliyle tehditlerden ve risklerden uzak olma durumudur. Kendini güvende hissetme, güvende olmamaya yönelik kaygı ya da endişelerden arınmış olma duygusudur. Güvenlik çalışmalarında kendisine sıkça referans yapılan David Baldwin'e (1997) göre güvenlik edinilmiş değerlere yönelik zarar gelme ihtimalinin düşük olması olarak tanımlamaktadır. Dolayısıyla güvenlik belirli bir nesneye yönelik tehditle karşılaşılmadığı durumda ya da en azından olası olmadığı durumlarda ortaya çıkmaktadır. Küreselleşme ise devletlerin ve toplumların güvenlik açısından çeşitli risk ve tehditlere karşı korunma kabiliyetini zorlaştırmıştır. Bir bakıma küreselleşmeyle güvensizlik de küreselleşir hale gelmiştir.

Küreselleşmenin bilgi ve iletişim teknolojilerinde ortaya çıkardığı yeni gelişmeler devletleri siber güvenlik açısından daha temkinli davranmaya ve politika geliştirmeye teşvik etmektedir. Çünkü teknolojik ilerlemeler toplumların yaşamını kolaylaştırmak ve hayat kalitesini artırmakla beraber devletin ve vatandaşlarının siber saldırılara maruz kalma riskini artırabilmekte, güvenlik açıklarına sebebiyet verebilmektedir (İrdem vd., 2021, s. 35-36).

Küreselleşmenin yansıması olan dijital dönüşüm kişisel verilerin çalınmasından yapay zekâ destekli sahte içeriklerin yayılmasına, biyometrik verilerin kötüye kullanılmasından otomasyon sistemlerinde güvenlik ihlallerine ve bilgisayar korsanları tarafından veya zararlı yazılımlar aracılığıyla bireylere, devlet kurumlarına ve şirketlere yönelik saldırılara kadar pek çok güvenlik sorununu gün yüzüne çıkarmaktadır. Bu nedenle, dijitalleşmeyle beraber siber güvenlik hiç olmadığı kadar önem kazanmıştır. Sistemlerin, ağların, programların dijital saldırılara karşı korunması anlamına gelen siber güvenlik verilere ilişkin tüm kategorilerin korunmasını esas almaktadır. Siber saldırılar genel olarak hassas bilgilere erişmeyi, onları değiştirmeyi ya da yok etmeyi amaçlamaktadır. Özellikle, saldırganların sürekli olarak kendini geliştirerek yeni yöntem ve metotlar tercih etmesi, yeni cihaz ve araçlardan yararlanması siber güvenlik önlemlerini zorlaştırmakla birlikte devletlerin ilgili birimlerini de potansiyel saldırılara karşı koymak, potansiyel tehditleri önceden öngörebilmek ve gerekli önlemleri almak açısından kendisini sürekli geliştirmeye ve her daim saldırganlardan bir adım önde olmaya zorlamaktadır.

Siber güvenlik sorunu ile karşılaşılması devletleri ve ilgili aktörleri telafisi mümkün olmayan sonuçlarla karşı karşıya bırakabilmektedir. Statista (2025) tarafından yapılan siber güvenlik pazarındaki 'Siber Suçun Tahmini Maliyeti' göstergesine göre 2023-2028 yılları arasında siber güvenlik maliyetinin 5,7 trilyon ABD doları kadar sürekli artacağı tahmin edilmekte ve 2028 yılında bu maliyetin 13,82 trilyon ABD dolarına ulaşarak zirveye ulaşacağı tahmin edilmektedir. Bununla birlikte siber korsanlar tarafından geliştirilen çeşitli kurum ve kuruluşlara, bankalara, şirketlere yönelik saldırı amaçlı yazılımların başarılı sonuç vermesi ya da vatandaşların kişisel bilgilerini çalmaya yönelen bir girişimin amacına ulaşması kamu güvenliğinden ekonomik istikrara kadar her şey risk altına sokabilmektedir. Özellikle, kamu hizmetlerinin giderek dijital platformlardan gerçekleşmesi olası siber saldırı riskini artırmakla birlikte, böyle bir durumda kamu hizmetinin görülmesini engellemekle kalmayıp kamu güvenini zedeleme ihtimali de doğurabilmektedir. Üretici yapay zekâ uygulamaları ise yalnızca siber saldırılarla değil, aynı zamanda izinsiz veri madenciliği yoluyla da bireylerin mahremiyetini tehdit etmektedir. Bu bağlamda üretici sistemlerin, internetten elde edilen verilerle eğitilmesi sonucu, anonimleşmemiş özel nitelikli verileri yeniden üretme kapasitesine sahip olduğu ifade edilmektedir (Hickok, 2023, s. 6). Bu nedenle, çeşitlenen siber tehditler karşısında devletlerin önleyici mekanizmalar geliştirmesi elzem haline gelmiştir. Eğitimden sağlığa, ulaşımdan telekomünikasyona, finans sistemlerinden su ve enerji sistemlerine kadar devletin kritik alt yapıları koruma misyonu artarak siber güvenlik özelinde devletlere ayrı bir sorumluluk yüklemiştir.

Siber güvenlik kişisel verilerin korunmasında önemli bir zırhtır. Bu zırhın koruduğu temel değerlerin başında ise 'kişisel veriler' gelmektedir. Nitekim, pek çok siber saldırı kişisel verileri hedef almaktadır. Kimlik bilgilerinden bireylerin kredi kartı ve telefon numarasına, sağlık kayıtlarından banka hesaplarına ve ikametgâh adreslerine kadar bu veriler kazanç temin etmek maksadıyla ele geçirilebilmektedir. Kişisel veriler üzerinden dolandırıcılık, sahtekarlık ve şantaj yapılabilmekte, bireylerin dijital varlıkları siber alanda istismar edilebilmektedir. Bu yüzden, siber güvenliğin etkili bir şekilde temin edilmesi bireylerin dijital dolaşımını güvence altına almakta ve siber uzayda mahremiyetini sağlamaktadır.

Kişisel Verilerin Korunması

Kişisel verilerin korunmasından anlaşılması gereken şey; kişinin veriler üzerinde kontrol sahibi olması, başkalarına emanet edilen verinin onda gizli kalması ve gerektiği durumlarda veri sahibine açıklanması için muhafaza edilmesidir (Gürpınar, 2017, s. 683). Bir kişiye ait özel, iş, ailevi özelliklerini yansıtan, o kişiyi diğerlerinden farklı kılan ve niteliklerini açığa vuran bilgiler kişisel veri olarak kabul edilmektedir (Akkurt, 2020, s. 21).

Türkiye'de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'na (2016) göre kimliği belirli ya da belirlenebilir gerçek kişiye yönelik her türlü bilgi kişisel veridir (KVKK, 2016, Madde 3). Kişisel veri bireye sıkı sıkıya bağlı olup, şahıs varlığı hakkı bağlamında değerlendirilebilir (Oğuz, 2018, s. 121).

Avrupa Birliği'nde (AB) 25 Mayıs 2018 tarihinde uygulanmaya başlanan AB 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (AB Genel Veri Koruma Tüzüğü-GDPR) kişisel verilerin korunması ve gizliliğinin sağlanması açısından önemli bir dönüm noktası olmuştur. AB Genel Veri Koruma Tüzüğü bireylerin kendi kişisel verileri üzerinde daha fazla kontrole sahip olmasını güçlendirmeyi, veri korumaya AB genelinde bütünleşik bir yaklaşım sergilenmesini, veri yasalarının teknolojik gelişmelerle birlikte yeniden gözden geçirilmesini ve kuruluşlara olan güvenin artırılmasını amaçlamaktadır (AB Genel Veri Koruma Tüzüğü-GDPR, 2016). Ayrıca, ülkelerin iç hukukunda yasal uyumun ötesinde kamu ve özel sektör kuruluşlarına etik norm ve değerleri özendirme misyonu gütmektedir (Hijmans ve Raab, 2021, s. 64). Türkiye de AB uyum sürecinin bir parçası olarak veri koruma mevzuatını AB Genel Veri Koruma Tüzüğü ile uyumlu hale getirmeye çalışmaktadır.

