HAKEMLİ

Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler*

Metin BULUT**

ORCID ID: https://orcid.org/0000-0002-7770-9056
DOI: 10.30915/abd.811902
Makalenin Geldiği Tarih: 08.01.2019 **Kabul Tarihi:** 23.08.2019

* **Bu makale hakem incelemesinden geçmiştir ve TÜBİTAK–ULAKBİM Veri Tabanında indekslenmektedir.**

** Hacettepe Üniversitesi Hukuk Fakültesi Kamu Hukuku Anabilim Dalı Doktora Öğrencisi.

ÖZ

Hassas kişisel veriler, özel nitelikli kişisel veri kavramlaştırmasıyla ulusal ve uluslararası alanda hukuksal düzenlemeye konu olan ayrıcalıklı veri kategorilerini oluşturur. Bilgi teknolojilerindeki hızlı dönüşümün ortaya çıkardığı riskler ve bilgiye erişim ağlarının büyümesi hukuk oluşturma sürecinde hassas verileri ulusal ve küresel boyutlarda özel hale getiren önemli bir faktördür. Kişisel verilerin alt kategorisine ait olan özel nitelikli kişisel veriler, açıklanması ve başkaları tarafından erişilmesi halinde kişinin toplum içinde ayrımcılığa uğramasına veya mağdur edilmesine yol açacak inanç, politik-ideolojik görüş, adli sicil kayıtları, biyometrik ve genetik veriler, ırk, etnik köken ve sağlık bilgileri ile cinsel yaşam gibi yüksek duyarlıklı bilgi türlerini içerir. Bu nedenle kişi güvenliği, temel haklar, özel yaşam, gizlilik, çalışma hakkı, demokratik katılım ve toplumsal saygınlığın korunması, genel kişisel verilere kıyasla hassas veriler düzeyinde daha çok önemsenen hukuksal menfaat alanlarını betimlemektedir.

Anahtar Kelimeler: Hassas kişisel veriler, genel kişisel veri, açık rıza, özel yaşam, insan onuru.

A SPECIFIC LEGAL PROTECTION AND DATA CATEGORY AREA: SENSITIVE PERSONAL DATA

ABSTRACT

Sensitive personal data forms the category of privileged data which is a subject to legal regulation at national and international level with the conceptualization of special qualified personal data. The risks revealed by the rapid transformation of information technologies and the growth of access to information networks are important factors that make sensitive data, special in national and global dimensions in the process of law formation. Special personal data belonging to the sub-category of personal data includes information, which will lead to discrimination or victimization of the individual in the community if disclosed and accessed by others, to high-sensitivity and special features like sexual life and beliefs, political-ideological views, criminal records, biometric and genetic data, race, ethnicity and health information. For this reason, personal safety, fundamental rights, private life, privacy, right to work, democratic participation and protection of social dignity describe areas of legal interest which are considered more important at the level of sensitive data than general personal data.

Keywords: Sensitive personal data, general personal data, explicit consent, private life, human dignity.

GİRİŞ

Bilgi varlığı içinde önemli bir yer tutan kişisel veriler, davranış stratejisi oluşturmak, idari analizler yapmak, kamu düzenine ilişkin önlemler almak, kişilik profilleri çıkarmak, yapılandırılmış kişisel veri dizileri elde etmek ile siyasal, ekonomik ve kültürel eğilimleri etkilemek kapsamında değişik amaçlara konu yapılabilecek çok katmanlı bir düzlemde görünürlük kazanır. Kamu hizmeti sunumuna ilişkin kayıtlar, sağlık kuruluşlarınca oluşturulan kişisel dosyalar, tıbbi veri bankaları, güvenlik birimleri arşivi, sosyal güvenlik bilgi sistemi, sigorta sektörü ve istihdam alanında toplanan veriler ile telekomünikasyon, multimedya, elektronik işlemler ve internet ağlarında biriken bilgiler, kişisel verilerin dolaşım içine girdiği başlıca bilgi mecralarını meydana getirir.[1] Bireyin günlük yaşamını idame ettirdiği ve somut işlemler alanında doğrudan temas kurduğu sektörler ise sınav hizmetleri, elektronik bankacılık, e-ticaret, e-imza, e-devlet, e-okul ve uzaktan eğitim gibi dijital çağ uygulamalarını kapsayan yaygın bir sektör çeşitliliği sergilemektedir.[2] Gerek kurumsal ağ ortamlarıyla internet platformlarında gerçekleştirilen aktiviteler gerekse ziyaret edilen web siteleri yoğun bireysel başvuru ve faaliyetleri kayıt altına alarak son noktada tüm bilgileri kişisel hayatın dijital izleri halinde devasa bir arşiv birikimine dönüştürmektedir.[3]

Enformasyon ve bilgi teknolojilerinin kazandığı büyük boyutlu yenilik ve risklere bağlı olarak gelişim gösteren kişisel veriler ise kendisini kuşatan dijitalleşen dünyada güvenlik, kişi hakları, kamu yararı, kamu düzeni ve uluslararası ilişkiler sistemi gibi farklı dinamiklerin etkisi altında gelişim gösteren özel bir disiplin niteliği taşır. Bu sebeple başta Avrupa Birliği olmak üzere uluslarüstü kuruluşlarca düzenlenen belgelerde kişisel verilerin toplanması, kaydedilmesi, organizasyonu, saklanması, uyarlanması, değiştirilmesi, geri alınması, kullanılması, iletim yoluyla ifşa edilmesi, engellenmesi ve imha

---

[1] HENKOĞLU, Türkay, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, 1. Baskı, Yetkin Yayınları, Ankara, 2015, s. 20-21.

[2] ÖZENÇ, Köksal, **Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması**, Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık, 2007, Ankara, s. 183. .http://www.iscturkey.org/assets/files/2016/03/2007-26.pdf (Erişim Tarihi: 13.05.2018).

[3] GÜRSEL, İlke, "Protection of Personal Data İn İnternatıonal Law and The General Aspects of The Turkish Data protection Law", **DEÜ Hukuk Fakültesi Dergisi**, Yıl: 2016, Cilt: 18, Sayı: 1, s. 48-49.

edilmesi süreçleri titiz ve ayrıntılı çalışmaların konusu haline getirilmiştir.[4] Tasarlanan zaman, süreç ve eylem dinamiği içinde özellikle kişi haklarının güvence altına alınması ile kişisel verilerin korunması arasında yakın bağlar kurularak güçlü elektronik/dijital sistemler inşa edilmesi önerilerine sıkça rastlanmaya başlanmıştır. Bilgi güvenliği sistemlerinin kurulmasını zorunlu hale getiren formal eğilim sonuçta kamu yönetimi alanında da ayrıntılı normatif düzenlemeleri ve teknik yönetsel kapasite edinmeyi kaçınılmaz gören resmi bir pozisyon almayı gerektirmiştir. Bilgi teknolojilerinin yaygın kullanımı ölçüsünde bir risk yönetimi algısının eşzamanlı olarak yerleşmeye başladığından söz edilmeye başlanması[5] ise kişisel verilerle ilgili hukuksal düzenlemelere hız veren önemli bir motivasyon kaynağını ortaya çıkarmıştır. Bilgi varlığı, depolama sistemlerinin oluşturulması ve güvenlik sorunları ekseninde oluşan ilişki zeminiyle kişisel verilerin korunması arasında yakın hukuksal bağlantılar olduğunun belirtilmesi, ekonomik ve yönetsel sektörlerde risk yönetiminin çeşitli boyutlarına biçim vermekte ve koruma rejiminin kazanacağı içerikte tayin edici bir rol yüklenmektedir. Aynı anda mevcut toplumsal bilinç düzeyi, kamusal ve bireysel çapta beliren menfaat alanlarının uygun hukuki araçlarla bağdaştırılması çabasını teşvik ederek hukuksal, teknik ve yönetsel girişimlerin varlığını açığa çıkaran kendine özgü bir anlam dünyasını inşa etmektedir.

Veri koruma kanunları, yoğun çıkar kümeleri arasında bilgi güvenliği politikası alanında atılmış en önemli adımlardan birini oluşturur. Küresel standart ve direktiflerin izlenmesi ise hukuksallaşma çabalarının ana kaynağı durumundadır. Ulaşılan normatif çerçeve yarattığı istisnaların yoğunluğuna rağmen etik ve hukuksal sorumluluk alanında güçlü bir mevzuat kapasitesi kurmak amacıyla veri ihlallerini önlemeyi temel öncelikler sıralaması içine alan aktif bir görünüm sergilemektedir. Bu ilişkisel durumun öne çıkan yönü, temel hak ve özgürlükler düzeni, mahremiyetin korunması ve özel nitelikli hassas kişisel verilerin işlenmesi arasında kurulan çok yönlü bağlantıda yansıma bulur. Özel kişisel veriler ile hukuksal çerçeve ve teknik donanımın kesiştiği ortak zeminde güvenilir karar destek sistemleri ve potansiyel dijital ayrımcılıkla mücadele için etkili tahmin modelleri oluşturma, karmaşık

[4] ZİLİOBAİTE, Indre/CUSTERS, Bart, "Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models", **Artif Intell Law**, Yıl: 2016, Sayı: 24, s. 186.

[5] HENKOĞLU, **2015**, s. 22-25.; ÖZENÇ, **2013**, s. 183-184.

menfaat çatışmaları dikkate alındığında yüksek nitelikli bilgi güvenliği politikalarının vazgeçilmez gereklilikleri olarak görülmektedir.[6]

Özel nitelikli kişisel veri kavramının tanımı, içeriği, unsurları, işlenme koşulları ve istisnaları bilgi güvenliği ve koruma önlemlerinin kapsamı açısından yaşamsal önemde görüldüğünden, bu çalışmada yer verilen hukuksal açıklamalar öncelikle sözü edilen bilgi çerçevesinin analizi ve oluşturulan hukuksal mekanizma ve süreçlerin temel yönlerine ışık tutma amacı taşımaktadır. Türk ulusal mevzuatının küresel gelişmelerle bağını ortaya koyma çabasının bir parçası olarak evrensel hukuk birikiminin aldığı biçim, oluşturduğu kamusal işleyiş ve sistem araçları öncelikle hassas verilere yönelik genel açıklamanın mekânsal uygulama detaylarına odaklanma hedefiyle kendini sınırlamıştır. Türk hukuk mevzuatının özel nitelikli kişisel veriler etrafında geliştirdiği işleme ve koruma koşullarının genel kişisel veriler için öngörülen işlem süreçlerinden hangi açılardan farklılaştığı, küresel standart ve düzenlemelere uyumu ile inşa edilen yasal-kurumsal önlemlerin güçlendirilmiş özel bir veri alanının varlığı için yeterli ve etkili bir hukuksal mekanizma ortaya çıkarıp çıkarmadığına ilişkin sorular ise cevaplanması ve çözümlenmesi gereken diğer çekirdek sorun alanlarını oluşturmaktadır.

Özel Nitelikli Hassas Kişisel Verilere İlişkin Kavramsal Çerçeve

Özel nitelikli veriler[7], ortak hukuksal alanı paylaştığı kişisel veriler için yapılacak muhakemeye paralel olarak veri (data), enformasyon (information) ve bilgi (knowledge) temelinde tanımlanması gereken birçok teknik kavramı içinde barındırmakta ve ancak bağlantılı kavramların açıklanmasıyla belli bir somutluk kazanabilmektedir.

---

[6] ZİLİOBAİTE / CUSTERS, **2016**, s. 186.

[7] Özel nitelikli hassas kişisel veriler, çeşitli ülke kanunlarında ve uluslararası belgelerde special personal data (özel kişisel veri), sensitive personal data (hassas kişisel veri), special categories of personal data-besondere arten personenbezogener daten (özel kategorili kişisel veriler), veya data deserving special protection (özel korumaya layık olan veriler) gibi kavramlarla karşılanmaktadır. AKGÜL, Aydın, **Kişisel Verilerin Korunması Açısından İdarenin Hukuksal Sorumluluğu ve Yargısal Denetimi**, Doktora Tezi, Kocaeli, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2013, s. 13.; KAYA, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi" **İÜHFM**, Yıl: 2011, Cilt: LXIX, Sayı: 1-2, s. 318.

Veri, henüz işlenmemiş, düzenlenmemiş belirleyicileri ve hakkında yorum yapılmamış ham gerçeklikleri, olgu ya da sayıları[8] ifade ederken, bilginin anlamlı işlenişi ile verilerin kullanımı ve yorumlanması anlamına gelen *enformasyon*, bireyin düşünsel yapısında değişim oluşturan formlar ile zihinsel soyut verilerin işlenerek somut çıktılara dönüştüğü bilgi alanını meydana getirir. Başka bir anlatımla enformasyon, elde edilen veriler belirli bir konsept içine yerleştirildiğinde ve bir entelektüel sermaye ile geliştirildiğinde fark yaratan ayrım çizgisi olarak ortaya çıkar.[9] Anlamsal farklılığın her iki kavramın karmaşık ve belirsiz yapısı nedeniyle veri koruma hukuku bakımından etkili bir ayırt edicilik niteliği taşımayan yapay bir kategori yarattığı ve birbirinin yerine geçer şekilde kullanılmasının sorun teşkil etmeyeceği savunulmuş olsa da[10] koruma süjelerinin belirlenmesi açısından bilgi katlarını simgeleyen nitel şablonların korunmasında yarar olduğu savı karşı görüş olarak dile getirilebilir.

Knowledge karşılığı kullanılan bilgi ise yapısal olarak karar vericilik kriterine göre bireyin kişisel gerçekliğini yansıtan ve erişimi izne tabi olan olgulara karşılık gelir. Değer kazanmış enformasyon anlamına gelen bilgi[11], gerçekte birey tarafından algılanabilir her türlü kaynağı, veri ise tek başına dağınık ve anlamsız malumat yığınının bilgisayar sistemiyle anlamlandırıldığı bir işleme sürecini betimler. Veri ve enformasyon sıralamasından sonra gelen katmanda ileri bir safha içine konumlanan bilgi (knowledge) her iki kavramı da arka planına alarak bir kişiye, gruba veya esere atfedilen enformasyonun

---

[8] KÜZECİ, Elif, **Kişisel Verilerin Korunması**, 2. Baskı, Turhan Kitabevi, Ankara, 2018, s. 10. Anayasa Mahkemesi de verdiği kararda veri kavramına ilişkin aynı içerikte bir nitelemede bulunmuştur. Karara göre, "*'veri', bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öğe, muta, done' anlamına gelmekte olup bilimsel, istatistiki, ekonomik, kişisel bilgileri de içine alan bir kavramdır.*" AYM, E. 2010/40, K. 2012/8, K.T. 19.01.2012.

[9] TANG, Victor/YANİNE, Fernando/VALENZUELA, Lionel, "Data, İnformation, Knowledge and İntelligence The Mega-Nano Hypothesis and İts İmplications in İnnovation", **İnternational Journal of İnnovation Science**, Yıl: 2016, Cilt: 8, Sayı: 3, s. 203.

[10] KÜZECİ, **2018**, s. 12-13.

[11] MYERS, P.S., **Knowledge Management And Organizational Design**, Boston:Butterworth-Heinenman, 1996. Akt. ÇETİN, Hakan "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi" **Akdeniz İ.İ.B.F. Dergisi**, Yıl: 2014, Sayı: 29, s. 88.

kullanımına dayalı etkin bir eylem kapasitesi olarak adlandırılır.[12] Bu sıralanış ve konum hiyerarşisi içinde birbirini ilerletme ve biri diğerine kaynak olma açısından veri-enformasyon ve bilgi arasında kurulacak ilişkisel veya anlamsal düzen, güvenlik ve sistem yönetimi süreçleriyle bağlantılı bilgi varlığı ile kişisel veri öznelerinin korunması açısından yaşamsal önem taşır. Hukuki himaye görmesi beklenen bilgi türünün somut, nesnel, her çeşit medya ortamlarında depolanabilen ve erişilebilir olgulara ilişkin olmasının yanı sıra bilişsel süreçlere etki eden düzenli ve transfere açık bir yapı özelliği sergilemesi de temel gereklilikler arasındadır.