Kişisel verilerin özel hayatın gizliliği kapsamında korunması ve üçüncü kişilerin eline geçmemesi için gerekli olan hukuki güvencelerin bulunması önemli bir zorunluluktur. Kişisel veriler 1982 Anayasası'nın 20. Maddesinde koruma altına alınmıştır. Anayasanın "*Özel Hayatın Gizliliği*" başlıklı 20. Maddesine eklenen 3. fıkraya göre herkes; kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir ve bu hak kişinin kendisiyle ilgili veriler hakkında bilgilendirilme, bu verilere erişim sağlama, verilerin düzeltilmesini veya silinmesini talep etme ve belli amaçlar doğrultusunda kullanılıp kullanılmadığını öğrenme gibi unsurları da içermektedir (2709 sayılı Türkiye Cumhuriyeti Anayasası, 1982). Dolayısıyla kişisel verilerin korunması kanuna ve anayasaya dayanan, insan haklarını temel alan, hukuk devleti ilkesini teminat altına alan bir haktır.

Avrupa İnsan Hakları Sözleşmesi (AİHS) ile Avrupa İnsan Hakları Mahkemesi (AİHM) kararları incelendiğinde Türkiye'deki mevzuatla benzer tanımlamalar söz konusudur. Bu kapsamda kimlik bilgileri, bireysel harcamalar, eğitim ve sağlık durumuna ilişkin veriler, güvenlik bürokrasisine yönelik kayıtlar, sosyal medya araçlarındaki bilgiler, resimler ve fotoğraflar ile genel olarak siyasi ve inançsal olmak üzere özel nitelikteki veriler bu çerçevede değerlendirilmektedir (Kutlu ve Kahraman, 2017, s. 46).

Kişisel verilerin korunmasında temel değer; veri sahibinin kendisinden ziyade veri sahibinin kişiliğidir. Bunun sebebi ise özel verilerin ifşa edilmesi, farklı analiz ve yorumlamalara konu edilmesi halinde veri sahibinin maddi ve manevi varlığının koruma ve geliştirme özgürlüğünün kısıtlanmasına yol açması, bedensel bütünlüğünün, sağlığının zarar görebilmesi, kimi zaman ölümle sonuçlanabilmesi, malvarlığı kayıpları ile ciddi zarara uğrama gibi riskler taşımasıdır (Gürpınar, 2017, s. 684).

Kişisel verilerin korunmasında hedef; yalnızca veri işlemeye karşı bir önlem almak değil, aynı zamanda veri korumayla ilgili temel ilkelerle uyuşmayan işlemleri engellemektir (Gürsel, 2016, s. 58). Kişinin rızası olmaksızın bilgilerinin başkalarınca ele geçirilmesi, kullanılması, üçüncü kişilere aktarılması, aleyhine sonuç ve tespitlerde bulunulması kişinin geleceğini belirleme hakkını kısıtlamaktadır (Doğan, 2019, s. 52). Bununla birlikte kişisel verilerin korunması bilgi iletişim teknolojilerinin kullanımının her geçen gün yoğunlaştığı bir süreçte bilginin serbest dolaşımını olumlu yönde etkilemektedir. Bilginin serbest dolaşımının sağlanması bakımından bir sınır belirlemekte, mahremiyetlerinin ihlal edildiği yönünde daha az endişe duyan insanların kişisel verilerini daha çok paylaşma eğiliminde bulunmasına katkı sağlayarak bilginin erişilebilirliğinin ve paylaşımının artmasına neden olmaktadır (Aksoy, 2010, s. 77). Kişisel verilerin korunmasına ilişkin düzenlemelerle hangi verilerin paylaşılacağı ya da bilginin nasıl kullanılacağı konusunda net kuralların belirlenmesi, yani bir başka ifadeyle hukuki çerçevenin çizilmesi, bir yandan kişisel verilerle ilgili mahremiyeti sağlarken öte yandan da verinin güvenli ve kontrol edilebilir şekilde paylaşılmasını beraberinde getirmektedir. Bu kapsamda Anayasa Mahkemesi (AYM), A.N. kararında, kimlik numarası, imza ve adres gibi kişisel bilgilerin sosyal medyada rıza olmaksızın paylaşılmasının, Anayasa'nın 20. maddesi anlamında kişisel verilerin korunmasını isteme hakkını ihlal ettiğine karar vermiştir. Mahkeme, bu tür verilerin ifşasını ifade özgürlüğü kapsamında değerlendiren yaklaşımı anayasal güvencelere aykırı bulmuş ve yeterli özenin gösterilmediğini belirtmiştir (AYM, 2021, B. No: 2018/24439).

Kişisel verilerin hangi amaçla ve nasıl işleneceğini belirleyen, veri kayıt sisteminin oluşturulmasından ve yönetilmesinden sorumlu olan gerçek ya da tüzel kişilere "veri sorumlusu" denir (KVKK, 2016, s. 1). 6698 sayılı KVKK'nın 12. Maddesinde belirtildiği üzere veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilerin hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamakla yükümlüdür. Bu amaçla her türlü teknik ve idari tedbirleri almak zorundadır. Veri sorumlusu veri işleme faaliyetini kendisi gerçekleştireceği gibi teknik yetersizlikler, çalışma alanları kapsamında olmaması veya başka nedenlerden ötürü veri işleme faaliyetini üçüncü bir kişi de gerçekleştirebilir. Veri sorumlusu tarafından verilen yetkiye dayanarak onun adına veri işleme faaliyetinde bulunan üçüncü kişi ise veri işleyendir (Deniz, 2023, s. 99).

Kişisel verilerin işlenmesinde bazı genel ilkeler söz konusudur. Kişisel veriler işlenirken 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; işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uygun olarak hareket edilmelidir (KVKK, 2016, Madde 4/2). Bu genel ilkelerin her biri kişisel verilerin korunmasında eşit derecede öneme sahip olup, bu ilkelere uygun olmayan işlemler hukuka aykırı sayılmaktadır (Yücedağ, 2019, s. 48).

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) 1980 yılında "Özel Hayatın Korunması ve Sınır Ötesi Kişisel Veri Akışına İlişkin Rehber İlkeler" belirlemiştir. Bu ilkeler gerek AB Genel Veri Koruma Tüzüğü gerekse 6698 Sayılı

KVKK gibi modern veri koruma düzenlemelerinin temel taşlarından birisi olmuştur. Kişisel verilerin korunmasıyla ilgili uluslararası standartları beraberinde getirmiştir. Bu ilkeler şu şekildedir (OECD, 1980):

1) Veri toplama sınırlılığı ilkesi: Bu ilkeye göre kişisel verilerin toplanmasında sınırlamalar olmalı, kişisel veriler veri sahibinin izni ve rızasıyla adil ve hukuka uygun şekilde toplanmalıdır. Bu ilkeyle gereksiz veri toplamanın önüne geçilmesi amaçlanmaktadır.

2) Veri Kalitesi İlkesi: Kişisel veriler kullanılacak amaçla uyumlu olmalı, gerekli olduğu ölçüde doğru, eksiksiz ve güncel bir şekilde tutulmalıdır.