Veri konusuna ait kimlik bilgilerinin ya açıkça ya da ek bilgilerle dışa yansıdığı enformatif bilgi anlamındaki kişisel veri gerçekte uluslararası ve ulusal hukuk metinlerinde standart bir tanım olarak geçen belirli ya da kimliği belirlenebilir gerçek kişi ile bağlantılı bilgileri içerir.[13] Ancak enformasyon dâhil her tür bilgi ve veri parçacığı, bireye ilişkin tanımlayıcı karakteri olduğu sürece himaye görme, tanınma ve hukuki korumadan yararlanma hakkına sahip olmalıdır. Nitekim Türk hukuk sistematiği açısından 07.04.2016 tarihli ve 29677 sayılı Resmi Gazetede yayınlanarak yürürlüğe giren 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun genel gerekçesinde, bireylerin kimliklerini belirli hale getirmeye elverişli her tür bilgi tabanı esas alınarak[14] kişisel veri tanımı somutlaştırılmaya çalışılmıştır. Bireyin bizatihi kendisinin merkeze alındığı tanımda etkileşim kurulan çevre sınırına ilişkin olarak ise yargı içtihatlarında kişisel verilerin yetkisiz üçüncü kişilerin bilgisine sunulmayan, istendiğinde iradi olarak başka kişilere açıklanabilir olan ve dar bir toplulukla paylaşma özelliği gösteren niteliklere referans verilerek belirlemeler yapılmıştır.[15]

[12] TANG / YANİNE / VALENZUELA, **2016**, s. 2013.

[13] TÜRKAY, **2015**, s. 27-28.; AKGÜL, **2013**, s. 7-8.; Handbook On European Data Protection Law 2018 Edition, s. 83. https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf (Erişim Tarihi: 29.10.2018).

[14] Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 4. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi 13.05.2018).

[15] Y.12.C.D, E. 2017/2960, K. 2018/1541, K.T. 14.02.2018.

25 Mayıs 2018 tarihinden itibaren yürürlük kazanan ve henüz Türk iç hukukunun bir parçası sayılmayan Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR)[16] "*Tanımlar*" başlıklı 4/1. maddesinde 'kişisel veri' terimine ilişkin olarak '*tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi*' nitelemesinde bulunulmuş ve kendisinden önceki uluslararası hukuki metinlerde geçen tanım tekrar edilmiş olmakla birlikte veri sahibi kavramına ilişkin açıklamada '*tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı tanımlanabilen bir kişi*' denilerek kişisel veri kavramına yeni bir içerik tasarımıyla eğilmek gerektiği ima edilmiştir. Bu yaklaşımda özellikle '*gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü*' bilgiler kişisel verilerin kapsamı içinde zikredilmiş görünse de kişisel veri alanının özel nitelikli hassas verilere ilişkin öğelerle keskinleştirilerek belirginleştirilmeye çalışıldığı dikkatlerden kaçmamaktadır.

GDPR düzenlemesine yerini bırakmış olan 95/46/EC Sayılı Direktifin[17] 'Tanımlar' başlıklı 2. maddesi ise kişisel veri tanımı içinde veri öznesine ait fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğe özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı tespit edilebilen bilgileri zikrettiğinden hassas verilerin kişisel veri kapsamında hangi öğeleri içerdiğine yönelik giriş mahiyetinde bir başlangıç yapıldığı söylenebilir.

Anlam tespiti ve yorumlama çabasının tartışmaya açık olduğu ve pratikte hukuksal sınırlarının kolaylıkla çizilemediği hassas kişisel veriler[18], bu kavramsal çerçeve içinde belirli ya da kimliği belirlenebilir gerçek kişi ile ilgili her tür bilgi içinde sonuçları yönünden temel farklılıklar gösterir. Veri konusunun mahremiyetini temsil eden özellikli enformasyon ve bilgi

[16] Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016.

[17] Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayılı Ve 24 Ekim 1995 Tarihli Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi.

[18] KİNDT, Els, J., **Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis**, Springer: Newyork London, 2013, s. 124.

alanlarıyla bağlantısı ile sergilediği hassasiyet yoğunluğu nedeniyle özel kişisel veriler, daha sıkı yasal koşullara tabi tutularak belirlenir ve değişken bir korunmanın savunulduğu[19] özel arşivleme işlemine tabi tutulur.[20] Dolayısıyla kişisel verilerin alt kategorisine ait ve nitelikleri ile ifşası özel normlarla teminat altında olan hassas veriler, daha yüksek korumaya layık görülen ve bu nedenle bir dizi katı kuralların denetimi altına alınan kişisel veri kategorileridir.[21]

Söz konusu olan, açıklanması ve başkaları tarafından erişilmesi halinde kişinin toplum içinde ayrımcılığa uğramasına veya ötekileştirilmesine yol açacak inanç, politik-ideolojik görüş, adli sicil kayıtları, ırk, etnik köken, sağlık, üye olunan kurum ve kuruluş bilgileri ile cinsel yaşam gibi yüksek duyarlıklı ve hassas niteliğe sahip bilgi alanlarıdır.[22] Ulusal ve küresel düzeydeki entegre düzenlemelerle özel koruma altına alınan veri-enformasyon-bilgi katlarına ilişkin hukuki değerler, taşıdığı kişisel ve toplumsal riskler nedeniyle kişi güvenliği, temel haklar, özel yaşamın korunması, gizlilik[23] ve çalışma hakkı ile toplumsal saygınlığın korunması bakımından kamu otoriteleri ve devlet dışı kuruluşlarca uyulması gereken dikkat ve özen yükümünün öncelikli konusu haline getirilmiştir. Bu bakımdan hassas verilerle ilgili yapılacak yorumlarda tek başına bilginin yer aldığı veri kategorisinden ziyade, nitelik olarak aidiyet bağı kurulan bağlam ve anlam çerçevesine yoğunlaşmak hukuksal menfaat alanlarının tespiti için doğru bir yöntem olarak gözükmektedir.[24]

Türk pozitif hukuk düzeninde 6698 sayılı Kanun, hassas verileri küresel hukuk düzenlemelerine uyumlu bir şekilde ve ayrıntılı sayılabilecek bir çeşitlilik içinde saymış ancak herhangi bir tanım, açıklama ve gruplandırma

[19] KİNDT, **2013**, s. 124-125.

[20] KRANENBORG, Herke, "Access To Documents and Data Protection in The European Union: On The Public Nature of Personal Data", **Common Market Law Review**, Yıl: 2008, Sayı: 45, s. 1086.

[21] KUSCHEWSKY, Monika/GERADİN, Damien. "Data Protection in The Context of Competition Law Investigations: An Overview of the Challenges", **World Competition**, Yıl: 2014, Cilt: 37, Sayı: 1, s.73.; KRANENBORG, 2008, s. 1094.

[22] TÜRKAY, **2015**, s. 28.; KÜZECİ, **2018**, s. 253.; ZERDİCK, Thomas, "European Aspects of Data Protection: What Rights for the Citizen?", **Legal Issues of Economic Integration**, Yıl: 1995, Sayı: 2, s. 62.

[23] ZERDİCK, **1995**, s. 62.

[24] KÜZECİ, **2018**, s. 251.

yapmamıştır.[25] Kanunun 6/1. maddesine göre, '*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*

[25] Yargıtay 12. Ceza Dairesi'nin henüz 6698 sayılı Kanun'un yürürlükte olmadığı dönemde verdiği 15.05.2012 tarihli ve E. 2011/ 20072, K. 2012/ 12126 sayılı kararının muhalefet şerhinde kişisel verilerle ilgili olarak büyük oranda hassas verileri içine alan pratik ve açıklayıcı sayılabilecek bir sınıflandırma yapıldığı göze çarpmaktadır. Karara göre kişisel verilerin neler olabileceği şu başlıklar altında sınıflandırılmıştır:

a- Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançlara, cinsel tercihlere, etnik kökene, suç geçmişine, politik eğilimlere ve kişisel özel aktivitelere ilişkin bilgilerdir.

b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler ve kredi kartlarına ilişkin verilerdir.

c- Bilişim alanına ilişkin kişisel veriler: E-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. İnternette gezinti yapan kişinin birçok kişisel bilgileri paylaşması, bu bilgilerin kayıt altına alınması, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması bu alana verilen önemin başlıca nedenleridir.

d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak kimliğini tespit için dijital teknolojiden faydalanma bilimi) veriler de kişisel veriler arasındadır.

e- Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihlerinin toplum katmanları arasında bilinmesi halinde ayırımcılığa maruz kalma ihtimalini ortaya çıkarabilen bilgi kategorileridir.

Anayasa Mahkemesi ise önceki kararlarına atıfla kişisel verilerle ilgili olarak hassas kişisel verileri de içine alan genel bir örnek liste geliştirmiştir. Karara göre; "kişisel veri", "belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler" kişisel veri olarak kabul edilmektedir (E.2013/122, K.2014/74, 9.4.2014; E.2014/149, K.2014/151, 2.10.2014; E.2013/84, K.2014/183, 4.12.2014; E.2014/74, K.2014/201, 25.12.2014; E.2014/180, K.2015/30, 19.3.2015). AYM, E. 2015/32, K. 2015/102 K.T. 12.11.2015.; E. 2014/196, K. 2015/103 K.T. 12.11.2015.; B.No. 2014 / 4399, K.T. 21.09.2016.

mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.' Kanun maddesi sınırlı sayı (numerus clausus) esasını benimsemiş olsa da çeşitli ülke uygulamalarında milli köken, siyasi partilere veya hareketlere aidiyet, engellilik, bağımlılık, alkol ve uyuşturucu kullanımı, destek ve sosyal refah yardımları[26] WEB tarama geçmişleri, e-ticarette satın alma ve mal arama trafiği[27] gibi farklı bilgi kaynakları da özel nitelikli kişisel hassas veri türleri içinde kabul edilebilmektedir.

6698 sayılı Kanun sistematiği takip edildiğinde hassas veriler arasında gösterilen *ırk*, kalıtımsal olarak ortak fiziksel ve fizyolojik özelliklere sahip insanlar topluluğu, bir tür içinde belirgin farklılık gösteren birey grubu veya alt tür olarak tanımlanmaktadır. Ayrıca kavram için deri, göz, saç rengi, saç ve baş biçimi, boy, kan grubu vb. kalıtımsal özellikleri ile birlik gösteren kişilerin oluşturdukları doğal topluluk adlandırması da yapılmaktadır.[28] *Etnik köken* bilgisi ise dirimbilimsel (biyolojik) ve ekinsel (kültürel) bakımlardan türdeş özelliklerle birbirine bağlanmış üyelerden kurulu olan ve bu özelliklerle kimliklendirilen toplumsal kümeyi ifade etmektedir.[29]

Diğer bir hassas veri türü olarak kanunda yerini alan *siyasi düşünce*, devletin etkinliklerinin amaç, yöntem ve içerik açısından hangi esaslara göre düzenlenmesi ve gerçekleştirilmesi gerektiğine ilişkin kişilerin düşüncelerini belirtir. *Dini görüş*, kişinin Tanrı'ya, doğaüstü güçlere, çeşitli kutsal varlıklara inanma ve tapınma sistemini içerirken, *mezhep* bir dinin görüş, yorum ve anlayış farklılıkları sebebiyle ortaya çıkan kollarından her birini tasvir eder.[30] *Felsefi görüş* kavramıyla ise, kişinin inceleme amacı taşıyan düşünce etkinliği sonucunda ulaştığı tüm görüşler anlatılmak istenir. Kanunda geçen *kılık*

[26] KAYA, 2011, s. 319.

[27] ÇAKAN, Cansu, "Kişilik Hakkı Kapsamında Korunan Bir Değer Olarak Kişisel Veriler", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2013, Sayı: 2, s. 195.

[28] http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.5b0350a8c86216.44879670; http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b03504c269c89.67813800 (Erişim Tarihi: 08.05.2018).

[29] http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.5b03536c04b525.03378534 (Erişim Tarihi: 08.05.2018).

[30] AYM, E. 2016/125, K. 2017/143, K.T. 28.09.2017.

kıyafetle de kişinin üstü başı, giyinişi ve dış görünüşüne ilişkin bilgilerin kastedildiği söylenebilir.[31]

Dernek, kazanç paylaşma amacı gütmeyen gerçek veya tüzel kişi en az yedi kişinin belirli ve ortak bir amacı gerçekleştirmek üzere, bilgi ve çalışmalarını sürekli olarak birleştirmek suretiyle oluşturdukları özel hukuk tüzel kişileridir. *Vakıflar*, gerçek veya tüzel kişilerin yeterli mal ve hakları belirli ve sürekli bir amaca özgülemeleriyle teşkil ettikleri tüzel kişiliğe sahip mal topluluklarıdır.[32] *Sendika* ise 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu'nun 2/ğ maddesinde 'işçilerin veya işverenlerin çalışma ilişkilerinde, ortak ekonomik, sosyal hak ve çıkarlarını korumak, geliştirmek için en az yedi işçi veya işverenin bir araya gelerek bir işkolunda faaliyette bulunmak üzere oluşturdukları tüzel kişiliğe sahip kuruluşlar" şeklinde tanımlanmış; 4688 sayılı Kamu Görevlileri Sendikaları ve Toplu Sözleşme Kanununun 3/f maddesinde ise kamu görevlilerinin ortak ekonomik, sosyal, meslekî hak ve menfaatlerini korumak ve geliştirmek için oluşturdukları tüzel kişiliğe sahip kuruluşlar olarak nitelendirilmiştir. Her üç kuruluşa üyelik, kişinin siyasal görüşü, kültürel tercihleri ve toplumsal statü bilgisi açısından özel yönler içerdiğinden kayıtlı verilerin hassas kişisel veri kapsamında kabul edilmesi gerekmiştir.

Farklı bir hassas veri türü olan *Cinsel hayatı* oluşturan unsurlar, bireye özgü cinsel eğilimleri ve seks hayatına ilişkin olguları kapsar.[33] Kişinin cinsel tercihleri veya benimsediği yaşam tarzı toplumsal önyargıları harekete geçirme etkisi taşıdığından birey hakları, ayrımcılığa uğramama ve kişilik değerlerinin korunması açısından bu aidiyetler, duyarlık düzeyi yüksek veriler olarak etiketlenmiştir.

İnsan onuru, kişilik hakları, özel hayatın gizliliği ve kişisel verilerin korunması haklarıyla sıkı bağlantılar içindeki *sağlık verilerinin* ise veri mahremiyetinin korunması açısından önemli bir yere sahip olduğu açıktır. Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi, Lizbon Hasta Hakları Bildirgesi, Bali Bildirgesi, 1981 tarihli Dünya Tabipler Birliği Hasta Hakları

[31] http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b035cae955f04.22462695 (Erişim Tarihi: 08.05.2018).

[32] GÖZLER, Kemal, **İngilizce Karşılıklarıyla Hukukun Temel Kavramları**, 8. Baskı, Ekin Yayınları, Bursa, 2011, s. 190,194.

[33] AKDAĞ, Hale, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Ankara, Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 29.

Bildirgesi, Amsterdam Bildirgesi ve 1998 tarihli Hasta Hakları Yönetmeliği ile 1999 yılında yürürlüğe giren 164 sayılı Avrupa Konseyi Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve İnsan Haysiyetinin Korunması Sözleşmesi hasta hakları konusunda özel veri esaslarına yer veren başlıca düzenlemelerdir. Örneğin, 1981 tarihli Dünya Tabipler Birliği Hasta Hakları Bildirgesine göre hasta tüm tıbbi ve özel hayatına ilişkin bilgilerin gizliliğine saygı duyulmasını bekleme hakkına sahiptir.[34]

Türkiye uygulamasında *kişinin dokunulmazlığı, maddi ve manevi varlığı* başlıklı 17. madde ile *sağlık hizmetleri ve çevrenin korunması* başlıklı 56. madde sağlık verileri alanında anayasal çerçeveyi oluşturmaktadır. 20.10.2016 tarihli ve 29863 sayılı Resmi Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in "*Tanımlar*" başlıklı 4/f maddesinde *kişisel sağlık verisi*, kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili veriler olarak belirtilmiştir. "*Kişisel sağlık verilerinin korunması*" başlıklı 6. maddede ise veri güvenliğinin sağlanması için alınacak önlemler sıralanmış; kişisel sağlık verilerinin hukuka aykırı işlenmesini ve erişilmesini önlemek, bu verilerin muhafazasını sağlamak amacıyla uygun güvenlik yapısını temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak ve bu tedbirlerin veri sorumlusu tarafından denetlenmesine izin vermek veri işleyen görevlinin uymak zorunda olduğu yükümlülükler kapsamında düzenleyici işlem kuralı haline getirilmiştir.[35]

---

[34] TEZCAN Durmuş/ERDEM Mustafa Ruhan/ SANCAKDAR Oğuz/ ÖNOK Rifat Murat, **İnsan Hakları El Kitabı**, 6. Baskı, Seçkin Yayınları, Ankara, 2016, s. 607.

[35] Avrupa İnsan Hakları Mahkemesi (AİHM), 25 Şubat 1997 tarihli Z.-Finlandiya kararında. kişinin özel hayatına ve aile yaşamına saygı hakkı kapsamında tıbbi verilerin gizliliğine saygı göstermeyi AİHS'e taraf olan bütün sözleşmeci devletlerin yasal sistemlerinin temel bir prensibi olarak görülmesi gerektiğini belirtmiştir. I v. Finlandiya Kararı da aynı yönde açıklamalar içermektedir. KÜZECİ, **2018**, s. 255.; ÇOKMUTLU, Metin, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, Doktora Tezi, Kocaeli, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s. 93-97,98. Tıbbi verilerin kullanımında özel hayatın gizliliğinin, demokratik bir toplumda gerekli görülenin ötesinde, orantısız bir şekilde müdahaleye uğramaması yönünde S. and Marper Kararı için bkz. ÇOKMUTLU, **2014**, s. 99. Anayasa Mahkemesine göre sağlık verilerinin işlenmesini öngören kuralla, halk sağlığının geliştirilmesi, hastalık risklerinin azaltılması ve önlenmesi suretiyle kamu sağlığının korunması; sağlık hizmetleri ile bu hizmetlerin finansmanının planlanması ve yönetimi suretiyle teşhis, tedavi ve rehabilite edici sağlık hizmetlerinin yürütülmesi, eğitim ve araştırma faaliyetlerinin geliştirilmesi, insan gücü ve maddi kaynaklarda tasarruf

Kanunda hassas kişisel veri türleri arasında sayılan diğer bir kategori, önemi ve kapsamı itibariye geniş yer tutan *biyometrik ve genetik* verilerdir. Grekçe yaşam anlamına gelen *bios* ve ölçü anlamına gelen *metron* kelimelerinden türeyen biyometrik[36] ve genetik veriler ile anlatılmak istenen, biyolojik veya davranışsal özellikleriyle birlikte, kimliksel doğrulama yapmak amacıyla fizyolojik veya davranışsal niceleyicilerini kullanan bireyin kendine has, benzersiz, genelde ömür boyu aynı kalan, güvenilirlik düzeyi yüksek veri bütünlüğüdür. Kimliksel tanımlama için kullanışlı öğeler sunan biyometri, bir kişinin ölçülebilir fiziksel veya evrensel tüm gerçek kişilerde mevcut olan temel karakteristiği veya özelliğini ifade eder.

Biyometrik sistem, araştırma konusu kişiyi biyometrik verileri sistemde saklanan diğer bireylerden ayırt ederek tanıma yapan bir veri eşleştirme düzeneğidir. Bireyin genetik bilgisinin depolandığı, her insan için benzersiz, kalıcı ve evrensel DNA (Deoxyribonucleic Acid), parmak, avuç içi damar izi ve retinal tarama, el, ses tanıma verisi, yüz imajı, el ve parmak geometrisi, kulak kanalı, kişilerin irisi ve çeşitli biyometrik teknolojilerin kombinasyonlarını içeren çoklu biyometrik sistemler, bu yapı içinde öne çıkan başlıca veri unsurlarıdır.[37] Hassas kişisel veri grubu içinde biyometri ve genetik bilgilerin ayrıca bireysel kimliğe sıkı sıkıya bağlı olduğu ve kontrol edilmesi halinde objektif sonuçlar doğurduğu gerekçesiyle nitelikli verileri temsil ettiği varsayılmaktadır.[38]

---

sağlanması ile verimin artırılması amaçlanmaktadır. AYM, E. 2016/125, K. 2017/143, K.T. 28.09.2017.

[36] TRANBERG, Charlotte Bagger, "Biometric Data in Scandinavia", **European Business Law Review**, Yıl: 2008, Cilt: 19, Sayı: 2, s. 389.

[37] ERDİNÇ, Göksu H., **Bilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler**, Yüksek Lisans Tezi, İstanbul, İstanbul Teknik Üniversitesi Bilişim Enstitüsü, 2017, s. 50.; TRANBERG, **2008**, s. 389-390.; KİNDT, **2013**, s. 141 vd. "*DNA Kan, saç, bukkal mukoza, tükürük, ter, insan dokusu, deri kabukları, tırnaklar, kemik, dişler, idrar ve meni gibi çok sayıda biyolojik materyalden elde edilebilir.*" s. 166.

[38] Avrupa İnsan Hakları Mahkemesinin *S. ve Marper/Birleşik Krallık Davası (Başvuru No.30562/04 ve 30566/04)*, s.19, 22.
Downloads/CASE%20OF%20S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20-%20[Turkish%20Translation]%20by%20the%20COE%20Human%20Rights%20Trust%20Fund.pdf (Erişim Tarihi: 07.11.2018).

Son olarak Türk hukuk düzenlemesinde *ceza mahkumiyetine* ilişkin veriler 5237 sayılı Türk Ceza Kanunu'nun 45. maddesi uyarınca suç karşılığında yaptırım olarak öngörülen hapis (hürriyeti bağlayıcı ceza) ve adli para cezaları (malvarlığı değerlerine yönelik ceza) bilgisinden oluşur. Suç işleyen kişinin tehlikelilik durumu, suçun konusu ile ilgili ya da suçun işlendiği araçla bağlantılı olarak veya maruz kaldığı tehlike hali dikkate alınarak uygulanan koruma ve iyileştirme amaçlı ceza hukuku yaptırımlarına ilişkin TCK'nın 53-60. maddeleri arasındaki hükümler ise güvenlik tedbiri kapsamındaki verilerdir. Örneğin belli haklardan yoksun bırakılma, eşya ve kazanç müsaderesi, çocuklara ve akıl hastalarına özgü güvenlik tedbirleri, suçta tekerrür ve özel tehlikeli suçlular, sınır dışı edilme ve tüzel kişiler hakkında uygulanan güvenlik tedbirleri [39] pozitif hukuk çerçevesinde sayılabilecek veri parçalarıdır.

Özel Nitelikli Hassas Kişisel Verilerin Ulusal ve Küresel Düzeyde Koruma Altına Alınması

Genel olarak kişisel verilerin korunması hakkına yönelik ulusal düzeydeki hukuksal düzenlemeler, 20.yüzyılın son çeyreğine rastlayan dönemleri kapsar. 1970'te Almanya, 1973'te İsveç, 1974'te Amerika Birleşik Devletleri, 1976'da İspanya, Avusturya, Portekiz ve 1978 yılında Fransa kişisel verilerin koruma altına alınmasında ilk ulusal düzenlemeleri yapan ülkelerdir.[40] Küresel düzeyde koruma alanının oluşturulması ise bilgi sistemleri ve bilişim ağlarının ulus aşırı genişlemesi süreçleriyle bağlantılı nitel bir gelişim öyküsüne sahiptir. Devlet, özel kuruluşlar ve bireysel kullanıcılar tarafından bilginin yaygın kullanımı, bilişim teknolojilerindeki hızlı dönüşümün ortaya çıkardığı riskler ve bilgiye erişim ağlarının büyümesi küresel düzenlemelerin çıkış noktası ve temel hareket kaynağını teşkil etmiştir.

Kişisel verilerin korunması alanında Avrupa Konseyi bünyesinde ilk ulus aşırı çalışmalar 1970'li yıllara kadar götürülse de kişisel verilerin korunması hakkı, modern dönem ulusal hukuk düzenlemelerinden esinlenerek ancak 1980'li yıllardan itibaren uluslararası sözleşme ve hukuksal düzenlemelerde yer almaya başlamıştır. Konsey çalışmasından önce küresel çaptaki ilk örnek, modern teknolojilerin neden olduğu değişen bilgi ortamları karşısında üye

[39] KOCA, Mahmut / ÜZÜLMEZ, İlhan, "**Türk Ceza Hukuku Genel Hükümler**", 10. Baskı, Seçkin Yayınları, Ankara, 2017, s. 554, 611-613.

[40] KÜZECİ, **2018**, s. 112 vd.

ülkelerdeki serbest veri akışını sağlama amacına yanıt vermek üzere Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın (OECD) yayınladığı 23 Eylül 1980 tarihli *Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler*'dir. Avrupa Konseyi kaynaklı '*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme* ise üye ülkelerin belli bir standarttan yoksun dağınık ve bölünmüş mevzuatını uyumlaştırmayı amaçlayan veri koruma alanındaki bağlayıcı ilk uluslararası hukuksal belge niteliğindedir. Kişisel verilerin aktarımı ile gizlilik hakkını uzlaştırmaya yönelen sözleşme,[41] 28 Ocak 1981 tarihinde Strazburg'da imzaya açılarak 1 Ekim 1985'te yürürlüğe girmiş, Türkiye tarafından 28 Ocak 1981 yılında imzalanmasına karşın ancak 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete'de yayımlanarak iç hukukta yürürlük kazanmıştır. Sözleşme, kişisel verilerin sınır ötesi akışının yoğunluk kazanması karşısında temel hak ve özgürlüklere ilişkin güvencelerin ve özel yaşama saygı hakkının genişletilmesine taraftar olduğunu belirtmiş ve bu kapsamda hassas kişisel verileri ***özel veri kategorileri*** (Special categories of data) başlığı altında 6. maddesinde düzenlemiştir. Düzenlemeye göre, iç hukukta uygun ve yeterli güvenceler sağlanmadıkça, ırksal köken, siyasi düşünceler, dini veya diğer inançlar, sağlık veya cinsel hayat ile ceza mahkumiyeti kapsamındaki kişisel veriler, otomatik işleme tabi tutulamayacaktır. Sözleşme, istisnalar ve kısıtlamalar başlıklı 9. maddesinde ise 6. maddede öngörülen güvence sistemine belirli gerekçeler ışığında istisna ve kısıtlama hükümleri getirilebileceği kuralına yer verir.

Sözleşmede, taraf devletin kanunlarında öngörülmüş olması, demokratik bir toplumda devlet ve kamu güvenliğinin korunması esasının gözetilmesi, devletin mali menfaatleri veya suçların önlenmesi ile kişinin veya başkalarının hak ve özgürlüklerinin garanti edilmesi sebeplerine dayalı olarak hassas verileri düzenleyen 6. maddeye konulabilecek istisnai durumlara açıklık kazandırmak amaçlanmıştır. Ancak maddede istisna hükümlerin genel ve yoruma açık hukuki sebeplerden oluşması, hassas veriler açısından hukuksal belirlilik ve güvenlik ilkelerini ihlal eden potansiyel risklere kapı aralamaktadır.

Konsey, 08.11.2001 tarihinde kabul ettiği *181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol* ile

[41] KİNDT, **2013**, s. 91.

hassas kişisel verileri de içine alan tüm kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici makam kurulmasını taahhüt etmiş ve verilerle ilgili alınacak önlemlerin özerk bir yönetsel birim tarafından üstlenilmesini şart koşmuştur. Avrupa Konseyi'nin 4.4.1997 tarihli Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesinin "*Özel yaşam ve bilgi edinme hakkı*" başlıklı 10. maddesinde ise '*Herkesin, kendi sağlığıyla ilgili bilgiler bakımından özel yaşamına saygı gösterilmesi, kendi sağlığı hakkında toplanmış herhangi bir bilginin öğrenilmesi hakkına sahip olduğu*' belirtilerek özel yaşam bağlamında sınırlı bir hassas veri yaklaşımı geliştirildiği görülmektedir.

Hassas kişisel veriler bakımından Avrupa Konseyi'ne atfedilebilecek diğer bir hukuki belge, 4 Kasım 1950'de Roma'da imzalanarak 3 Eylül 1953'te yürürlüğe giren *İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi*'dir. Sözleşme, kişisel verilerin korunması, işlenmesi, depolanması veya erişime açılması hakkında doğrudan bir düzenleme içermemekle birlikte Avrupa İnsan Hakları Mahkemesi'nin geliştirdiği içtihatlar ve sözleşmenin özel hayata ve aile yaşamına saygıyı düzenleyen 8. maddesi dolaylı olarak hassas kişisel verilere yönelik hukuki koruma sağlamaktadır.

Avrupa Birliği (AB) düzeyinde kişisel verilerin korunması kapsamında hassas verilere ilişkin temel haklar vurgusuyla ayrıntılı hukuki düzenlemeler yapılmış ve birlik üyelerini bağlayıcı etkili hukuk metinleri oluşturulmuştur. İlk hukuksal düzenleme Birlik ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılması ve kişilerin mahremiyet haklarını korumayı amaçlayan 95/46/EC sayılı *Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi*'dir. AB üyesi ülkelerin kişisel verilerin korunmasına yönelik yasal düzenlemelerini yönlendirici etkisiyle direktif, yakın zamana dek geniş bir nüfuz alanına sahip olmuştur. Türkiye'nin yürürlüğe koyduğu kişisel verilerle ilgili 6698 sayılı Kanun da benimsediği hukuk sistematiği ve haklar düzeni açısından temel noktalarda anılan Direktif hükümlerini yasalaşma pratiğine model olarak almıştır.[42]

[42] "**Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler**", Kişisel Verileri Koruma Kurulu yayınları, 2018, s.3-7. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ead8e671-e01e-4ca7-a6a3-bc3c6f79f7c7.pdf (Erişim Tarihi 01.05.2018).; KİNDT, **2013**, s. 92.

Hassas kişisel veriler bakımından konuya yaklaşıldığında, 95/46/EC sayılı Direktifin 8. maddesinde bu tür verilerin, '***Özel kategorilerdeki kişisel verilerin işlenmesi***" (The processing of special categories of data) başlığı altında düzenlemeye konu kılındığı görülmektedir.[43] Ancak Direktif, 25 Mayıs 2018 tarihinden itibaren yürürlük kazanan Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) yerini bıraktığından hassas kişisel veriler bakımından bu son tüzük hükümlerinin geçerli olduğunu vurgulamak gerekir. Tüzük, hassas veri kavramını karşılamak üzere 9. maddesinde aynı madde başlığıyla '***Özel kategorilerdeki kişisel verilerin işlenmesi***' (processing of special categories of data) terimini kullanmıştır.[44]

7 Aralık 2000 Tarihli AB Temel Haklar Şartı ise[45] "*Kişisel bilgilerin korunması*" başlıklı 8. maddesinde herkesin, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahip olduğunu, kişisel verilerin belirtilen amaçlar ekseninde ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılması gerektiğini, kişinin kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkını haiz olduğunu düzenlemesine karşın, sözleşme doğrudan hassas veri kavramına yer vermemiştir.

Hassas verileri kapsamasa da OECD'nin "*Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri*" (23 Eylül 1980) ile Birleşmiş Milletler'in '*Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri*' (14 Aralık 1990) kişisel verilerin korunmasına ilişkin uluslararası düzeyde belirtilebilecek etkili hukuki belge örnekleri arasındadır. Yine ayrımcılıktan kaçınma ilkesine göre '*etnik köken, cinsel yaşam, dini ve felsefî inanç gibi konular kapsamındaki bilgilerin toplanmasında kanunî sınırlar söz konusu olmalı ve kanunun çizdiği sınırlar içerisinde sadece hukuka uygun şekilde ve gerektiğinde veri toplanmalıdır*' denilerek sözü edilen belgede hassas veri kavramına uygun özel bir belirleme yapıldığı göze çarpmaktadır.[46] Bunun yanında Birleşmiş Milletler Genel Kurulu'nun 10

[43] KAYA, Mehmet B./ TAŞTAN Furkan G., **Veri Koruma Hukuku: Mevzuat İçtihat**, s. 55-56. http://www.muharrembalci.com/kitaplika/79.pdf (Erişim Tarihi 13.05.2018).