3) Amaç Belirleme İlkesi: Kişisel verilerin hangi amaçla toplandığı, toplanmadan önce veya en geç veri toplama sırasında belirtilmelidir. Kişisel veriler ilk toplanma amacı dışında başka bir amaçla kullanılmamalıdır.

4) Kullanım Sınırlaması İlkesi: Kişisel veriler ilgili kişinin rızası olmadan veya yasal bir zorunluluk bulunmadan üçüncü kişilere açıklanmamalı ya da kullanıma sunulmamalıdır.

5) Güvenlik Önlemleri İlkesi: Kişisel veriler kaybolma, yetkisiz erişim, yok edilme kullanılma, değiştirilme ya da veri ifşası gibi risklere karşı makul güvenlik önlemleriyle korunmalıdır.

6) Açıklık İlkesi: Kişisel verilerle ilgili gelişmeler, uygulamalar ve politikalar konusunda genel bir şeffaflık politikası benimsenmelidir. Kişisel verilerin varlığı, niteliği, kullanım amaçları, veri sorumlusunun kimliği ve yerleşim yeri gibi hususlara ilişkin bilgiler bireyler için anlaşılır ve kolayca erişilebilir olmalıdır.

7) Bireysel Katılım İlkesi: Kişisel veri sahipleri veri sorumlusuna başvuru yaparak bilgi talep etme, kendisiyle ilgili verileri öğrenme, iletilmesini isteme, düzeltme ve silme hakkına sahip olmalıdır.

8) Sorumluluk İlkesi: Veri sorumluları kişisel verileri koruma ilkelerine uymaktan sorumlu olmalıdır.

Kişisel verilerin korunması ile 'veri güvenliği' sıkça birbiri ile karıştırılmaktadır. Birbirleriyle ilişkili kavramlar olsalar da aynı anlama gelmemektedir. Kişisel verilerin korunmasında amaçlanan şey, birey hak ve özgürlüklerinin korunmasıdır. Veri güvenliğinde ise verinin bizzat kendisi korunmaktadır. Ancak burada dikkat edilmesi gereken husus, verinin güvenliğinin sağlanmasının, ilgili kişinin kişisel verisinin korunmasına da hizmet ettiği gerçeğidir (Yürük, 2023, s. 904). Veri güvenliği teknik ve sistematik bir güvenlik çerçevesi sunarken, kişisel verilerin korunması bu çerçevenin insan odaklı etik ve hukuki boyutunu oluşturmaktadır. Verinin bütünlüğüne ve erişimine yönelik kontrol bireyin mahremiyetini de sağlamaktadır. Veri güvenliğine ilişkin bir ihlal durumuyla karşı karşıya kalındığında kişisel veriler kötüye kullanılabilmekte, yetkisiz erişimlere açık hale gelebilmekte, manipülasyon ile karşı karşıya kalınabilmekte veya siber suçlar için bir araç haline gelebilmektedir. Bu yüzden, her iki kavram bütüncül bir şekilde birlikte değerlendirilmeli, biri diğerine göre ihmal edilmemelidir.

Kişisel Verileri Koruma Kurumu

6698 sayılı KVKK'nın getirdiği en önemli düzenlemelerden birisi Kişisel Verileri Koruma Kurumu'dur. Kurum; idari ve mali özerkliğe sahip bir şekilde örgütlenmiştir.

Kişisel Verileri Koruma Kurumu'nun görevi ve yetkileri KVKK'nın 19. Maddesinde açıkça belirtilmiştir. Bu maddeye göre kurum; görev alanı doğrultusunda kişisel verilerle ilgili mevzuat ve uygulamaları takip ederek değerlendirmede ve öneride bulunabilmekte, araştırma ya da inceleme yapmakta veya yaptırabilmektedir. İhtiyaç duyulması halinde kamu kurumları, sivil toplum kuruluşları ve çeşitli paydaşlarla işbirliği yapan Kişisel Verileri Koruma Kurumu, uluslararası gelişmeleri yakından takip etmektedir. Uluslararası işbirliğine açık bir şekilde faaliyet yürüten Kurum, yıllık faaliyet raporunu Cumhurbaşkanlığına ve TBMM İnsan Haklarını İnceleme Komisyonu'na sunmakla mükelleftir (KVKK, 2016, Madde 19).

Kişisel Verileri Koruma Kurumu'nun karar organı Kişisel Verileri Koruma Kurulu'dur. Kurul; Avrupa Konseyi'nin 108 Sayılı Sözleşmesi ve AB'nin 95/46/EC Sayılı direktifine uygun biçimde bağımsız olarak oluşturulmuştur (KVKK, 2016, s. 1). Kurul, görevlerini ve yetkilerini bağımsız şekilde yerine getirmektedir. Hiçbir kurum, yetkili veya şahıs Kurul'un faaliyetlerine yön veremez, emir veremez ya da herhangi bir telkinde bulunamaz (KVKK, 2016, Madde 21). Bu açıdan kendi görevini icra edip yetkilerini kullanırken hiçbir dış etkiye hukuken maruz bırakılamaz. Kurul'un hiçbir otoritenin hiyerarşisi altında olmaksızın tamamen kendi iradesiyle hareket etmesi, aldığı kararların objektif olmasına, görevini hukukun üstünlüğüne uygun ve tarafsız bir şekilde yerine getirmesine imkân tanımaktadır.

Kurul'un en temel görevlerinin başında kişisel verilerin temel hak ve özgürlüklere uygun biçimde işlenmesini sağlamak gelmektedir. Kişisel verilerine yönelik haklarının ihlal edildiğini iddia edenlerin şikayetlerini karara bağlamak Kurul'un görevleri arasındadır. Bu durumda Kurul, bir şikâyet söz konusu olduğunda ya da ihlale yönelik iddiayı öğrendiğinde re'sen harekete geçip kişisel verilerin mevzuata uygun olarak işlenip işlenmediğini inceleyebilmekte ve gerekli önlemleri alabilmektedir (KVKK, 2016, Madde 22). Tıpkı diğer düzenleyici ve denetleyici kuruluşlarda olduğu gibi Kurul gerekli gördüğü bilgi ve belgeyi ilgililerden isteme, ilgililerin bilgilerine başvurma ve gerektiğinde yerinde incelemede bulunma görevine sahiptir (Gürsel ve Düğmeci, 2018, s. 324). Kurul'un diğer görevleri arasında kanunda belirtilen idari yaptırımlara karar verme, özel nitelikli verilerin işlenmesine yönelik gerekli önlemleri belirleme, veri güvenliğine ilişkin yükümlülüklerin belirlenmesi, veri sorumlusu ile temsilcisinin görev, yetki ve sorumluluklarını tespit

etmek amacıyla düzenleyici işlem yapma, stratejik planları karara bağlama, kurumun bütçe tekliflerini görüşme ve karara bağlama gibi faaliyetleri bulunmaktadır (KVKK, 2016, Madde 22).

Kurumsal bağlamda özerk ve karar organlarının merkezi idareden bağımsız hareket etme serbestisine sahip olduğu denetleyici ve düzenleyici kuruluşlar görevlerini ifa etme sürecinde düzenleme, denetleme, kural koyma ve gerek gördüğünde hukuki yaptırım uygulama yetkisine sahip olup, bu yetkiyi Anayasa'dan ve kendisine ait hukuki düzenlemelere bağlı kalarak yerine getirmektedirler (Çilingir, 2018, s.11). Kişisel Verileri Koruma Kurul'u da bu kapsamda düzenleyici işlemler tesis etmekle birlikte inceleme sırasında bir ihlal tespit ederse idari para cezası veya hukuka aykırılığın giderilmesi gibi idari yaptırım kararı verebilmektedir (Saygı, 2020, s. 31).