[44] https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (Erişim Tarihi 13.05.2018).

[45] TÜRKAY, **2015**, s. 51-52.

[46] ÇAKAN, **2013**, s. 204.

Aralık 1948 tarihli ve 217 A(III) sayılı kararı ile kabul edilen 1948 tarihli *Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi*'nin özel yaşamı koruyan 12. maddesi ile 19 Aralık 1966 tarihinde 2200 A (XXI) sayılı kararla kabul edilen *Kişisel ve Siyasal Haklar Sözleşmesi*'nin mahremiyet hakkını koruyan 17. maddesi dolaylı yoldan hassas kişisel verileri koruma altında tutan sınır ötesi hukuki metin örnekleri arasında sayılabilir.

Türkiye'de kişisel verilerin korunması bakımından temel norm niteliğiyle anayasal düzeyde ilk düzenleme 12.09.2010 tarihinde yürürlüğe giren 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanunla gerçekleşmiştir. "*Özel hayatın gizliliği*" başlıklı 20/2. maddede, hassas kişisel veriler vurgusu yapılmadan kişisel verilerin korunması yönünde düzenleme yapıldığı görülmektedir. Genel bakış açısıyla bir bütün olarak irdelendiğinde, Anayasanın 2. maddesindeki "Hukuk Devleti" ilkesi, "*Temel hak ve hürriyetlerin niteliği*" başlıklı 12. maddesi, 17. madde ile güvence altına alınan "Kişi Dokunulmazlığı, Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı", "Kişi Hürriyeti ve Güvenliği"ni düzenleyen 19. madde, 21. maddede geçen "Konut Dokunulmazlığı" hakkı, 20. ve 22. maddelerde düzenlenen "Özel Hayatın Gizliliğinin Korunması Hakkı" ve "Haberleşme Hürriyeti", "*Din ve vicdan hürriyeti*" başlıklı 24. madde ile "*Düşünce ve kanaat hürriyeti*"ni düzenleyen 25. madde[47], özel nitelikli verilere de teşmil edilebilecek kişisel verilere yönelik koruma sağlayan temel hükümler niteliğindedir.

Anayasal hükümlerin ardından Türk pozitif hukuk düzenlemesi kapsamında münhasır ilk kanunlaştırma hareketini temsil eden 6698 sayılı Kanun'un 6. maddesinde hassas veriler, ***özel nitelikli kişisel veri*** kavramıyla karşılanmış ve madde, içerdiği istisna hükümleriyle verilerin işlenme şartlarına bütünsel bir bakışla açıklık getirmeye çalışmıştır. Daha genel nitelikte olmak üzere 5237 sayılı Türk Ceza Kanununun kişisel verileri doğrudan veya dolaylı koruyan hükümleri ise özel hayata ve hayatın gizli alanına karşı suçlar bölümünde 132-140. maddeler arasında düzenlenmiştir.[48] Kanunun "*Özel hayatın gizliliğini ihlal*" başlıklı 134. maddesinde kişilerin özel hayat gizliliğinin ihlaliyle özel hayata ilişkin görüntü veya seslerin hukuka aykırı

[47] AYDIN, Sedat E., **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2015, s. 58-64.

[48] BÜK, Alaattin, **Bilişim Alanında Kişisel Verilerin Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2018, s. 82.

olarak ifşasının cezai yaptırım gerektiren fiiller kapsamında değerlendirilmesi, kişisel verilerin hem bağlantı kurulan pozitif hukuk kaynağını hem de suç tanımını gösteren önemli bir düzenleme niteliğindedir.

Korunan hukuki değerin özel hayat olarak belirlendiği kişisel verilerin kaydedilmesi başlıklı 135. maddede suç tipi kişisel veri tanımı açısından belli bir açıklık taşımasa da[49] maddenin ikinci fıkrasında daha kesin olarak hukuka aykırı yollarla kişisel verileri kaydeden kimseye verilecek hapis cezasının tayin edilmesinde suç olgusuna konu kişisel verinin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda ceza yönünden ağırlaştırıcı sebep öngörülerek kişisel veriler arasında uluslararası eğilimi yansıtan özel bir yasal kategori oluşturulmuş ve hassas veriler bu yasal himaye içine yerleştirilmiştir. Madde içeriği, hassas veri kategorisinde ağırlaştırıcı sebep düzenlemesi öngörerek nitelikli suç tavsifi yoluyla önemli bir bilinçlilik durumu ortaya koyabilmiştir.

Dikkat çekici diğer bir farklı durum 6698 sayılı Kanun'un "*Özel nitelikli kişisel veri*" başlığıyla 6. maddede düzenlediği veri türleri içinde yer almayan ahlaki eğilim[50] kavramının hassas kişisel veri kategorisine dâhil edilmiş olmasıdır. Kanun'da düzenlenen *kılık, kıyafet, dernek ve vakıf bilgileri ile ceza mahkûmiyeti ve güvenlik tedbirlerine* ilişkin veriler ise ceza kanununun zikredilen maddesinde hassas veri statüsünde sayılmamıştır. Dolayısıyla genel bir kıyaslama yapıldığında 6698 sayılı Kanun'un, özel nitelikli kişisel verileri ceza kanunu hükmüne göre daha ayrıntılı bir yaklaşımla düzenleme eğilimi içinde olduğu ifade edilebilir. Kılık, kıyafet, dernek ve vakıf bilgileri, ceza mahkûmiyeti ve güvenlik tedbirleri ile ahlaki eğilim verileri arasında iki yasal düzenleme bakımından farklılık arz eden bu normatif yaklaşım, kanunlar arasındaki hassas veri türleri karşılaştırmasında uyumsuzluk doğurmasının yanısıra hangi hukuksal ölçütlere ve menfaat önceliğine göre seçim yapıldığını anlamak açısından da güçlükler yaratmaktadır. Bu nedenle, TCK

[49] ÖZBEK, Veli Ö./ BACAKSIZ, Pınar/ DOĞAN, Koray, vd., **Türk Ceza Hukuku Özel Hükümler**, 12. Baskı, Seçkin Yayıncılık, 2017, Ankara, s. 569.

[50] Bu veri türü mevcut kavram itibariyle uluslararası belgelerde yer almamaktadır. KÜZECİ, 2018, s. 351. Ahlaki eğilimin TCK'nın "Genel Ahlaka Karşı Suçlar" bölümünden hareketle toplumun genelinin kınadığı özellikle cinsellik içeren davranışlara yönelik bir anlam taşıdığı belirtilmiştir. BÜK, **2018**, s. 39.

hükmünün 6698 sayılı Kanun maddesinde düzenlenen özel nitelikli veri türlerini esas alması ve aynı doğrultuda bir norm standardının yakalanması gerektiği haklı bir hukuksal öneri olarak öne sürülmüştür.[51]

Ceza muhakemesi ve ceza kanunu normlarının farklı hükümleri çerçevesinde konuya yaklaşıldığında ise kişisel verileri hukuka aykırı biçimde başkasına verme, yayma veya ele geçirme eylemlerinin yer aldığı 136. madde ile kanunların belirlediği süreler geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemeleri fiilini suç olarak düzenleyen 138. madde hükümleri, özel veri kategorisine mahsus olmayan ancak genel kişisel veri güvenliği alanında koruma getiren yasal kurallar niteliğindedir. 5271 sayılı Ceza Muhakemesi Kanununun "*Gözlem altına alma, muayene, keşif ve otopsi*" başlıklı 3. bölümünün genetik inceleme sonuçlarının gizliliği ile ilgili 80. maddesinde de, 75, 76 ve 78. maddelere atıfla kişinin kan, saç, tükürük, tırnak veya benzeri biyolojik örnekleri, cinsel organlar veya anüs bölgesi muayene sonuçları ile moleküler genetik incelemeye ait bilgileri, özel kişisel veri kapsamında sıralanmış; bu verilerin başka bir amaçla kullanılamayacağı ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına aktarılmayacağına ilişkin yasak alanlar ihdas edilerek sınırlı alanda belirlenen hassas kişisel veriler özel bir koruma rejimiyle yasal çerçeve içine alınmıştır.

Özel kişisel verilerle ilgili farklı bir yasal kaynak olan 5502 sayılı Sosyal Güvenlik Kurumu *Kanunu'nun* "*Kurumun taşınmaz edinimi, taşınır ve taşınmaz mal varlıkları ile gayri maddi haklarının hukuki durumu*" başlıklı 35. maddesinde kişisel veriler ile ticari sır niteliğindeki bilgilerin veri sahibinin noter onaylı muvafakatiyle gerçek veya tüzel kişilerle paylaşılabileceği ancak sağlık verisinin bu yetkinin dışında olduğu hükmü öngörülerek münhasıran bu alanda diğerlerinden ayrılabilen özel vasfa sahip bir hassas veri kategorisinin tanındığı belirtilmiştir.

4721 sayılı Türk Medeni Kanunu'nun "*kişiliğin korunması*" başlıklı 23-25. maddeleri ile 6098 sayılı Türk Borçlar Kanunu'nun 58. maddesi konuyu dolaylı olarak kişilik haklarını koruyucu hükümler kapsamında değerlendirirken 4857 sayılı İş Kanunu'nun "*işçi özlük dosyası*" başlıklı 75. maddesi işverenin, istihdam ettiği her işçi için düzenlediği özlük dosyasında işçinin kimlik bilgilerinin yanında, her türlü belge ve kayıtları saklamak ve

[51] ÖZBEK, Veli Ö./ BACAKSIZ, Pınar/ DOĞAN, Koray, vd., **2017**, s. 579.

bunları istendiği zaman yetkili makamlara göstermek zorunda olduğu ve işverenin işçi hakkında edindiği bilgileri dürüstlük kurallarına ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlü bulunduğu hususlarını hükme bağlayarak hassas veri tanımı içine girecek veri parçaları için özel idari önlemler geliştirmiştir.[52]

Genel bir perspektifle değerlendirildiğinde, pozitif hukuk düzenlemelerinin kişisel, toplumsal ve iktisadi tüm alanları kuşatma eğilimi taşıdığı, kamu ve özel hukuk hükümleri tarafından yasal ve kurumsal garantiler sunularak özel kişisel verilerin koruma şemsiyesi altına alınmak istendiği fark edilmektedir. Yasal metinlerde kamu düzeni, üstün kamu yararı, yasal yetki kullanımı, kişisel rıza, veri güvenliği ve kişilik hakları arasında menfaat dengesinin kurulmaya çalışıldığı görülmekle birlikte hassas veri türleri bakımından hukuksal düzenlemeler arasında türdeşlik olmaması ve hassas kişisel verilerin kendisini oluşturan unsurlar yönünden objektif bir tanım içine alınamaması, pozitif hükümlerin tüm olumlu yanlarına rağmen hassas veri tespiti konusunda ciddi uygulama zorlukları ve çelişkileri doğurmaya aday açık noktalar oluşmasına yol açmaktadır.

Özel Nitelikli Hassas Kişisel Verilerin Korunması Hakkının Yöneldiği Amaçlar

Ulusal ve uluslararası hukuk metinlerinde özel düzenlemelere konu edinilen ve işlenmesi belirli prosedürlere bağlanan hassas verilerle ilgili yasal statünün temel amacı, hak ve özgürlükleri yaşanılır kılma hedefine yönelik olarak insan onurunun korunması ve kişiliğin serbestçe geliştirilmesi[53] hakkını güvence altına almaktır. Diğer bir amaç kişisel bilgi varlığı içinde önemli yer tutan özel nitelikli veri girdilerinin kişinin nüfuz ve etki alanından çıkarılarak yetkisiz kişilerin erişimine açılması[54] sonucunda doğacak maddi ve manevi zararlardan bireyi korumak ve hassas veriler için etkin, meşru ve geçerli bir yasal himaye mekanizması oluşturmaktır.

[52] KAYA/TAŞTAN, **2018**, s, 210-212;224-227;234.

[53] AYM, E. 2015/61, K. 2016/172, K.T. 2.11.2016.; E. 2015/32, K. 2015/102, K.T. 12.11.2015.; E. 2014/180, K. 2015/30, K. T. 19.03.2015; E. 2014/2242, K. 2015/4991, K.T. 9.12.2015.

[54] KETİZMEN, Muammer/ÜLKÜDERNER, Çağlar, **E-Devlet Uygulamalarında Kişisel Verilerin Korunma(ma)sı**, s. 2, http://inet-tr.org.tr/inetconf12/bildiri/2.pdf (Erişim Tarihi 11.05.2018).

Hassas kişisel verilerin hukuksal açıkların doğurduğu denetimsiz ve ölçüsüz yaklaşımlarla kamuya açık hale gelmesi, içsel planda kişinin özel ve aile yaşamını, kamusal yaşamda ise bireyin toplumsal konumunu ve iş ilişkilerini olumsuz yönde etkileyen bir sosyal tehlikelilik durumu ortaya çıkarır. Bu nedenle toplum üyelerince kınanma, damgalanma ve lekelenme gibi informal cezalandırma süreçlerinin tetiklenmesine[55] bağlı olarak bireyin gelecek planlamasını ciddi oranda zedeleyecek etki ve sonuçları yok etmeye dönük veri güvenliği politikaları geliştirmek, özellikle temel hak ve özgürlükler rejiminin korunması bakımından kamu otoritelerince bir gereklilik olarak değerlendirilmektedir.

Özel hayatın korunması ve kişi güvenliğinin sağlanması ile hassas verilerin işlenmesi ikileminde veri merkezlerinde muhafaza edilen bilgilerin sebep olacağı psikolojik sonuçların olumsuz etkileri, başta Avrupa İnsan Hakları Mahkemesi olmak üzere uluslararası boyutlu dava süreçlerine ve yoğun içtihat oluşumuna kapı aralamıştır. İlk etapta Avrupa İnsan Hakları Sözleşmesi'nin "*Özel ve aile hayatına saygı hakkı*" başlıklı 8. maddesi kapsamında cinsel kimliğin belirlenmesi, cinsel eğilim ve cinsel yaşam gibi unsurlar, sağlığa ilişkin veriler, etnik kimlik ve görüntü hakları bireyin fiziksel/sosyal kimliğine dair özel hayat göstergeleri olarak kabul edilmiş;[56] devamında etnik ya da ırksal köken, politik görüşler, dini-felsefi inançlar ve sendika üyeliği ile ilgili veriler otomatik işleme fonksiyonu açısından yasak hükümler sınırı içinde tutulmuştur.[57]

Demokratik bir ülkede Anayasa ile güvence altına alınan temel hak ve özgürlüklere yönelebilecek saldırı ve tehditlerin karşısına hassas kişisel veri düzenini çıkarmanın temel gerekçesi, diğer kişisel verilerin etki düzeyine kıyasla bireyin toplumsal saygınlığını korumaya yönelik önlemler setinin hassas veriler korunmasıyla daha da sağlamlaştırılacağının varsayılmasıdır. Bireyin, yaşamsal önem taşıyan haklar düzleminde alenileştirilmiş olsa dahi özel nitelikli kişisel verilerin kullanımına yön verme yetkisi bu nedenle öncelikli koruma konusu yapılarak güvence altına alınmıştır.[58]

---

[55] KÜZECİ, **2018**, s. 256.

[56] Avrupa İnsan Hakları Mahkemesinin *S. ve Marper/Birleşik Krallık Davası (Başvuru No.30562/04 ve 30566/04)*, s. 19, 21.

[57] ZERDİCK, **1995**, s. 67.

[58] BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması**, 1. Baskı, Yetkin Yayınları, Ankara, 2004, s. 45; TÜRKAY, 2015, s. 29.