Kişisel Verilerin Korunmasında İdarenin Hukuki Sorumluluğu

İdarenin özel hukuka tabi faaliyetlerine ilişkin sorumluluğu özel hukuk hükümlerine göre tanzim edilirken; idari işlem, eylem ya da sözleşmelerden kaynaklanan sorumluluğu idare hukuku hükmü kapsamındadır (İrdem, 2021, s. 209). 1982 Anayasasının 125. Maddesinde belirtildiği üzere "İdarenin her türlü eylem ve işlemlerine karşı yargı yolu açıktır." Ayrıca, aynı maddenin devam eden hükmünde "İdare, kendi işlem ve eylemlerinden doğan zararı ödemekle yükümlüdür" ifadesi yer almaktadır (2709 sayılı Türkiye Cumhuriyeti Anayasası, 1982). Dolayısıyla idare hukuku açısından idarenin gerçekleştirdiği faaliyetler neticesinde karşılaşılan zararların idare tarafından tazmin edilmesi temel bir zorunluluktur (Durkal, 2019, s. 160).

İdarenin sorumluluğundan bahsedilebilmesi için üç şartın bir arada olması gerekmektedir. Bunlardan ilki, idarenin fiili olarak nitelendirilebilecek idari işlem veya eylemdir. İkincisi, idarenin yaptığı eylem ya da işlemin hukuken korunan bir menfaate yönelik zarar doğurmasıdır. Üçüncüsü ise zarar ile zarar veren olay arasında bir illiyet bağı kurulması hususudur (Kaya, 2018, s. 137).

Kişisel verilerin korunması bağlamında öncelikle değinilmesi gereken sorumluluk türü idari sorumluluktur. Veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmemesi, veri güvenliğine ilişkin gerekli yükümlülüklerin göz ardı edilmesi, Kurul tarafından re'sen ya da şikâyet üzerine gerçekleşen incelemeler neticesinde Kurul'un verdiği kararın yerine getirilmemesi, veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi veya ilgili kanun kapsamında bildirim yükümlülüğüne uyulmaması durumlarında veri sorumlusu idare hakkında idari para cezası uygulanabilmektedir. İdari para cezalarına ilişkin alt ve üst sınır KVKK'nın 18. Maddesinde "Kabahatler" kapsamında değerlendirilmektedir.

İdare hukukunda sorumluluk idarenin işlem ve eylemlerinden kaynaklanan zararların tazmin edilmesi yükümlülüğünü ifade etmektedir. İdarenin iş ve eylemlerinden kaynaklanan sorumluluğu; kusur ve kusursuz sorumluluk olmak üzere iki biçimde ortaya çıkmaktadır. İdarenin kusura dayalı sorumluluğu kusur sorumluluğunu oluşturmaktadır. Kusur sorumluluğu ya da diğer adıyla hizmet kusuru; idarenin kamu hizmeti ve faaliyetleri sırasında kusurlu bir davranış sergileyerek sebep olduğu zararı tazmin etmesidir (Çağlayan, 2017, s. 313). Kamu görevlileri, görevlerini ifa ederken kendilerine verilen araç, gereç ya da yetkileri kullanmak suretiyle görevleriyle doğrudan ya da dolaylı şekilde bağlantılı hukuka aykırı işlem veya eylemlerde bulunmaları hâlinde, bu fiillerden doğan zararlar nedeniyle üçüncü kişilere karşı sorumludurlar. Bu tür zararlar, idare açısından hizmet kusuru kapsamında değerlendirilir (Bozdağ, 2010, s. 36).

Kusurlu sorumluluk kapsamında kabul edilen durumlar hizmetin kötü işlemesi, hizmetin geç işlemesi, hizmetin hiç işlememesi halleridir (Nohutçu, 2016, s. 313). Kusur sorumluluğun temel özellikleri ise asli, bağımsız, genel, anonim ve değişken olma niteliklerine sahip olmasıdır (Işıklar, 2019, s. 120).

Bir kamu görevlisi tarafından gerçekleştirilen kişisel kusur idarenin hizmet kusurunu ya da sorumluluğunu ortadan kaldırmamaktadır. İdare kişisel kusuru olan kamu personelini kendi bünyesinde istihdam ettiğinden ve kamu personeli üzerinde denetim, gözetim ve eğitim verme yükümlülüğü bulunduğundan dolayı hizmet kusuru ile kişisel kusur birbirinden ayrı değerlendirilmemektedir (Sancakdar vd., 2022, s. 136). Nitekim, Danıştay 10. Dairesi (2024), sağlık hizmeti verilen bir hastanın fotoğraflarının izin almak suretiyle çekilmesi ancak davacıdan izin almaksızın internet sitesinde yayınlanması olayında, ilgili hekimin kamu hizmeti çerçevesinde hareket ettiğini ve bu nedenle, eylemin kişisel değil görev kusuru niteliğinde olduğunu belirtmiş; söz konusu eylemin idarenin sunduğu kamu hizmetinin parçası sayılması gerektiğini vurgulayarak, ortaya çıkan zararın idare tarafından tazmin edilmesi gerektiğine hükmetmiştir. Kamu personelinin hizmet içindeki kişisel kusurlu davranışları idarenin söz konusu görevlerini yeterince yerine getirmediğini göstermektedir. Bu nedenle, tazminatı ödeyecek olan idarenin, olayda kişisel kusuru ve sorumluluğu saptanacak kamu görevlisine yasal yollar çerçevesinde rücu etmesi gerekmektedir (Sancakdar vd., 2022, s. 136).

İdare, hukuka uygun olarak gerçekleştirdiği eylem ve işlemlerden doğan zararı hiçbir kusuru olmasa dahi bazı durumlarda tazmin etmek durumundadır ki, bu durum karşımıza kusursuz sorumluluk olarak çıkmaktadır (Gözler ve Kaplan, 2017, s. 205). Kusursuz sorumluluğun ortaya çıkması için nedensellik bağı yeterli olup, idare kusursuz eylem ve işlemlerinden doğan zararı karşılamakla yükümlüdür (Kaya, 2018, s. 136).

Kusursuz sorumluluk; iki başlık altında sınıflandırılmaktadır. Tehlikeli şeyler, tehlikeli yöntemler, mesleki riskler gibi unsurları içeren "risk sorumluluğu" ile toplumun tümü tarafından yararlanılan eylem veya işlemlerin neden olduğu külfetlerin belli kişi ya da kişilerin üstünde kalması durumunda zararın tazmini yani fedakârlığın denkleştirilmesi anlamına gelen "kamu külfetleri karşısında eşitliğin bozulmasından dolayı sorumluluktur" (Gözler ve Kaplan, 2017, s. 211-214).

Risk sorumluluğu, idarenin kendi faaliyetleri veya kullandığı araç gereçlerden kaynaklanan zararları tazmin etme sorumluluğudur. Birey ya da bireylerin diğerlerine göre orantısız şekilde daha fazla kamu külfetine maruz bırakılması durumunda ise eşitlik ilkesi ihlal edilmekte ve idare açısından kamu külfeti karşısında eşitliğin bozulmasından dolayı sorumluluk doğmaktadır. Kusursuz sorumlulukta idarenin kusuru olmadan zararı karşılamasının temel amacı adalet, eşitlik, hakkaniyet gibi değerleri tesis etmektir (Şaşmaz, 2016, s. 223).

İdarenin sorumluluğunu azaltan ya da kaldıran birtakım durumlarla karşılaşılmaktadır. İdarenin kusurundan doğan sorumluluğu mücbir sebepler, beklenmedik haller, zarar görenin kusuru ya da üçüncü bir kişinin veya kişilerin kusuru hallerinde tamamen ya da kısmen ortadan kalkabilmektedir. İdarenin sorumluluğu kusursuz sorumluluk bağlamında mücbir sebep ya da zarar görenin kusuru hallerinde azalma veya kalkma şeklinde olabileceği gibi beklenmedik durumların varlığı halinde ya da üçüncü kişilerin kusuru durumlarında kusursuz sorumluluk hali değişmeksizin sürebilmektedir (Tan, 2017, s. 497).

Kişisel verilerin korunması yükümlülüğü devlete aittir. Nitekim, devlet bu verilere erişim yetkisini münhasıran elinde bulundurduğundan koruma sorumluluğun süjesi olarak ön plana çıkmaktadır. İdare ise devletin yürütme yetkisini temsil eden otoritedir ve verilerin işlenmesi, depolanması ve muhafaza edilmesi süreçlerinde normatif bir sorumluluğa sahiptir. İdare, hukuki normlara ve etik ilkelere dayalı bir veri yönetimi stratejisi izleyerek kişilerin mahremiyetlerini korumakla mükelleftir. İdare verileri hukuka uygun olarak işlemeli, kullanmalı ve aktarmalıdır.

Sosyal devlet ilkesi gereği kamu hizmetini yerine getirmesi gereken idare, kamu hizmeti ifa ederken kamu yararı ile kişinin bireysel hakları arasındaki dengeyi iyi bir şekilde gözetmelidir (Aydın, 2020, s. 78). Demokratik bir hukuk devletinin ontolojik bir gerekliliği olarak idareden beklenen, bireylerin mahremiyet alanının nüvesini oluşturan kişisel verilerin hukuki açıdan güvence altına alınmasını sağlayacak koruma rejimini tesis etmektir. Bu kapsamda AYM, F.Ç kararında, kişisel verilerin hukuka aykırı biçimde ele geçirilmesine dair iddialar hakkında etkin bir ceza soruşturması yürütülmemesinin Anayasa'nın 20. maddesi anlamında kişisel verilerin korunmasını isteme hakkını ihlal ettiğine hükmetmiş, etkili bir hukuki mekanizmanın işletilmediğini vurgulamıştır (AYM, 2024, B. No: 2020/36976).

Veri sorumlularının kamusal otorite olması halinde idarenin sorumluluğu gündeme gelmektedir. Çünkü bir hizmet kusurunun varlığı söz konusu olup, veri işleme sırasında ortaya çıkan aksaklık kamu hizmetinin ifası sırasındaki hizmet kusuru sayılmaktadır (Gürpınar, 2017, s. 691). İdarenin kişisel verilerin korunmasına yönelik hizmet kusuru kişisel verileri işlerken KVKK'da belirtilen ilkelere uygun davranış sergilememesi durumunda ortaya çıkmaktadır. Veri işleme faaliyetinin hukuka aykırı gerçekleşmesi, hukuka uygun olmayan bir biçimde veri paylaşılması ya da aktarımı, veri güvenliğinin sağlanamaması, verilerin güncelliğini yitirmesi, doğru bir şekilde tutulmaması, amacın hâsıl olmasına rağmen silinmesi gereken kişisel verilerin silinmemesi gibi haller idareye sorumluluk yüklemektedir (Aydın, 2020, s. 81). Kişisel Verileri Koruma Kurulu'nun 2020/915 sayılı kararında belediyede görev yapan memurun işe giriş çıkışlarının biyometrik veri olan parmak iziyle takip edilmesinin, ölçülülük ilkesine ve veri işleme şartlarına aykırı olduğu değerlendirilmiş; veri sorumlusunun açık rıza olmaksızın özel nitelikli kişisel veriyi işlemesi nedeniyle Kanun'un 12. maddesine aykırı hareket ettiği hükme bağlanmıştır. Kurul, bu sebeple uygulamaya son verilmesini, mevcut verilerin imha edilmesini ve sorumlular hakkında disiplin süreci başlatılmasını kararlaştırmıştır (Kişisel Verileri Koruma Kurulu, 2020). AYM de benzer şekilde A.C kararında, idarenin kişisel verileri üçüncü kişilere aktararak başvurucunun özel hayata saygı hakkını ve kişisel verilerin korunmasını isteme hakkını ihlal ettiğine hükmetmiştir. Kararda, kişisel verilerin işlenmesinin açık rıza veya kanuni bir dayanakla mümkün olduğu, bu yükümlülüğe aykırı işlemlerin temel hak ihlali oluşturduğu açıkça vurgulanmıştır (AYM, 2020, B. No: 2016/4060).

Veri güvenliği açısından idarenin kusur sorumluluğu, genellikle ölçülülük ilkesine aykırı veri paylaşımı, hukuki bir dayanak olmaksızın verilerin kamuyla paylaşılması ve toplanan verilerin korunması için yeterli ve gerekli tedbirlerin alınmaması durumlarından kaynaklanmaktadır (Aydın, 2020, s. 82). Sağlık Bakanlığı'na bağlı bir kamu hastanesinde yaşanan, kişisel ve özel olan sağlık verilerinin yetkisiz kişiyle paylaşıldığı 2021/761 sayılı Kurul kararında (Kişisel Verileri Koruma Kurulu, 2021), veri sorumlusunun gerek teknik gerekse idari yükümlülüklerini ihlal ettiği tespit edilmiş; bu çerçevede açık rıza olmaksızın yapılan veri aktarımı Kanun'un 6. ve 8. maddelerine, erişim denetimi eksikliği ise 12. maddeye aykırı bulunmuştur. Kurul, veri güvenliği politikalarının geliştirilmesi, personel eğitimi, yetki matrislerinin yeniden düzenlenmesi ve olayın sorumluları hakkında disiplin süreci başlatılması yönünde yaptırım uygulamıştır (Kişisel Verileri Koruma Kurulu, 2021). Ayrıca, rızası alınması gereken bir bireyin rızası alınmadan verisinin işlenmesi de kusura dayalı sorumluluk halidir.

Siber ortamda verileri bozma, yetkisiz şekilde değiştirme, sistemlere erişimi engelleme veya zarar vermek amacıyla gerçekleştirilen saldırılar bireylerden geniş çaplı organizasyonlara, terör örgütlerinden devletlere kadar muhtelif sistemleri alaşağı etmeyi ve kullanılamaz hale getirmeyi hedeflemektedir (Çifci, 2023, s. 4). Hakkaniyet ilkesinin bir gereği olarak dijital ortamda çok sayıda veriyi rahatlıkla toplayabilen, depolayabilen ve analiz edebilen veri sorumluları bu veriyi aynı ortamda gerektiği gibi koruyamama riskini de üstlenmiş sayılmalıdır (Gürpınar, 2017, s. 691). Eğer idare veri koruma yükümlülüğünü yerine getirirken gerekli özen ve tedbirden yoksunsa kusurlu olarak kabul edilmesi gerekir. Çünkü KVKK'nın (2016) 12. Maddesinde veri sorumlusunun yükümlülüklerinden bahsedilmekte ve ilgili maddeye göre veri sorumlusu; kişisel verilerin hukuka aykırı işlenmesini önlemek, hukuka aykırı erişilmesini önlemek, kişisel verilerin muhafazasını sağlamakla amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her

türlü teknik ve idari tedbiri almakla mükelleftir. Bununla birlikte veri sorumlusu kendi kurum ve kuruluşunda bahse konu kanunun tatbik edilmesini sağlamak amacıyla gerekli denetimleri yapmak ve yaptırmak zorundadır. Nitekim, konu KVKK kapsamında değerlendirildiği için idarinin yeterli siber güvenlik önlemi almaması durumunda kusurlu kabul edilmesi en makul seçenektir. Ancak idarenin kendi hizmet kusuru olmasa da işlemleri ve eylemleri neticesinde risk ve kamu külfetleri karşısında eşitlik ilkesi gereği doğan zararı tazmin etmekle yükümlü olduğundan, idarenin her türlü önlemi almasına rağmen öngörülemeyen ve engellenemeyen bir siber saldırıya maruz kalması halinde kusursuz sorumluluk durumu da istisnai olarak gündeme gelebilir. Burada somut olayın özelliğini de göz önünde bulundurmak gerekir.