Bilgisayar sistemlerinin kullanımı ve internet teknolojisinin anlık popüler aktarım gücü veri koruma sorununu her zamankinden daha önemli hale getirdiğinden hassas kişisel verilere yönelik koruma düzeyinde farklılıklar yaratılması veya bu tür verilerin güçlendirilmiş hukuksal rejime tabi tutulmak istenmesi kaçınılmaz bir toplumsal ve beşeri gereklilik kavrayışıyla hukuksal düzenlemelere yön veren ana motivasyonu teşkil etmiştir. Dolayısıyla hassas kişisel verilerin elde edilmesinden beklenen yarar ile anayasal temel hakların korunması bakımından doğması muhtemel riskler arasında denge kurma arayışı hukuksal rejim farklılaşmasının temel sebebidir. Aynı zamanda çıkarların dengelenmesi veya bir işlemin hukuka uygunluğunun saptanması adına veri konusu ile veri kullanıcısının menfaatlerinin birbirlerine karşı ağırlıklandırılması, uygulama açısından meşru temeller elde etmede önemli bir beklentiyi oluşturur.[59] Çeşitli kuruluşlar ve ülkelerce kişisel bilgilerin korunması için gizlilik düzenlemeleri yayınlanması, hassas kişisel verilerin açıklanmasının istisnai durumlara özgülenmesi, verilerin birleştirilmiş veya anonimleştirilmiş formlar kullanılarak sağlanmaya çalışılması, detaylı veri güvenlik politikaları geliştirilmesi, adil bilgi uygulamalarının yaygınlaştırılması (fair information practices-FIP) ve bilgi paylaşım standartlarının saptanması sözü edilen denge arayışına yanıt bulma çabalarının somut birer yasal-kurumsal örnekleri niteliğindedir.[60]

Açıklanması halinde ayrımcılık duygularını diğer kişisel verilere göre daha çok kışkırtacak olması ve ortaya çıkaracağı zararın büyüklüğü hassas verileri özellikli ve koruma öncelikli hukuksal varlıklar haline getiren önemli bir etkendir. Ancak hangi verilerin bu kapsamda değer kazanacağını belirginleştirmek bir hayli güçtür. Zira toplumsal koşulların değişmesi ve sosyal gelişmişlik seviyesi işlendiği zaman özel önem atfedilmeyen bir bilgiyi sonradan hassas veri kategorisinde nitelendirmeyi gerekli kılabilir. Bağlamsal (contextualised) yaklaşımı yansıtan bu görüş taraftarlarına göre, verilerin işlenmesi ve kullanılmasının gerçekleştiği şartlar, değişen toplumsal, ekonomik ve kültürel konjonktürün dönüştüreceği kişisel algı düzeyi dikkate alındığında özel nitelikli verileri mutlak sınıflandırma iddiasından

[59] ZERDİCK, **1995**, s. 67.

[60] EFRAİMİDİS Pavlos S./DROSATOS Georgios/NALBADİS Fotis, vd., "Towards Privacy in Personal Data Management", **İnformation Management & Computer Security**, Yıl: 2009, Cilt: 17 Sayı: 4, s. 310.; COOPER Daniel P. "İnvestigations: Understanding Data Privacy", **Journal of Financial Crime**, Yıl: 2005, Cilt: 12, Sayı: 4, s. 354.

uzaklaştırabilecek bir görecelilik durumu ortaya çıkarır. Dolayısıyla verinin elde edildiği koşullar, toplanma amacı, işlenmesinin ilgili kişiler bakımından doğuracağı muhtemel sonuçlar, veri kütüğü sahiplerinin menfaatleri ile veri bankasının potansiyel alıcıları gibi etkenler göz önünde bulundurularak hassas veri kavramına çok yönlü parametrelerle açıklık getirilmesinin gerekli olduğu savunulmaktadır.[61]

Bu aşamada kişisel verinin hassasiyet derecesinin tespitinde, işlenen verilerle doğması muhtemel yarar-zarar arasında kişi-kamu boyutlu belirli denge hesaplarının yapılması mutlak bir gerekliliğe işaret eder. Koruma düzeyini içeren yararın derecesi ile tehlikenin boyutlarının kıyaslanması kaçınılmaz bir kamusal yükümlülük olarak göz önünde bulundurulur. Amaçsal (purpose-based) yaklaşıma göre ise, bir verinin hassas nitelikte olup olmadığını belirleyen ana ölçüt, işlenme amacında saklıdır. Hassas veriyi paylaşma ve açıklamada kullanılan kamusal gerekçe, işlemenin amacını belirlemede önemli bir gösterge olarak kabul edilir.[62] Örneğin kamu idareleri ve kurumları kamu düzenine yön vermek, vergi yükümlülüğünün etkin şekilde yerine getirilmesini sağlamak, refah politikaları tasarlamak ve kamu hizmetlerinde verimliliği elde edecek etkili bir yapılanma gerçekleştirmek; özel teşebbüsler ise organizasyonel başarıya ulaşmak, insan kaynakları politikası oluşturmak, verimlilik ve karlılık prensiplerini gözeten bir vizyon inşa etmek amacıyla dijital veri tabanlarında düşük maliyet ve emeğe dayalı pratik yollar deneyerek kişisel bilgileri işleme ve analiz etmeyi tasarlayabilir. Bu süreçte her iki tüzel kişilik temel hak ve özgürlükler alanında ihlaller doğuracak hukuki sorun ve açıklar yaratabilirler. Sürekli izlendiği, politik veya kişisel eğilimleri ile sağlık bilgilerinin elde edildiği endişesiyle başkalarının kontrolü altına girdiği duygusuna kapılan bireyin temel hak ve özgürlüklerini kuşku duymadan kullanacağını bu caydırıcı şartlarda ileri sürmek pek mümkün görülmemektedir.[63] Özellikle kişinin ırksal veya etnik kökeni, politik görüşleri, dini-felsefik inançları, sendika üyeliği, sağlık veya cinsel hayatı ile cezai suçlar kapsamındaki bilgilerinden oluşan hassas kişisel veriler, işlenme ve ifşa sürecinde güvenlik şartları ve gizlilik prosedürleri vasıtasıyla

[61] AKSOY, Hüseyin C., **Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Ankara, Üniversitesi Sosyal Bilimler Enstitüsü, 2008, s. 45-46.

[62] AKSOY, 2010, s. 46.

[63] KORKMAZ, İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 1.Baskı, Seçkin Yayıncılık, Ankara, 2017, s. 58.

daima kontrol altında tutulmazsa özel hayatın korunması kuralına aykırı telafisi güç zararlar ortaya çıkabilir. Kaldı ki yargı kararlarında da vurgulandığı gibi[64] prensipte herhangi bir kişisel verinin işlenmesini kapsayan yetki veya talep, özel hayatın gizliliğine ilişkin temel hakkın önüne geçen üstün ve meşru bir çıkar alanı ve hukuksal saygı küresi ortaya çıkarma gücünden her durumda yoksun sayılmalıdır.

Tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin hassas verilerin teknik önlemler alınmadan kaydedilmesi, kanun önünde eşitlik prensibi gereğince kamu hizmeti sunumunda önyargılar ve adil olmayan uygulamalar doğurabileceği gibi bireyin hizmete erişimden uzaklaşmasına neden olacak mahsurlar da ortaya çıkarabilir. Hassas veriler konusundaki ülke düzenlemelerinin sivil zararların giderildiği adil bir hukuk politikasına göre şekillenmesi eğilimi, temelde özgürlük-güvenlik dengesindeki kamusal endişelerin minimuma indirgenmesi amacına yöneliktir.[65] Gizlilik ve hassas verilerin işlenmesi arasındaki yakın ilişki aynı nedenle kişisel menfaatler, özel yaşam, demokratik katılım, bedensel bütünlük, aile hayatı ve evin kutsallığı üzerine kurulu hukuksal menfaatleri içeren geniş bir meşruiyet zemini ve çoklu değerler üzerinde etkileşim içinde bulunmaktadır.[66]

Hassas kişisel verilerin korunmasına yönelik sıkı kurallar öngörülmesini gerektiren en geçerli sonuçlar, cinsel ve sağlık verileri alanından örneklendirilebilir. Özel yaşamın merkezini teşkil eden bu bilgilerin herhangi bir kayıt ve şarta tabi tutulmadan ifşa edilmesi durumunda kişinin tedavi sürecinin devamı ve sosyal hayat içinde ayrımcı tutum ve davranışlara maruz kalması ciddi riskler arasındadır.[67] Bireylerin veya yetkisiz kurumların eline geçmesi halinde veri öznelerinin şantaj ve tehdide maruz kalabilecekleri, iş güvencesinin zarar göreceği yönündeki haklı endişeler, hassas verilerin farklılaştırılmış bir rejim içine alınması zorunluluğunu ortaya çıkaran yaygın gerekçeleri teşkil etmektedir. [68] Dolayısıyla hassas veri kategorileri aracılığıyla inşa edilen

[64] İstanbul BAM 23.H.D. E. 2017/596, K. 2017/527, K.T. 31.3.2017.; D.15.D. E. 2016/10500, K. T. 6.7.2017.

[65] COOPER Daniel P., **2005**, 352-354.

[66] PURTOVA, Nadezhda, "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights", **Netherlands Quarterly of Human Rights**, Yıl: 2010, Cilt: 28 Sayı: 2, s. 181.

[67] GÜRSEL, **2016**, s. 48-49.

[68] AKSOY, **2010**, s. 48-49.

koruma hakkı öncelikle, kişinin mesleki ve gündelik yaşamında belirebilecek risklerden olabildiğince azade kılınmasını sağlama işleviyle tezahür eder. Bu fonksiyonun arka planında güçlü gözetim ve veri yönetimi araçlarının yaygın kullanımı başlıca caydırıcı etkeni meydana getirir. Elektronik dünyadaki önemli sorunlardan birinin kişisel verilerin özel hayat güvenliği aleyhine ağ dolaşımı ve dijital ortam hareketliliği içinde kazandığı etkinlik olduğu dikkate alındığında yeni hukuksal paradigmaların, bireylerin kişisel veriler üzerindeki kontrolünün geliştirilmesi etrafında yoğunlaşma göstermesine şaşırmamak gerekir.[69]

Bilgisayar teknolojisi ile internet dünyasının sürüklediği ve demokratik değerlerin geri plana itildiği gözetim toplumuna karşılık özel hayat alanının korunması gereğine yapılan vurgu, birey özerkliği ve bireyin yalnız bırakılma hakkıyla veri güvenliğini aynı hukuksal menfaat zemininde bir araya getirmiştir. Hak sahibi, mevcut hukuksal birleşme içinde gözetim teknolojileri, bilişim araçları, merkezi veri bankaları ve bu enstrümanların oluşturmak istediği dijital kişiliklere karşı kişisel veri dizileri üzerinde kontrol imkânını sağlayan güvencelerle donatılmak istenmiş; izleme, gözetleme ve verilerin takibi ürünü olan kişisel bilgilerin hukuki sebepler olmaksızın toplanmaması, işlenmemesi ve transferinin yapılmaması ile yetkisiz kişilerin erişimine kapatılması yönündeki talepler, hassas verilerin korunması haklarının yöneldiği merkezi amaçları ifade eder hale gelmiştir.[70]

Özellikle hassas kişisel verilerin kapsamlı bir şekilde sürekli kaydedildiği, resmi veya özel otoritelerin elinde öngörülemeyecek birtakım işlemlere araç kılındığı kaygısının birey tarafından hissedildiği negatif toplumsal ve psikolojik algı ortamında kişiliğin sağlıklı gelişim göstermesini beklemek demokratik toplumun geleceği açısından ciddi güven açıkları ve sosyal öngörülemezlik anlamı taşır. Kişinin kendini geliştirme olanaklarını kullanma hakkına kısıtlamalar getirmesi veya kamu hizmetlerinden yararlanmada duyacağı tedirginlikle otolimitasyona yönelmesi, hassas kişisel veriler üzerinden doğabilecek muhtemel ve yakın risklere örnek olarak verilebilir.[71] Bu nedenle hassas verilerin toplanması, işlenmesi veya erişime açılması işlemleri yapılırken, özel önlemler ve koruma tedbirleri alınarak veri konusunu gönüllü, özel ve bilgiye dayalı göstergelerle desteklemek gerekmiş;

[69] EFRAİMİDİS/DROSATOS/NALBADİS vd., **2009**, s. 316.

[70] TÜRKAY, **2015**, s. 31-32.; KORKMAZ, **2017**, s. 59.

[71] KORKMAZ, **2017**, s. 70; KÜZECİ, **2018**, s. 256.

rıza sorunlarının çözümlenmesi veya işlemlerin sıkı kurallara tabi tutulması işlem güvenliği ve hukuksallık ilkeleri uyarınca uyulması gereken standart prosedürler olarak kabul edilmiştir.[72]

Ulusal çapta ise 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun meclise sevk edilen genel gerekçesinde kanunun kabul edilmesi sürecinde birçok faktörün etkili olduğu belirtilerek veri koruma alanında daha ziyade kamusal etken ve gerekçelerin kaynaklarına değinilmiştir. Avrupa Birliği tam üyelik sürecinde müzakere fasıllarından dördünün doğrudan ilgili olması nedeniyle sürecin ilerleyebilmesi için kişisel verilerin korunmasına ilişkin temel bir kanunun yürürlüğe girmesi yönündeki beklenti ve birliğin Türkiye için hazırladığı ilerleme raporlarında veri koruma alanındaki kanuni boşluğa işaret edilmesi veri güvenliğine yönelik gerekçelerin dış dinamikler açısından güncel kaynaklarını göstermektedir.

Kişisel verilerin korunmasını içeren yasal bir düzenleme bulunmaması nedenine bağlı olarak polis birimleri arasında etkin işbirliğini hayata geçirmeyi amaçlayan EUROPOL ile Türk güvenlik birimleri arasında operasyonel işbirliği anlaşması yapılamaması, elektronik bilgilerin teati edilememesi bibi etkenlerin yol açtığı güvenlik boşlukları, kanun düzenlemesine duyulan aktüel ve acil ihtiyacı açıklamada pratik gerekçeler halinde sunulmuştur. Başka bir anlatımla istihbarat ve güvenlik alanındaki bilgi temini güçlüklerinin giderilmesine odaklanılması ile kamu düzeninin korunması ve suçla mücadele alanında hedef bazlı çabalara yoğunlaşma gösterilmesi, veri politikasının aynı zamanda kamusal eksenli talepleri öne alan bir tercihe yaslandığını göstermektedir. Benzer gerekçe, sınır aşan suçlarda değişik ülkelerin yargı mercilerinin ortak operasyonlar yapabilmesi için EURO JUST ile etkili bir işbirliği mekanizması kurulması amacı etrafında da kurgulanmıştır.

Türkiye'deki yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından askerlik, vatandaşlık, kimlik ve malvarlığı gibi konularda veri paylaşımında yaşanan sorunların aşılması, yabancı ve Türk sermaye girişimlerinin etkin bir şekilde yönetebilmesi için ihtiyaç duyduğu veri aktarımının kanuni çerçevesini oluşturmak ise medeni yaşama ilişkin ticari gereklilikleri ve ekonomik etkenleri yansıtan gerekçeleri oluşturmuştur. İşaret edilen ulusal ve küresel gerekçelerin hassas kişisel verileri de kapsayan tüm kişisel veriler için aynı doğrultuda referanslar oluşturduğu açık olarak görülmektedir.

[72] TRANBERG, **2008**, s. 394.

Kanuni yaklaşım genel kişisel veri etrafında kurgulanmış olsa da kanunun tümüne yönelik oluşturulan gerekçede istisnai olarak yalnızca sağlık verileri bağlamında hassas kişisel veri örneğine yer verildiği dikkati çekmektedir. Bu kapsamda hastalara yönelik sağlık kuruluşlarında tutulan çok sayıda özel nitelikli verilere ilişkin kanuni dayanağın olmaması, veri güvenliğinin sağlanmasına hizmet eden yeterli önlemlerin alınmaması ve yetkisiz kişilerce bu nitelikteki bilgilerin ifşa edilmesi eylemleri, Avrupa İnsan Hakları Mahkemesinde ihlal kararları verilmesine ve hukuksal maliyetler doğmasına yol açan ulusal hukuk boşlukları olarak gerekçede dile getirilmiştir. Dolayısıyla yalnızca muayyen bir konudan hareket edilerek hassas veri kavramına atıfta bulunulmuş ve diğer hassas veri türlerine değinme gereği duyulmamıştır. Hassas verileri düzenleyen madde gerekçesinde ise doğrudan bir tanım yapılmamakla birlikte özel kişisel veri normuna yönelik amaçlar ile yapılan kavramlaştırmanın nedenleri üzerinde durularak verilerin işlenmesine dair sınırlı durumlar örnekler eşliğinde açıklanmaya çalışılmıştır.[73]

Özel Nitelikli Hassas Kişisel Verilerin Korunması ve İşlenmesi Hakkının Kapsamı ve İstisnaları

Kişisel verilerin işlenmesi, pozitif hukuk düzenlemelerine yansıyan kural ve yargısal kararlara[74] göre otomatik ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan araçlarla gerçekleşir. İşlenmesi aşamasında kişisel verilerin geçirdiği işlem süreçleri ise 6698 sayılı Kanun'un 3/e maddesi ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) 'Tanımlar' başlıklı 4/2. maddesinden hareket edildiğinde, veri öznesine (data subject/ilgili kişi/kişisel verisi işlenen gerçek kişi) ait kişisel verilerin veya veri setlerinin elde edilmesi, kaydedilmesi, düzenlenmesi, yapılandırılması, muhafaza edilmesi, değiştirilmesi, uyarlanması, yeniden düzenlenmesi, açıklanması, yayılması, erişilebilir kılınması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması, birleştirilmesi, kısıtlanması, veri kombinasyonunun sağlanması, anonim hale getirilmesi veya kullanılmasının engellenmesi/bloke edilmesi gibi elektronik veya fiziki veri kayıt sistemi içinde farklı boyut ve konu alanlarını içeren işlemler dizisinden oluşmaktadır.