Kimi zaman devlet tarafından ortaya koyulan sosyal ve ekonomik hedeflere planlı bir şekilde ulaşabilmek için anketler yoluyla istatistiklerden yararlanılmaktadır. Kişilere yönelik yapılan anketlerde veriler anonimleştirilerek işlense de bireylerin bu durumdan zarar görme ihtimali bulunduğu için kamu külfetleri karşısında eşitlik ilkesi gereği idarenin kusursuz sorumluluğundan bahsedilebilmektedir (Aydoğdu, 2021, s. 281).

Kamu kurum ve kuruluşlarınca bireylerin verisi işlenirken bir ihlal gerçekleşirse ilgililer kişisel verilerini hukuka aykırı olarak depolayan ya da güvenliğini sağlayamayan idareye karşı maddi ve manevi zararını karşılamak için tam yargı davası açabilir. İptal ve tam yargı davası birlikte açılabileceği gibi önce iptal davası akabinde ise bu davanın neticelenmesiyle birlikte süresini geçirmemek kaydıyla tam yargı davası açılması mümkündür (2577 sayılı İdari Yargılama Usulü Kanunu [İYUK], 1982, Madde 12). İptal davası zararın tazmininden ziyade idarenin hukuka aykırı işlem veya eyleminin iptali, hukuka aykırılığın giderilmesi için açılır.

İdari eylem sebebiyle hakları ihlal edilmiş olanlar idari dava açmadan önce idareye başvurmalıdır. Buradaki temel kural, bu eylemin yazılı bildirim veya başka suretle öğrenildiği tarihten itibaren bir yıllık süreye tabi olmasıdır. Ancak her koşulda eylemin gerçekleştiği tarihten itibaren beş yıllık genel zamanaşımı süresinin aşılmaması şarttır. İlgili idareye yapılan talebin kısmen ya da tamamen reddi durumunda işlemin tebliğ edildiği günü takip eden gün itibarıyla dava süresi işlemeye başlar. İdareye yapılan başvuruya otuz gün içinde cevap verilmemesi durumunda ise bu sürenin bitimini izleyen tarihten itibaren dava süresi içinde yargısal yollara başvurulabilir (İYUK, 1982, Madde 13).

KVKK'nın 18. Maddesinin 1. fıkrasında sayılan ve kanunun ilgili maddelerinde belirtilen aydınlatma yükümlüğünün yerine getirilmemesi, veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi, Kişisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi, veri sorumluları siciline kayıt ve bildiri yükümlülüğüne aykırı hareket edilmesi, bildirim yükümlülüğünün yerine getirilmemesi gibi eylemlerin kamu kurum ve kuruluşları ile meslek kuruluşları bünyesinde gerçekleşmesi durumunda, Kurul tarafından yapılan bildirim üzerine, ilgili kamu kurum ve kuruluşlarında görev ifa eden memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem tesis edilerek sonucu Kurul'a bildirilmektedir (KVKK, 2016, Madde 18).

Türk Ceza Kanunu'nun 135-140. Maddeleri kapsamında kişisel verilerin hukuka aykırı olarak kaydeden, başkasına veren, yayan, ele geçiren, kanunların belirlediği süre geçmiş olmasına rağmen verileri sistem içinde yok etmeyen kişiler hakkında cezai işlem uygulanmaktadır. Bu suçların kamu görevlisi tarafından görevinin verdiği yetkiyi kötüye kullanarak ve mesleğinin sağladığı kolaylıktan istifade ederek işlenmesi halinde kamu görevlisinin cezai sorumluluğu doğmakta ve verilecek ceza yarı oranında artırılmaktadır (5237 sayılı Türk Ceza Kanunu, 2004).

Kişisel Verilerin Korunmasında Etik Boyut ve Yeni Teknolojiler

İdare, insan haklarına saygılı devlet yönetimi ilkesi çerçevesinde başta Evrensel İnsan Hakları Beyannamesi'nde ve AİHS'de güvence altına alınan özel hayatın gizliliği ve bireysel özerklik gibi temel ilkeleri esas almak üzere kişisel verilerin korunmasını sağlama görevini üstlenmektedir. Kişisel veriler özel hayatın gizliliğinin ve bireysel özerkliğin en temel nosyonudur.

Kişisel verilerin korunması hukuki bir boyuta sahip olduğu gibi aynı zamanda etik ve teknik bir meseledir. Teknik boyut kişisel verilerin korunmasında teknoloji temelli yazılımsal ve donanımsal önlemleri kapsamaktadır. Şifreleme, erişim kontrolü, veri maskeleme, güvenlik duvarları, siber güvenlik protokolleri bunlardan en önemlileridir. Etik boyut ise veri korumada bireysel mahremiyete saygıyı, toplumsal değerleri ve sorumlulukları göz önünde bulundurmayı esas almaktadır. Nitekim, KVKK'nın yayımladığı rehberde de yapay zekâ sistemlerinin "tasarımdan itibaren mahremiyet" ilkesine uygun şekilde geliştirilmesi ve yüksek riskli veri işleme faaliyetlerinde mahremiyet etki değerlendirmesinin zorunlu tutulması gerektiği vurgulanmaktadır (Kişisel Verileri Koruma Kurumu, 2023).

Nasıl ki hukuki boyut ve etik boyut genellikle birbiri ile ilişki içindeyse teknik boyut ve etik boyut da birbirinden tamamen bağımsız değildir. Şöyle ki; idarenin teknolojik alt yapısını güncellememesi sonucu veri ihlali yaşanmasının ya da teknolojinin ortaya çıkardığı yeni nesil tehditlere karşı koyacak eğitimli insan kaynağı eksikliğinin olmasının ispatı durumunda idarenin hizmet kusurunu tartışmaya açabilmektedir.

İdare güvenlik yönetimi bağlamındaki faaliyetlerinde kişisel verilerin korunmasına yönelik politikalar geliştirirken mutlaka özgürlük-güvenlik dengesini gözetmelidir. Özgürlüğün hizmetinde olmayan bir güvenlik anlayışının temel hedefinden sapacağı unutulmamalıdır (İrdem ve Bayansar, 2022, s. 140).

İdare kişisel verileri sadece önceden belirlenen amaca uygun olarak toplamalı ve işlemelidir. Amaca uygun olmayan gereksiz veri toplamaktan kaçınmalı, meşru amaca yönelik belirli bir sınır dâhilinde hareket etmelidir. Örneğin bir kamu hizmetinin görülmesi sırasında idare için yalnızca T.C. Numarası, isim, soy isim ve ikamet ettiği adresi yeterli iken; kişinin diğer aile üyeleri hakkında bilgi talebinde bulunulması o kişi ya da kişilerin mahremiyet ihlaline sebebiyet verebilmektedir. Ayrıca, idarenin gerektiğinden fazla veri toplanması olası bir siber saldırı durumunda güvenlik riskini artırabilmekte, hem idarenin güvenirliğinin vatandaş nezdinde sorgulanmasına sebebiyet vermekte hem de bireyler açısından telafisi güç zararlar doğurabilmektedir.

İdare kişisel verilerin korunmasına yönelik farkındalığı artırmalıdır. Bireylerin kendi kişisel verileri üzerindeki yetkisini, bu verilerin kim tarafından nasıl işlendiğini ve korunduğu öğrenmesi idarenin vatandaşa karşı etik yükümlülüğünün bir parçasıdır.