Çeşitli hukuk sistemleri hassas kişisel veri elde edilmesi ve işlenmesi işlemlerinde ilgili kişinin rızasını, yaşamsal nitelikteki kamu çıkarlarının

[73] http://www2.tbmm.gov.tr/d26/1/1-0541.pdf (Erişim Tarihi 13.05.2018).

[74] Y.12.H.D. E. 2016/59. K. 2016/68, K.T. 13.10.2016.

korunmasını, bizatihi hak sahibinin verileri paylaşmasını ve doğabilecek yargılama sebeplerini kaynak-sebep olarak kullanmıştır.[75] Hukuksal izin ve olanakları denetlemek, hak sahipleri arasındaki olası çıkar çatışmalarını önlemek, tüm bireyler için eşit koruma sağlamak ve tarafların sahip olduğu hakları doğru nitelendirmek için ayrıca hassas verilerin işlenmesinde **kesinlik** (finality), **orantılılık** (proportionality), **rıza** (consent) ve **çıkarların tartılması veya ağırlıklandırılması** (the weighing of interests) kriterlerinden hareket edilerek güvenli veri elde edilmesi ve sınırlama nedenlerinde belirli bir denge noktasına ulaşılması hedefleri gözetilmiştir.[76]

Uluslararası hukuk metinlerine de konu olan denetim ve sınırlama kavramlarından *kesinlik*, verilerin toplanmasının açık, spesifik, meşru amaçlara uygun olmasını ve sonraki herhangi bir işlemin başlangıçta belirtilen amaçlarla uyumsuzluk göstermemesi gerektiğini belirtir. *Orantılılık*, işlenen verilerin toplandığı amaca ulaşmak için gerekli olandan daha fazlasını içerip içermediğine dair somut bir değerlendirme yapılmasını öngörür. *Rıza* ilkesi, çıkarların dengelendiği ortamda veri öznesi olan kişinin, verilerin işlenmesini gönüllü kabul ettiğini gösteren özel ve bilgiye dayalı izni ifade eder. *Çıkarların tartılması/ağırlıklandırılması* ise somut değerlendirme ve göstergelerden hareketle, veri işleme eyleminin veri konusu çıkarlardan üstün tutulmasını gerektiren sebepler ile amaç için gerekli olduğunu gösteren etkenlerin ortaya konulması faaliyetini tanımlar.[77]

Tanımı yapılan kavramlardan hareketle verilerin adil ve yasal süreçler çerçevesinde işlenmesi, açık, meşru ve ilan edilen ilkelerle uyumlu bir veri işleme faaliyetinin sağlanması, işlenme amaçlarıyla bağlantıyı koparan gereksiz veri elde edilmesinden kaçınılması, doğru, güncel ve eksiksiz bir veri kaydı tutulması ile verilerin kişisel form içinde gereken sürelerden daha uzun kullanımda tutulmaması yönünde belirli güvenceler içeren ayrıntılı amaçlar benimsendiği görülmektedir. Hassas verilerin elde edilmesinde işlem süreçlerini hukuk kuralları ve kamu yararına uygun normatif bir çerçeveye kavuşturmak hedefi ise sıralanan ilkelerin evleviyetle göz önünde tutulmasını gerektiren bir hukuki değer kavrayışı ve yükümlülüğüne işaret

[75] KORKMAZ, **2017**, s. 53, 57.

[76] TAYLOR, Mark j., "Data ProtectİIon,Shared (Genetic) Data and Genetic Discrimination", **Medical law İnternational**, Yıl: 2006, Cilt: 8, s. 68.

[77] TRANBERG, **2008**, s. 392-394.

etmektedir.[78] Vurgulanan hukuksal ölçütlere, daha geniş anlamda güvenlik ve gizlilik ile veri faydası arasında denge kurulması, gizlilik politikasının güçlendirilmesi için veri kümelerine ait özniteliklerin belirli değer aralıklarında kişi ve veri bazında genelleştirilmesi ile verilerin anonimleştirilmesi işlemleri eklenebilir.[79] 1960'lı yıllardan itibaren veri koruma ve işleme süreçleriyle ilgili hukuksal ve kamu düzeni irtibatlı bu tür garantiler sağlanması ve artan kurumsal ilgiye rağmen paradoksal olarak veri koruma ve gizlilik arasındaki ilişki konusunda hala bir uzlaşma sağlanamaması ve meşruiyet sınırlarının belirsiz yönler içermesi yönetsel kapasite gelişiminin henüz tamamlanamadığını gösterir.[80] Yine de değişmeyen olgu, hassas verilerin sisteme sınırlı ölçülerde kaydedilmesi eğilimi ile kontrol altında bir işleme politikasının benimsenmesi yönündeki yoğun kamusal taleptir.[81]

6698 sayılı Kanun'un "*Genel ilkeler*" başlıklı 4. maddesi belirtilen ilkelerin özüne uygun bir yaklaşım tarzı takip ederek kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilme kriterlerini öngörerek evrensel standartları gözetme eğilimini benimsemiştir.[82] Dolayısıyla genel kişisel veriler ile özel nitelikli hassas verilerin koruyucu yasal ilkeler bakımından eşitlenmeye çalışıldığı formal bir statü elde edilmiştir.[83] Aynı yaklaşımın anayasal düzeydeki güçlendirici

---

[78] TAYLOR, **2006**, s. 54.

[79] TAKCI, Hidayet/CANBAY, Pelin, "Kişisel Verilerin Korunmasında Öznitelik Tabanlı Gizlilik Etki Değerlendirmesi Yöntemi", **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi**, Yıl: 2017, Cilt: 32, Sayı: 4, s. 1303.

[80] PURTOVA, **2010**, s. 181.

[81] KAYA, **2011**, s. 324.

[82] Benzer bir düzenleme, 'Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.' Hükmünü taşıyan 5809 sayılı Elektronik Haberleşme Kanununun '*Kişisel verilerin işlenmesi ve gizliliğin korunması*' başlıklı 51. maddesinde yer almaktadır.

[83] Anayasa Mahkemesi de verilerin elde edilmesi ve kullanım süreçlerine ilişkin genel nitelikli ve ilkesel sayılabilecek ölçütler ortaya koymuştur. Buna göre, "Sisteme bilgilerin girilmesi, müdahaleye temel oluşturan meşru amaçları taşıma şartına bağlı olmalı ve söz konusu yasal düzenleme, hangi bilgilerin kayıt altına alınabileceği, hangi yetkililere iletilebileceği, böyle bir iletimin hangi koşullarda mümkün olabileceği ve

tezahürü, temel hak ve özgürlüklere yönelik sınırlamaların amaçla orantılı olarak Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gerekleri ile ölçülülük ilkesine aykırı olamayacağı, hak ve özgürlüklerin özlerine dokunulmayacağı yönünde Anayasa'nın 13. madde düzenlemesinde üst norm halinde yansıma bulmuştur.[84]

Hassas kişisel verilerin elde edilmesi ve işlenmesinde ayrıntılı teknik prosedür, hukuksal ilke ve normlar öngörülmesinde, uluslararası istikrar kazanmış uygulamaların teşvik ettiği özel hayatın korunması amacı ve bu çıkar alanına yönelik genel işlem yasağı kuralı önemli bir etken olmuştur. Kısmen Türk iç hukukuna da hâkim olan ayrıntılı kural ve prosedürel süreçlerin geliştirilmesinin arka planında, hassas verilerin işlenmesinde genel rıza ilkesi ve hukuka uygunluk sebeplerinin tek başına geçerli olmaması kaidesi yer almaktadır.[85] Veri türlerine göre işleme sebeplerinin farklılaşması da aynı istisnai rejim düzeni ve hukuksal statü ayrımının bir sonucudur.

6698 sayılı Kanun'un 6/2. maddesinde işleme bakımından hassas verilerin kural olarak tümü için açık rıza şartı öngörülmüşken bu iradenin yokluğu halinde bir kısım veriler için (sağlık ve cinsel hayat dışındaki kişisel veriler) kanunla öngörülme, sağlık ve cinsel hayat verileri için ise belirli şartların gerçekleşmesiyle oluşan farklı izin gerekçeleri sevk edilmiştir. Başka bir deyimle hassas kişisel verilerin tüm kategorilerde işlenmesi bakımından, kanunun tanımlar kısmında yer verildiği şekliyle (m. 3-1/a) belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan irade beyanı çerçevesinde ilgilinin açık rızası[86] verilerin işlenmesinde yasal koşul ve izin sebebi

---

bilginin ilgili makamlara iletilmesi hususunda izlenecek usul, açık ve ayrıntılı hükümler içermelidir. Söz konusu sisteme ilişkin düzenleme; bilgi toplama, kaydetme ve ilgili makamlarla paylaşma veya sair şekilde kullanma konusunda, yetkili makamlara tanıdığı takdir yetkisinin kullanılma tarzı ve alanı bakımından vatandaşlara yeterince öngörüde bulunma olanağı sağlamak durumundadır." B. NO. 2013/2941, K.T. 11.05.2016.

[84] AYM, E. 2014/180, K. 2015/30, K.T. 19.03.2015.

[85] ÖZDEMİR, Hayrunnisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, 1. Baskı, Seçkin Yayınevi, Ankara, 2009, s. 127.

[86] Rıza kavramı, 2018 tarihli Avrupa Birliği Genel Veri Koruma Tüzüğünün (GDPR) Tanımlar başlıklı 4/11. maddesinde 'Veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge' tanımlamasıyla daha ayrıntılı ifadelerle açıklanmıştır.

olarak yeterli kabul edilmiştir. Ancak başka kanunlarda öngörülmüşse sağlık ve cinsel hayata ilişkin kişisel veriler hariç kişinin açık rızası alınmaksızın da verilerin işlenmesi söz konusu olabilecektir. İşlenme bakımından kanuna dayalı hukuka uygunluk sebebine istinat ettirilen bu veriler, yasal düzenlemenin 6. maddesinde kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık-kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleri ile biyometrik ve genetik veri dizilerini içermektedir. Hassas veri evreninde istisna kapsamına alınan sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak *kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi* amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın ve diğer kanunlarda bir düzenleme şartına başvurulmaksızın kanunda sayılan hukuka uygunluk sebeplerine dayalı olarak işlenebilecektir. Yasal düzenlemenin mevcut şartlarda Anayasanın "*Temel hak ve hürriyetlerin sınırlanması*" başlıklı 13. maddesinde geçen '*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir.*' hükmüne ve "*Özel hayatın gizliliği*" başlıklı 20/3. madde düzenlemesine aykırılık oluşturduğu ifade edilebilir.[87]

Veri işleme ile ilgili farklı bir durum ise kanunun *kişisel verilerin yurt dışına aktarılması* başlıklı 9. maddesi çerçevesinde hassas verilere ilişkin koruma alanının genişletildiği düzenlemedir. Madde hükmüyle mevcut işleme koşullarıyla yetinilmeyerek kişisel verinin aktarılacağı yabancı ülkede yeterli koruma önlemlerinin alınması, bu şartın sağlanmaması durumunda Türkiye'de ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmesi ve kişisel verileri koruma kurulunun izninin bulunması gibi ek koşullar aranmıştır.

Genel anlamda pozitif düzenlemenin hassas veri seçimi ve işlenme sürecini sağlık ve cinsel hayat verileri ile diğer veriler arasında ayrım yaparak kural haline getirdiği ve buna göre oluşturduğu veri grupları aracılığıyla yasal statüyü kurguladığı görülmektedir. Koruma alanının ulusal ve uluslararası düzeylerde belirlendiği bu sistematik yapıda yasal ölçütlerin gerekliliği ve seçimine ilişkin nedenler ile kamu yararı düşüncesiyle açıklanabilecek yeterli ve açık kamusal gerekçelerin tam anlamıyla ortaya konulamadığını belirtmek

[87] KÜZECİ, **2018**, s. 353.

gerekir. Yine de düzenlemenin mefhumu-u muhalifinden çıkan olumlu ve kesin bir sonuç, idari düzenleyici işlemler vasıtasıyla hassas kişisel verilere ilişkin herhangi bir işleme ve kayıt sebebine dayanılamayacak olmasıdır.

Kanunilik prensibine uygun hukuksal güvencelere karşın sağlık ve cinsel hayat dışındaki kişisel verilerin işlenmesi bakımından hukuka uygunluk sebebi olarak kanunun emrini yerine getirme ölçütünün vaz edilmesi ve diğer hassas veriler için özel hukuksal durumların işlenme sebebi olarak benimsenmesi kanunun tekelciliği prensibine göre kısmen hukuksal güvence sağlasa bile özellikle sağlık ve cinsel hayat verileri yönünden geniş yetkili bir idari müdahale alanı yaratılması nedeniyle en azından belirlilik ilkesine uygun bir düzenlemenin yapıldığını aynı kesinlikte öne sürmek mümkün görülmemektedir. Bunun dışında düzenleme sistematiği açısından 5237 sayılı Kanun'un 135. maddesine koşut olarak 6698 sayılı Kanun'da kişilerin siyasi, felsefi veya dini görüşleri ile ırki kökenleri temelinde mutlak; cinsel yaşam, sağlık durumu veya sendikal bağlantılar açısından ise hukuka aykırılık ölçütü vazedilerek nispi olmak üzere iki farklı koruma katmanı yaratılamamış tam aksine veri kaynakları açısından eş düzey bir hukuksal statünün ihdas edildiği çatışmalı bir yasal düzenleme ortaya konulmuştur. Kanunlar lehine herhangi bir değer yargısı ve tercih belirtme çabasına girmeden önce iki kanun arasında hassas kişisel veri kaynaklarının sıralanışı ve hukuki nitelendirme açısından verilerin işlenmesinde hüküm çatışması doğuracak ve uygulama çelişkilerine yol açacak özensiz bir düzenlemenin yapıldığını özellikle vurgulamak gerekir.[88]

Öne sürülebilecek diğer bir eleştiri noktası, özel nitelikli kişisel verilerin işlenme şartları başlıklı 6. maddenin küresel düzeyde kabul edilen hukuki düzenleme veya mevzuat metinlerine uygun olarak hassas veri türlerini tüketici nitelikte (numerus clausus) belirtmesi ve bu eğilimin sonucunda kanun kapsamında düzenlenmeyen verilerin kıyas yoluyla hassas veri içine dâhil edilemeyecek olmasıdır. Hassas kişisel veri sabitlemesi kanunilik ilkesi için uygun hukuksal zemin oluştursa da yasal düzenlemenin mantığı, değişen toplumsal koşulların hassas veri addedilmesini gerektirdiği yeni veri dinamizmine aynı ölçülerde tatmin edici bir yanıt vermekten uzaktır. Bu durumu yansıtan yerinde bir eleştiri noktası, daha önce Avrupa Birliği Yönergesi düzenlemesine getirilen itirazlara benzer şekilde kişiliğin değişik görünümlerini açığa çıkaracak finans ve yer bilgilerinin hassas veri

[88] BÜK, **2018**, s. 83-85.