Teknolojinin getirdiği fırsatlar her ne kadar fazla ise esasında karşı karşıya kalınan tehditler de bir o kadar fazladır. Bunlardan bir tanesi de son yıllarda adından sıkça söz ettiren yapay zekâdır. Bilişsel sınırların ötesinde büyük verilerin işlenmesinde, analizinde ve karar alma sürecinde hız, etkinlik ve maliyet avantajı sağlayan yapay zekâ, hassas verilerin güvenliğinin sağlanmasında kurumlar ve bireyler için ciddi tehditler ortaya çıkarmaktadır.

Yapay zekâ; kurum ve kuruluşlarına iş ve işlemlerin otomatikleşmesinde, kişiselleştirilmiş hizmetlerin geliştirilmesinde, verimliliğin ya da üretkenliğin artmasında birçok fayda sağladığı gibi yapay zekâ araçlarının yoğun bir şekilde kullanılması ve kontrolsüz veri paylaşımı veri sızıntılarına neden olabilmekte, bireylerin veri gizliliğinin ihlalini beraberinde getirebilmektedir. Bu nedenle, kamu kurum ve kuruluşları ile bu kuruluşların kendi aralarında güvenli veri paylaşım platformlarının oluşturulması, idarenin yerli ve milli imkânlarla geliştirilen bilişim uygulamalarına ön ayak olması, düzenlemelerde bulunması ve denetimler yapması etik sorunların önüne geçmek açısından yararlı olacaktır.

Yapay zekânın bireysel özerkliği zedeleyecek şekilde kötüye kullanımı idarenin veri korumaya yönelik hukuki sorumluluğunu da hukuksuz ve adil olmayan bir yapıya evirebilmektedir. Örneğin; 'öngörücü polislik' olarak nitelendirilebilecek yapay zekâ destekli suç tahmini uygulamasının ön yargılı verilerle eğitilmesi neticesinde belirli bireylerin ya da grupların kesin ve somut deliller olmaksızın yüksek riskli olarak kategorize edilmesi masumiyet karinesi ve adil yargılanma hakkı gibi temel hukuki kaidelerin çiğnenmesine yol açabilmektedir.

Yapay zekânın kullanımı konusunda etik standartların ve normatif değerler zincirinin oluşturulması büyük önem taşımaktadır. Mevcut yasal düzenlemelerin ve bürokratik yapıların bilgi iletişim teknolojilerindeki gelişmeleri ve özellikle, yapay zekâ alanındaki ilerlemeleri dikkate alacak şekilde güncellenmesi elzemdir.

İdarenin kişisel verileri korumak amacıyla gerekli önlemleri alması idarenin etik sorumluluğunun en önemli parçasıdır. İdare kişisel verilerin korunmasında özen yükümlülüğünü yerine getirmelidir. Veri koruma ve gizlilik politikalarında etik mümkün olduğunca dikkate alınmalı, etik bilinci oluşturulmalıdır (Fabino, 2019, s. 63). İdarenin kamu hizmetinin sunumuna ilişkin faaliyetlerinde kişisel verilerin korunmasına yönelik özensiz, yetersiz ve ihmalkâr bir davranış sergilemesi hem etik soruna hem de hizmet kusurunun varlığına neden olacaktır.

Sonuç

İnsan hak ve hürriyetlerini esas alan, demokratik hukuk devletinin en temel özelliklerinden birisi bireysel özgürlüklerin korunmasıdır. Kişisel veriler, kişilere sıkı sıkıya bağlı olan, özel hayatın gizliliği kapsamında korunan mahremiyete haiz bilgilerdir. Bu verilerin korunması bireysel özgürlükleri koruduğu gibi toplumsal güvenliğin sağlanmasında, vatandaşların devletin yürütme aygıtı olan idari otoritelere olan güveninin pekişmesinde önemli rol oynamaktadır.

Kişisel verilerin etkin bir şekilde korunmasının en önemli unsurlarından biri siber güvenliktir. Siber güvenlik kişisel bilgilerin gizliliğini, bütünlüğünü ve mevzuatlara uygun bir şekilde erişilebilirliğini temin etmektedir. Devletler siber saldırılara karşı koyarak ve veri güvenliğini sağlayarak kişisel verileri korumak için etkin önlemler almak zorundadır. Bu kapsamda idarenin kişisel verileri dijital ortamlarda tutma, saklama ve koruma görevi bulunmaktadır. Bu verilerin çalınması, izinsiz kullanılması veya amacı dışında kullanılmasının önüne geçilmesi gerekmektedir.

Öncelikle tüm kamu kurum ve kuruluşları siber güvenlik ihlallerine karşı acil durum planları hazırlamalı ve uygulamalı, hassas verileri anonim hale getirerek saldırılardan etkilenme riskini azaltmalıdır. Kurum ve kuruluşlar işlem yaptığı bireylerin kişisel bilgilerini kriptografik yöntemlerle kodlayarak, yetkili kişilere daha korunaklı yöntemlerle güvenli erişim sağlamalıdır. Bununla birlikte kesintisiz olarak güvenlik analizleri ve sızma testleri gerçekleştirilmeli, veri sızması durumunda şeffaf bir şekilde kamuoyu ile derhal paylaşılarak telafisi güç zararların önüne geçilmelidir. Ayrıca, uluslararası siber güvenlik standartlarına optimum şekilde uyum sağlanarak dijital alt yapının güvenliği sürdürülebilir kılınmalıdır. Bu kapsamda çıkarılan siber güvenlik kanunu önemli düzenlemeler içermektedir.

İdarenin yaptığı işlem ve eylemlerinin hukuki sorumluluğunu üstelenmesi ve oluşabilecek zararları telafi etmesi hukuk devletinin bir sonucudur. Kişisel verilerin korunması kapsamında idarenin ya da istihdam ettiği personelin kusurlu ya da olayın niteliğine göre kusuru olmasa bile kusursuz sorumluluk nedeniyle ortaya çıkacak zararı tazmin etme zorunluluğu hukuk devleti olmanın gereğidir.

Kişisel verilerin korunması yalnızca hukuki bir yükümlülük değil, aynı zamanda etik sorumluluğu da içerir. Bireyin mahremiyet hakkı, insan onuru gibi temel değerler, veri işleme süreçlerinde gözetilmesi gereken etik ilkelerin merkezinde yer almaktadır. Hukuki çerçeve verinin nasıl işleneceğini belirlerken, etik ilkeler verinin neden ve hangi amaçla işlenmesi gerektiğine yanıt arar. Bu nedenle, kişisel verilerin anonimleştirilmesi, açık rıza alınması ve verilerin amaç ve beklenen sonuca uygun ve ölçülü bir biçimde işlenmesi etik sorumluluğun temel unsurudur.

Kaynakça

AB 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (AB Genel Veri Koruma Tüzüğü-GDPR). (2016, 27 Nisan). Erişim adresi: https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf.

Akkurt, S. S. (2020). Kişisel veri kavramının hukuki niteliğine ilişkin yaklaşımlara mukayeseli bir bakış. *Kişisel Verileri Koruma Dergisi*, *2*(2), 20-32.

Aksoy, H. C. (2017). *Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması*. Ankara: Çakmak Yayınevi.

Anayasa Mahkemesi (AYM). (2020, 17 Eylül). "Arif Ali Cangı başvurusu". Başvuru No: 2016/4060. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/karar?kararNo=2016/4060

Anayasa Mahkemesi (AYM). (2021, 15 Haziran). "Aylin Nazlıaka (2) başvurusu". Başvuru No: 2018/24439. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/karar?kararNo=2018/24439

Anayasa Mahkemesi (AYM). (2024, 13 Şubat). "Furkan Çakır başvurusu". Başvuru No: 2020/36976. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/karar?kararNo=2020/36976

Aydın, M. (2020). *Kişisel verilerin korunması bağlamında idarenin sorumluluğu ve yargısal denetimi*. Yayımlanmamış Yüksek lisans tezi, Ufuk Üniversitesi, Ankara.

Aydoğdu, Y. (2021). Kamu İdaresinde kişisel verilerin korunması. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, *29*(1), 263-293.

Baldwin, A. D. (1997). The concept of security. *Review of International Studies, 23*(1), 5-26.

Bozdağ, A. (2010). İdare hukukunda idarenin hizmet kusuru ve danıştay uygulaması. *Türk İdare Dergisi,* (468), 33-48.

Çağlayan, R. (2017). *İdare hukuku dersleri: Temel bilgiler*. Ankara: Adalet Yayınevi.

Çifci, H. (2023). *Her yönüyle siber savaş*. Ankara: TÜBİTAK Popüler Bilim Kitapları.

Çilingir, G. A. (2018). Türkiye'deki düzenleyici ve denetleyici kuruluşların idari yapı içerisindeki rolü. *Osmaniye Korkut Ata Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(1), 1-13.

Danıştay 10. Dairesi. (2024). "Kamu görevlisinin kişisel verileri hukuka aykırı biçimde paylaşmasına ilişkin hizmet kusuru kararı". E. 2020/6405, K. 2024/4947.

Deniz, M. Ö. (2023). Kişisel verilerin işlenmesi sözleşmesinin türleri ve hukuki nitelikleri. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi* Dergisi, *6*(1), 97-114.

Doğan, B. (2019). *Kişisel verilerin işlenmesi şartları bağlamında açık rıza*. Yayımlanmamış yüksek lisans tezi, İstanbul Üniversitesi, İstanbul.

Durkal, M. E. (2019). İdarenin sorumluluğunun ortaya çıkışı ve temeli. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, *23*(1), 159-189.

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD). (1980, 23 Eylül). Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personel Data. Erişim adresi: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

Fabino, N. (2019). Ethics and the protection of personal data. *Systems, Cybernetics and Informations,* 12(2), 58-64.

Gözler, K. & Kaplan, G. (2017). *Kısa idare hukuku*. Bursa: Ekin Basım Yayın Dağıtım.

Gürpınar, D. (2017). Kişisel verilerin korunmamasından doğan hukuki sorumluluk. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *19*(Özel Sayı), 679-694.

Gürsel, E. & Düğmeci, F. (2018). Yapısal anlamda Türkiye'de Kişisel Verileri Koruma Kurumu'na ilişkin bir değerlendirme. *R&S – Research Studies Anatolia Journal*, *1*(2), 318-329.

Gürsel, İ. (2016). Protection of personal data in international law and the general aspects of the Turkish Data Protection Law, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *18*(1), 33-61.

Hickok, M. (2023). Üretici yapay zekâ neden mahremiyet, ön yargı ve siber güvenlik açısından bir kâbus oluşturuyor? *Kişisel Verileri Koruma Kurumu Aylık Bülteni*, (Temmuz Sayısı), 6. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/77b8ccca-1748-46ad-a252-849120a7766a.pdf

Hijmans, H. & Raab, C. (2021). Ethical dimensions of the GDPR, AI regulation, and beyond. *Assunto Especial, 18*(100), 69-90.

Işıklar, C. (2019). Danıştay kararlarında idarenin kusursuz sorumluluğunu kaldıran ve azaltan haller. *Yıldırım Beyazıt Hukuk Dergisi*, *4*(1), 115-158.

İrdem, İ. & Bayansar, R. (2022). Özgürlük-güvenlik ikilemi ve insan hakları bağlamında kolluğun toplumsal olay yönetimi. *Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 12*(1), 140-155.

İrdem, İ. (2021). *Anayasal düzen ve idari yapı*, Ankara: Polis Akademisi Yayınları.

İrdem, İ., Alkan, Ö., Gören, K. B. & Arslan, Ö. (2021). *Güvenlik yönetiminde çağdaş yaklaşımlar*. Ankara: Polis Akademisi Yayınları.

Kaya, M. (2018). *İdare hukuku ve Türk idare teşkilatı*. İstanbul: Temsil Kitap.

Kişisel Verileri Koruma Kurulu. (2020, 1 Aralık). "Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması". Karar No: 2020/915. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6872/2020-915

Kişisel Verileri Koruma Kurulu. (2021, 6 Ağustos). "Kişisel sağlık verilerinin hastanedeki yetkisiz çalışanlar tarafından velayete sahip olmayan ebeveyn ile paylaşılması". Karar No: 2021/761. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7137/2021-761

Kişisel Verileri Koruma Kurumu (KVKK), "Kişisel Verileri Koruma Kurulunun Yapısı ve Görevleri", (E.T.: 28.04.2025, https://www.kvkk.gov.tr/Icerik/4107/Kisisel-Verileri-Koruma-Kurulu'nun-Yapisi-ve-Gorevleri)

Kişisel Verileri Koruma Kurumu (KVKK), "Veri Sorumlusu ve Veri İşleyen". Erişim adresi: https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen

Kişisel Verileri Koruma Kurumu. (2023). *KVKK Bülteni*. Kişisel Verileri Koruma Kurumu Yayınları.

Kutlu, Ö. & Kahraman S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi, 5*(4), 45-62.

Nohutçu, A. (2016). *Devlet Teşkilatı Hukuku, İdare Hukuku ve İdari Yargılama Usulü Hukuku – 2 Cilt*. Ankara: Savaş Yayınevi.

Oğuz, S. (2018). Kişisel verilerin korunması hukukunun genel ilkeleri. *Bilgi Ekonomisi ve Yönetim (BEYDER) Dergisi,* 13(2), 121-138.

Sancakdar, O., Önüt, L. B., Özelçi, A., Çalışkan, E. A. & Seyhan, S. (2022). *İdari yargı pratik çalışma kitabı*. Ankara: Seçkin Akademik ve Mesleki Yayınlar.

Saygı, S. (2020). 6698 sayılı Kanun'un sistematiğinde yargısal başvuru yolları. *Kişisel Verileri Koruma Dergisi*, *2*(2), 30-61.

Statista. (2025). *Estimated cost of cybercrime worldwide 2017-2028*. Erişim adresi: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide).

Şaşmaz, A. P. (2016). İdarenin sorumluluğu ve Danıştay kararlarındaki görünümüne genel bakış. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi,* 2(2), 211-235.

Tan, T. (2017). İdare Hukuku, Ankara: Turhan Kitapevi.

Yücedağ, N. (2019). Kişisel Verilerin Korunması Kanunu kapsamında genel ilkeler. *Kişisel Verileri Koruma Dergisi, 1*(1), 47-63.

Yürük, Z. (2023). Veri sorumlusunun veri güvenliğine ilişkin idari ve teknik tedbirleri alma yükümlülüğü. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *22*(48), 899-920.

2577 sayılı İdari Yargılama Usulü Kanunu (İYUK). (1982, 20 Ocak). *Resmi Gazete* (Sayı: 17580). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2577&MevzuatTur=1&MevzuatTertip=5

2709 sayılı Türkiye Cumhuriyeti Anayasası. (1982, 9 Kasım). *Resmi Gazete* (Sayı: 17863 [Mükerrer]). Erişim adresi: https://mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf

5237 sayılı Türk Ceza Kanunu. (2004, 12 Ekim). *Resmi Gazete* (Sayı: 25611). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK). (2016, 7 Nisan). *Resmi Gazete* (Sayı: 29677). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5