kategorisinde sayılmaması, önem ve hassasiyet derecesi azımsanmayacak değerde olan kişisel verilerin özel koruma mekanizmasından yasal olarak yoksun bırakılmış olmasıdır. Oysa bu tür bilgilere erişim halinde tıpkı diğer hassas veri türlerinde olduğu gibi ayrımcılık duygularının harekete geçmesi veya finansal güvenlik sorunları riskinin yaşanacağı durumların ortaya çıkması hiç de göz ardı edilemeyecek güçlü bir ihtimaldir.[89] Kaldı ki hassas statüde tanımlanan veriler özel yaşam ve aile hayatına dokunduğu kadar kişinin sosyal pozisyonu, iş hayatı, bankacılık işlemleri, sermaye hareketlilikleri ile ticari eylem ve çalışma faaliyetleri ekseninde de benzer nitelikte varlık kazanır.[90]

213 sayılı Vergi Usul Kanunu "*Vergi mahremiyeti*" başlıklı 5. maddesinde 'Vergi muameleleri ve incelemeleri ile uğraşan memurların, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay'da görevli olanların, vergi kanunlarına göre kurulan komisyonlara iştirak edenlerin, vergi işlerinde kullanılan bilirkişilerin görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları ifşa edemeyecekleri ve kendilerinin veya üçüncü şahısların nef'ine kullanamayacakları' düzenlemesiyle nispeten finansal mahremiyet için güvence hükümleri getirse de madde hükmünün bütünlüklü bir hassas veri düzenlemesi için yeterli olduğunu iddia etmek mümkün gözükmemektedir. Oysa finansal bilgi akışının Bankacılık Düzenleme ve Denetleme Kurumu, Hazine ve Maliye Bakanlığı, Sermaye Piyasası Kurulu, Tasarruf Mevduatı Sigorta Fonu, Mali Suçları Araştırma Kurulu ve sigorta şirketleri[91] gibi geniş bir kurumsal hat üzerinde cereyan etmesi risk altındaki bilgi sistemleri dikkate alındığında hassas veri koruması talebini, karşılanması daha da acil bir ihtiyaç haline getirmektedir. Benimsenen bu yaklaşımın kökeninde esas olarak özel nitelikli kişisel verilerin güven içinde elde edilmesi ve işlenmesi süreçlerine verilen önem kadar, değişen sosyo-ekonomik şartların ortaya çıkaracağı yeni koruma ihtiyaçlarına yasallık kazandırma talebi de bulunmaktadır.

[89] KÜZECİ, **2018**, s. 257.

[90] KİNDT, **2013**, s. 94.

[91] TURAN, Metin, **Bilişim Hukuku**, 2. Baskı, Seçkin Yayınevi, Ankara, 2017, s. 168-170.

Mevcut açıklarına rağmen genel kişisel verilere sağlanan güvenceler dışında pozitif hukukun himaye altına aldığı hassas veriler için yasal düzenleme sınırlılığında yapılacak veri işlenmesi sürecini yönetmek ve standart ilkeler geliştirmek amacıyla kurulsal bir icra makamının teşkil edilmesini ise en azından başlangıç için olumlu bir düzenleme olarak karşılamak gerekir. Özellikle hassas kişisel verilerin korunmasına ilişkin temel haklarla bağlantılı beklentilerin gerçekleşmesinde yeni bir regülasyon kurumu kimliğiyle hukuk düzeninde yerini alan Kişisel Verileri Koruma Kurumu'nun yasal hükümleri pekiştiren kararlar alma performansı, uygulamaya yön verme ve oluşturacağı ek idari kapasite gücü, koruma alanının etkinliği konusunda belirleyici ölçütleri oluşturacaktır. Nitekim Kişisel Verileri Koruma Kanununun 6. maddesinin son fıkrasında açık bir dille ifade edildiği üzere Kişisel Verileri Koruma Kurulu, özel nitelikli kişisel verilerin işlenmesinde diğer verilere kıyasla daha etkili, münhasır ve yeterli önlemler almakla görevli kılınmıştır. Bu çerçevede kurulun 31.01.2018 tarihli ve 2018/10 sayılı *Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*[92] konulu kararı, prosedürel işlem süreçlerine yönelik ayrıntılı teknik müdahale araçları öngörmesi itibariyle hem veri kayıt sisteminin oluşturulmasına hem de veri işleyen gerçek ve tüzel kişiler ile veri sorumlusunun yönlendirilmesine hizmet eden detaylı rehber ilkeler içermektedir.

Kurul kararıyla, en başta özel nitelikli verilerin güvenliğine yönelik sistemli, kuralları net, yönetilebilir ve sürdürülebilir politika ile koruma prosedürlerinin belirlenmesine yönelik teknik nitelikte adımlar atıldığı görülmektedir. Kararda öncelikle hassas verilerin işlenmesi sürecinde görev alanlara yönelik düzenli eğitimler verilmesi, gizlilik sözleşmelerinin yapılması, verilere erişim sağlayanların yetki sınırı ve süresinin tespit edilmesi ile görev hareketliliklerinin takip edilerek periyodik yetki kontrollerinin gerçekleştirilmesi amaçlanmıştır. Veri güvenliği için geliştirilen önlemler ise oldukça ayrıntılı ve teknik değerde bir liste içermektedir. Elektronik ortam verilerinin kriptografik yöntemler kullanılarak ve kriptografik anahtarların güvenli ve farklı ortamlarda tutularak muhafaza edilmesi, işlem kayıtlarının güvenli yöntemlerle loglanması, veri ortamlarına ait güvenlik güncellemelerinin sürekli takip edilmesi, yazılım ve güvenlik testlerinin düzenli aralıklarla

[92] Kişisel Verileri Koruma Kurulunun 31.10.2018 tarihli ve 2018/10 sayılı **Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler konulu kararı**. http://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf (Erişim Tarihi 13.05.2018).

yapılarak kayıt altına alınması, verilere uzaktan erişim söz konusuysa en az iki kademeli kimlik doğrulama sisteminin oluşturulması, verilerin işlendiği fiziksel ortamların dış etken kaynaklı hasarlardan korunması ile veri aktarma kanallarına ilişkin yüksek güvenlikli koruma önlemleri alınması kararları, veri koruma kapasitesini güçlendirici idari önlemler seti niteliğindedir.

Kararda ayrıca özel nitelikli kişisel veriler aktarılacaksa kullanılan e-postaların şifreli-kurumsal nitelikte olması veya kayıtlı elektronik posta hesabının kullanılması, taşınabilir bellek, CD, DVD gibi ortamlar kullanılacaksa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarların ayrı ortamda tutulması, farklı fiziksel ortam sunucuları söz konusuysa sunucular arasında aktarım güvenliğinin sağlanması, kağıt ortamında aktarılan veriler için ise 'gizlilik dereceli belgeler' formatı kullanılması gerektiği belirtilerek özel nitelikli hassas kişisel verilerin işlenmesinde ayrıntılı teknik ve kurumsal önlemler geliştirilmesi amaçlarını gerçekleştirmeye yönelen güçlü bir sistem tasarımı ortaya konulmaya çalışılmıştır. Alınan önlemlerin kapsamlı olması, güvenlik eksenli öğeler taşıması ve teknik kapasite yoğunluklu bir yapı arz etmesi ise korunmak istenen hassas verilerin diğer kişisel verilere oranla temel hak ve özgürlüklerin kullanımını ciddi oranda etkileme potansiyeliyle açıklanabilir.

Hassas Kişisel Veri Koruması Açısından Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR): Kısa Bir Karşılaştırma

Üye devletlerin hukuk sisteminde doğrudan uygulanan[93] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) özel kategorilerdeki kişisel verilerin işlenmesi başlıklı 9. maddesinde ırk-etnik köken, siyasi görüşler, dini-felsefi inançlar, sendika üyeliği, bir gerçek kişinin kimlik teşhisinin yapılması amacıyla kullanılabilen genetik ve biyometrik veriler, sağlık bilgileri ile cinsel yaşam veya cinsel eğilime ilişkin veriler, prensip olarak belirli şartlar gerçekleşmemişse işlenmesi yasak hassas veri kategorilerini oluşturur.

6698 sayılı Kanun hükümleriyle karşılaştırıldığında birçok başlığın ortak olduğu fakat kişinin mezhep veya diğer inançları, kılık-kıyafeti ile dernek ve vakıf üyeliğine ilişkin bilgilerinin hassas veriler içinde düzenlenmediği görülmektedir. Cinsel yaşamla ilgili tüzük düzenlemesinde ise farklı olarak yalnızca gerçek kişinin cinsel eğilimine ait bilgiler hassas kişisel veri sınıflaması

[93] KÜZECİ, **2018**, s. 202.

içinde kabul edilmiştir. Başka bir anlatımla tüzük hükümlerinde geçen cinsel eğilim, bir hassas veri türü olarak Türk pozitif hukuk düzenlemesinde yer almamaktadır. Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ise '*Mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi*' başlığıyla müstakil bir maddede (m.10) düzenleme imkânı bulmuştur. Hassas kişisel verilerin seçimine ilişkin hukuki tercihin, büyük oranda veri türlerinin hassas verilere dönüşmesinde etkili olan toplumsal değer yargılarının değişken olmasından ve kültürel kodlara göre içerik kazanan gösterge ve referans değerlerin farklılaşmasından kaynaklandığı söylenebilir.

Tüzükte, Birlik veya üye devlet hukuku çerçevesinde sağlanması halinde hassas verilere ilişkin işleme yasağının veri sahibi tarafından kendi rızasıyla dahi kaldırılamayacağına ilişkin bir istisna hükmü öngörülmüşken 6698 sayılı Kanun'da kişilerin tasarruf alanına kişi hakları ve insan onurunun korunmasına öncelik verme düşüncesinden ilham alan bu tür kısıtlayıcı bir müdahale hükmü getirilmemiştir. Tüzük hükümleri, sağladığı genel koruma rejiminden ayrılarak işlenmesi yasak olan hassas veriler konusunda ise geniş sayılabilecek bir istisnalar listesi oluşturmuştur. Bu özel yaklaşımın sergilenmesinde kişinin kendi verileri üzerindeki tasarruf hakkının tanınması kadar, kamu yararı, kamu düzeni, bilginin sınırlı bir alanda ve belli amaçlar dâhilinde kullanılıyor olması, verilerin bizatihi kişi tarafından alenileştirilmesi ve bilgi işleme faaliyetinin kaçınılmaz olması gibi kriterlerden hareket edilmiştir. Buna göre Birlik veya üye devlet hukuku çerçevesinde veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlanması söz konusu ise 9. madde uyarınca; yasağın veri sahibi tarafından kaldırılamayacağına ilişkin istisna haricinde, ilgilinin tüzükte sıralanan bir veya daha fazla sayıda amacı gerekçe göstererek açık rıza ile onay vermesi söz konusuysa hassas verilerin işlenmesi Tüzük esaslarına uygun kabul edilecektir. Bir toplu sözleşme çerçevesinde izin verildiği sürece, kontrolörün veya veri sahibinin istihdam, sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi halinde yine verilerin işlenmesinde hukuki bir engel söz konusu olmayacaktır.

Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda bulunması, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından gerekli görülmesi, işleme faaliyetinin tereddütsüz biçimde kamuya açıklanan alenileştirilmiş kişisel verilerle ilgili olması ve

yasal iddiaların araştırılması veya savunulması amacıyla yargı yetkisinin mahkemelerce kullanımını gerekli kılması söz konusu ise işleme eylemi hassas veriler bakımından yasak kapsamında bir değerlendirilmeye tabi tutulmayacaktır. Veri işleme faaliyetinin vakıf, birlik veya kâr amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendikal amaçlarla ve uygun güvenceler sağlanarak meşru faaliyetler esnasında gerçekleşmesi halinde de, bu verilerin yalnızca mevcut veya eski üyeler ya da kuruluşun amaçlarıyla bağlantılı ve kendisi ile düzenli temas halinde bulunan kişileri kapsaması durumunda işleme için hukuksal şartların yeterli olduğu kabul edilecektir.

Gözetilen amaçla orantılı olması, veri koruma hakkının özüne saygı gösterilmesi, veri sahibinin temel hakları ile menfaatlerini güvencede tutan spesifik önlemler alınması gerçekleşmişse ve Birlik veya üye devlet hukuku açısından kamu yararına bağlı kayda değer sebepler işleme faaliyetini gerekli kılmışsa hassas verilerin işlenmesine ilişkin genel kurallardan ayrılmak ancak bu şartlarda mümkün olabilecektir.[94]

---

[94] Anayasa Mahkemesi bu kısımdaki bakış açısını tüzük hükümlerinden önce ortaya koyan etkili kararlar verebilmiştir. Mahkeme, hassas verilerin işlenmesini biyometrik yöntemlerle kimlik doğrulama işleminden hareket ederek anayasal hükümler bakımından değerlendirmiş ve kararında özellikle kamu hizmeti gereklilikleri, kamu yararı, hizmetin güven içinde sağlıklı, etkili ve düzenli işlemesi gibi kriterler kullanmıştır. Mahkemeye göre, "*Biyometrik yöntemlerle kimlik doğrulama, kişinin kendi özelliklerini esas alması nedeniyle izinsiz kullanımlara karşı güvenli, kamu kuruluşlarına yönelik yolsuzluk ve bunların neden olduğu zararlara karşı etkili ve sosyal güvenliği olan kişiler bakımından da güvenli hizmet alınmasını sağlayan bir yöntemdir. İtiraz konusu kuralla öngörülen yöntemin sağlık sektöründeki suiistimallerin engellenmesi ve bu konudaki sahteciliğin önlenmesi maksadıyla önemli bir güvenlik önlemi olduğunda şüphe yoktur. Nitekim itiraz konusu kuralın gerekçesinde sağlık hizmetlerinin elektronik ortamda güvenilir altyapılar üzerinden sağlanması ve hizmetten yararlananların kimliklerinin saptanmasında geleneksel yöntemlerin eksiklikleri nedeniyle ortaya çıkan kötüye kullanımların önlenmesinin amaçlandığı belirtilmiştir. Dolayısıyla kuralla öngörülen yöntemin etkin bir şekilde kullanılmasının, Sosyal Güvenlik Kurumundan haksız menfaat temin edilmesini engellemeye yönelik olduğu ve kuralda kamu yararı bulunduğu açıktır. Bu bağlamda itiraz konusu kuralla özel hayatın ve kişisel verilerin korunması haklarına yönelik olarak yapılan müdahalenin, öngörülen amaçla orantılı olduğu, müdahale edilen hakların özüne dokunmadığı ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediği anlaşıldığından Anayasa'ya aykırı bir yönü yoktur.*" Mahkemeye göre ayrıca verilerin üçüncü kişiler ya da kamu kurum ve kuruluşları ile paylaşılabilmesi için verilere erişebilme hususunda kişi ve kurumların kanunen yetkilendirilmesi ve bu yetki sahasının da görevlerin yerine getirilmesi için gerekli ve görevle sınırlı olması

Çalışan performansının değerlendirilmesi, tıbbi tanı, sağlık ve sosyal bakım hizmetlerinin veya tedavinin temin edilmesi, sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi sebepleri mevcutsa hassas veri işleme faaliyeti aynı yaklaşımla Tüzük hükümleri bakımından gereklilik arz eden bir görünüm kazanır. Başta mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına yönelik spesifik tedbirler geliştirilmesi, Birlik veya üye devlet hukukuna dayalı olarak sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması, sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları oluşturulması gibi halk sağlığı alanında kamu yararına yönelik işleme faaliyetinin gerekmesi durumu da Tüzük'e göre hassas verilerin işlenmesi konusunda meşru bir yetki alanı sunmaktadır.

Kamu yararına yönelik arşivleme, bilimsel, tarihi araştırma ya da istatistiki amaçlar doğrultusunda bir gereklilik olarak görülmesi halinde hassas verilerin istisna hükümleri kapsamında ele alınması ve işleme faaliyetinin meşru bir parçası olarak görülmesi gerektiği Tüzük hükümlerinde yansıma bulan diğer normatif esaslar arasındadır. Ancak üye Devletlerin genetik, biyometrik ve sağlık ile ilgili verilerde sınırlamalar da dâhil olmak üzere ek koşullar uygulamaya devam etmesi ya da bu konularla ilgili ek koşullar getirebilmesi hakkı, veri işleme rejimi içinde mahfuz tutulmuştur. Bu tutumun sebebi ilgili alanlardaki verilerin, kişilerin yaşamını müdahaleden uzak huzur içinde sürdürmesi ve özel hayatın gizliliği hakkına en çok yaklaşan haklar listesini oluşturması ile ihlale neden olma potansiyelinin en çok hissedildiği risk alanlarını içinde barındırmasından kaynaklanmaktadır.

İstisna hükümleri açısından hassas verilerin işlenmesine ilişkin yukarıdaki düzenlemeler, Türk ulusal mevzuatına kıyasla Avrupa Birliği Tüzük hükümlerinde daha kapsayıcı ve açıklayıcı bir anlatımla dile getirilmiştir. Kamu yararı ve kamu düzeni gibi kapsamı tam olarak somutlaştırılamayan ve tanımı verilmeyen gerekliliklerin konu bağlamı içinde somut bir konumlanma ve referans değeri kazandırılmasına da özellikle dikkat edilmiştir. Benzer bir yaklaşım, 6698 sayılı Kanun'da kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi gerekçeleri sıralanarak yalnızca sağlık ve cinsel hayata ilişkin kişisel veriler üzerinden

gerekir. (AYM. E. 2014/196, K. 2015/103 K.T. 12.11.2015; E. 2014 / 180, K. 2015 / 30, K. T. 19.03.2015).

sergilenmiş; diğer hassas veriler açısından ise kişinin rızasının alınması ve başka kanunlarda düzenleme yapılması şartının yeterli görülmesiyle yetinilmiştir. Ancak kanunun '*çeşitli hükümler*' bölümünün 'istisnalar' başlıklı 28. madde hükümlerinin hassas verilerle ilgili kısıtlı alandaki veri işleme yetkisini belirli gerekçeler eşliğinde bir hayli genişletmesi, AB Genel Veri Koruma Tüzüğü Sistemi'ne yaklaşan bir genel kural farklılaşması içinde konumlanıldığını göstermektedir. Kanun hükümlerinin uygulanmayacağı halleri belirten madde düzenlemesi genel kişisel veri-hassas kişisel veri ayrımı getirmediğinden ek istisna[95] sayılan durumların hassas verileri de içine almak üzere genele etkili bir geçerlik gücü taşıdığı söylenebilir. Kanun düzenlemesine göre genel/hassas kişisel veri işlemenin;

- Üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri,
- Resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla elde edilen verileri,
- Millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç oluşturmamak kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında bilgi derlenmesini,
- Millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetlerle irtibatlı veri kaydını,
- Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri kayıtlarını içeren özel hallere münhasır olgulara yönelik verileri kapsaması durumunda hassas kişisel veri rejimine ilişkin sınırlayıcı yasal düzenlemeler uygulama alanı bulamayacaktır.

[95] AYÖZGER, Ayşe Ç., **Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması**, Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2016, s. 39.

Yasal düzenlemenin aynı hükmüne göre kişisel veri işlemenin suçun önlenmesi veya suç soruşturması için gerekli olması, ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilere yönelik bir kapsamı içermesi, görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesiyle ilgili bulunması, disiplin soruşturma veya kovuşturması için işleme zaruretinin ortaya çıkması, bütçe, vergi ve mali konulara yönelik devletin ekonomik ve mali çıkarlarının korunması için gerekli olması koşullarının mevcudiyeti halinde ise kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. madde , zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. madde ve veri sorumluları siciline kayıt yükümlülüğünü düzenleyen 16. madde hükümleri hiçbir koşulda geçerli olmayacaktır.

Tüzükte hassas kişisel verilerin işlemesine ilişkin yasaklayıcı hükümlere getirilen istisnalar aynı madde içinde düzenlenmiş olmasına karşın 6698 sayılı Kanun sistemi farklı olarak istisna kuralları ihdas etme hedefine önemli ölçüde 6. ve 28. madde hükümleriyle ulaşabilmiştir. Vurgulanması gereken diğer bir önemli husus ise 6698 sayılı Kanun'un '*kişisel verilerin işlenme şartları*' başlıklı 5/2. maddesi uyarınca belirli şartların varlığı halinde açık rıza aranmaksızın kişisel verilerin işlenmesini mümkün kılan düzenleme hükmüdür. Maddeye göre kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya bağlantı kurulması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesine yönelik gereklilik içermesi, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, verilerin ilgili kişinin kendisi tarafından alenileştirilmesi, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin gerekli olması ve nihayet temel hak ve özgürlüklere zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumlarında ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkün hale getirilmiştir. Ancak özellikle belirtmek gerekir ki madde hükmüyle öngörülen istisnalar listesinin genel kişisel veriler dışında hassas verileri de kapsadığını gösteren kesin bir gönderme hükmü veya açıklayıcı bir düzenleme kuralı kanunda yer almamaktadır. Oysa tüzük hükümleri bu madde düzenlemesinde yer alan istisnai durumların hassas kişisel verileri de içerecek genişlikte

kaleme aldığını gösteren etkili normatif öğeler içermektedir. Dolayısıyla Tüzük hükümleri bağlamındaki hassas veri rejimi dikkate alındığında 6698 sayılı Kanun'un hassas verilerin işleme koşullarını ilgilinin açık rızası kaidesinin istisnaları bakımından oldukça geniş tutmak gerekeceği sonucuna ulaşılabilir. Bu eğilimin benimsenmesi halinde ise hassas kişisel verilerin korunması, elde edilmesi, işlenmesi ve transferi süreçlerinde kamu yararı, kurumsal gereklilikler, kamu hizmet standartları ve kamu düzeni kriterlerine en ziyade müsaadeye mazhar statünün verilmesi ve istisnalar rejiminin bir hayli geniş tutulması sonuçlarıyla karşılaşmak kaçınılmaz olacaktır.

SONUÇ

Genel kişisel verilere kıyasla ulusal ve küresel düzeyde özel hükümlerle ve istisna kaidelerle koruma altına alınan hassas kişisel veriler, kişi güvenliği, temel haklar ve toplumsal saygınlığın korunması bakımından kamu otoriteleri ve özel hukuk kişileri tarafından işlenmesi sıkı krallara bağlanan temel bir hak alanını oluşturur. Bu tutumun kökeninde, kişinin ayrımcılığa uğramaması, önyargılı yaklaşımların öznesi haline getirilmemesi ve kamu hizmetlerinden adil yararlanma koşullarının zedelenmemesi yönünde belirginlik kazanan temel anayasal ve kamusal amaçlar yer alır.

Hassas veriler dini inanç, politik-ideolojik görüş, adli sicil kayıtları, ırk, etnik köken ve sağlık verileri ile cinsel yaşam gibi özel niteliğe sahip veri türlerinin elde edilmesini kişinin kendini geliştirme hakkıyla bağdaştıran entegre bir zemin üzerinde yükselerek hukuksallık zırhı kazanmaya çalışır. Legalleşme çabasının 20. yüzyılın son çeyreğinde varlık kazanan ulusal hukuk inşa hareketlerini verilerin sınır aşan hareketliliği nedeniyle çok geçmeden küresel düzenlemelerle bütünleşme sürecine girmeye zorlaması ise iki yönlü gelişimin hukuk oluşturmakla sonuçlanan doğal bir sonucu niteliğindedir. Veri güvenliği sorunu bu etkiyle uluslar ötesi bir tartışma ve mutabakatın konusu haline gelerek hassas veri rejimine yer veren farklılaştırılmış bir veri güvenliği politikası çerçevesinde bir çözüm ve açıklama modeline yönelmiştir. Avrupa Konseyi, OECD ve Avrupa Birliği başta olmak üzere küresel merkezlerin bu alanda önemli bir hukuksal birikim örneği ve performansı sergilediğini vurgulamak gerekir.

Daha özel alanda kurgulanan hassas kişisel veri düzeninde benimsenen nihai amaç ise duyarlılık düzeyi yüksek kişisel verilerin özel bilgi veya tasarruf alanından çıkarılarak yetkisiz kişilerin erişimine açılması sonucunda, doğacak maddi ve manevi zararlar ile özel yaşam alanı ihlaline karşı bireyi korumak refleksine özgülenmiştir. Bu perspektif içinde Türk hukuk mevzuatı, başta Anayasa olmak üzere, ceza özlü kanunlar, medeni hukuk, iş hukuku ve sigorta hukuku gibi geniş bir hukuksal alanda kişisel veri koruma normlarını küresel standartlara adapte etmeye çalışmıştır. Verimli işbirliği olanaklarına rağmen her iki hukuki düzey ilişkisinde sorunsuz ve tam örtüşen bir norm aktarımının varlığından söz edilemeyeceği gerçekliğini ise idari, siyasi ve toplumsal gerekçelerin farklılaşmasına bağlı olarak özellikle göz önünde bulundurmak gerekmektedir. Bu çerçevede hem ulus ötesi hem de ulusal veri koruma mevzuatı açısından kural ihdas etme ve adaptasyon çabaları

sürecinde hassas verilerin korunması ile ilgili getirilebilecek en temel eleştiri noktası, kamu düzeni, kamu yararı veya kamu hizmeti örgütlenmesi ölçütleri etrafında yasal istisnalarla genişletilen bir yetki düzeninin muğlak bir yaklaşımla kamusal organlara tanınmış olmasıdır. Bu riskli alanın tolere edilmesi ve hukukun genel ilkelerine göre yapılandırılmasının yolu ise, kamusal ve işletme bazlı çıkarların hassas verilerin korunması çabasını etkisizleştirerek belirsiz durumlar yaratmasını bloke etmekten ve küresel düzeyde öngörülen güçlü mekanizma ve araçların iç hukuka transfer edilmesi çabasını desteklemekten geçmektedir. Aksi halde koruma mekanizmalarının teknik ve hukuksal araçlarla tahkim edilmediği ve kişisel hak alanın yeterince güçlendirilmediği düşük kapasiteli bir hassas veri düzeni, yasal amaçlarla uyumlu olmayan ağır bir güven açığı yaratacağı gibi sorumlu birimler, veri işleyen gerçek/tüzel kişiler, veri sorumluları ve özneleri nezdinde de onarılması güç bir hukuksal maliyet ve zarar tablosu ortaya çıkarmaktan kurtulamayacaktır.

KAYNAKLAR

Kitap ve Makaleler

AKDAĞ, Hale, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Ankara, Üniversitesi Sosyal Bilimler Enstitüsü, 2010.

AKGÜL, Aydın, **Kişisel Verilerin Korunması Açısından İdarenin Hukuksal Sorumluluğu ve Yargısal Denetimi**, Doktora Tezi, Kocaeli, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2013.

AKSOY, Hüseyin C., **Kişisel Verilerin Korunması**, Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2008.

AYÖZGER, Ayşe Ç., **Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması**, Doktora Tezi, İstanbul, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2016.

BAŞALP, Nilgün, **Kişisel Verilerin Korunması ve Saklanması**, 1. Baskı, Yetkin Yayınları, Ankara, 2004.

BÜK, Alaattin, **Bilişim Alanında Kişisel Verilerin Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2018.

ÇAKAN, Cansu, "Kişilik Hakkı Kapsamında Korunan Bir Değer Olarak Kişisel Veriler", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, Yıl: 2013, Sayı: 2, (s. 187-222).

ÇETİN, Hakan "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi" **Akdeniz İ.İ.B.F. Dergisi**, Yıl: 2014, Sayı: 29, (s. 86-105).

ÇOKMUTLU, Metin, **Türk Ceza Hukukunda Kişisel Verilerin Korunması**, Doktora Tezi, Kocaeli, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2014.

COOPER, Daniel P. "İnvestigations: Understanding Data Privacy", **Journal of Financial Crime**, Yıl: 2005, Cilt: 12, Sayı: 4, (s. 352-359).

EFRAİMİDİS Pavlos S./DROSATOS Georgios / NALBADİS Fotis, vd., "Towards privacy in personal data Management", **İnformation Management & Computer Security**, Yıl: 2009, Cilt: 17, Sayı: 4, (s. 311-329).

ERDİNÇ, Göksu H., **Bilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler**, Yüksek Lisans Tezi, İstanbul, İstanbul Teknik Üniversitesi Bilişim Enstitüsü, 2017.

GÖZLER, Kemal, **İngilizce Karşılıklarıyla Hukukun Temel Kavramları**, 8. Baskı, Ekin Yayınları, Bursa, 2011.

GÜRSEL, İlke, "Protection of Personal Data in İnternatıonal Law and The General Aspects of The Turkish Data protection law", **DEÜ Hukuk Fakültesi Dergisi**, Yıl: 2016, Cilt: 18, Sayı: 1, s. 48-49. (s. 33-61).

HENKOĞLU, Türkay, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, 1. Baskı, Yetkin Yayınları, Ankara, 2015.

KAYA, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi" **İÜHFM**, Yıl: 2011, Cilt: LXIX, Sayı: 1-2, (s. 317-334).

KİNDT, Els, J., **Privacy and Data Protection Issues of Biometric Applications A Comparative Legal Analysis**, Springer: Newyork London, 2013.

KOCA, Mahmut/ÜZÜLMEZ, İlhan, **Türk Ceza Hukuku Genel Hükümler**, 10. Baskı, Seçkin Yayınları, Ankara, 2017.

KORKMAZ, İbrahim, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 1. Baskı, Seçkin Yayınları, Ankara, 2017.

KRANENBORG, Herke, "Access to Documents and Data Protection in The European Union: on The Public Nature of Personal Data", **Common Market Law Review**, Yıl: 2008, Sayı: 45, (s. 1079-1114).

KUSCHEWSKY, Monika/GERADİN, Damien, "Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges", **World Competition**, Yıl: 2014, Cilt: 37, Sayı: 1, (s. 69-102).

KÜZECİ, Elif, **Kişisel Verilerin Korunması**, 2. Baskı, Turhan Kitabevi, Ankara, 2018.

ÖZBEK, Veli Ö./BACAKSIZ, Pınar/DOĞAN, Koray, vd., **Türk Ceza Hukuku Özel Hükümler**, 12. Baskı, Seçkin Yayıncılık, Ankara, 2017.

ÖZDEMİR, Hayrunnisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, 1. Baskı, Seçkin Yayıncılık, Ankara, 2009.

TAKCI, Hidayet/CANBAY, Pelin, "Kişisel Verilerin Korunmasında Öznitelik Tabanlı Gizlilik Etki Değerlendirmesi Yöntemi", **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi**, Yıl: 2017, Cilt: 32, Sayı: 4 (s. 1301-1310).

TANG, Victor/ YANİNE, Fernando/ VALENZUELA, Lionel, "Data, İnformation, Knowledge and İntelligence The Mega-Nano Hypothesis and İts İmplications in İnnovation", **İnternational Journal of İnnovation Science**, Yıl: 2016, Cilt: 8, Sayı: 3, (s. 199-216).

TAYLOR, Mark j., "Data Protection, Shared (Genetic) Data and Genetic Discrimination", **Medical law İnternational**, 2006, Cilt: 8, (s. 51-77).

TEZCAN Durmuş/ERDEM Mustafa Ruhan/SANCAKDAR Oğuz/ ÖNOK Rifat Murat, **İnsan Hakları El Kitabı**, 6. Baskı, Seçkin Yayıncılık, Ankara, 2016.

TRANBERG, Charlotte B., "Biometric Data in Scandinavia", **European Business Law Review**, Yıl: 2008, Cilt: 19, Sayı: 2, (s. 387-403).

TURAN, Metin, **Bilişim Hukuku**, 2. Baskı, Seçkin Yayınevi, Ankara, 2017.

PURTOVA, Nadezhda, "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights", **Netherlands Quarterly of Human Rights**, Yıl: 2010, Cilt: 28 Sayı: 2, (s.179-198).

ZERDİCK, Thomas, European Aspects of Data Protection: What Rights for the Citizen?, **Legal Issues of Economic İntegration**, Yıl: 1995, Sayı: 2, (s. 59-86).

ZİLİOBAİTE, Indre/CUSTERS, Bart, "Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models", **Artif Intell Law**, Yıl: 2016, Sayı: 24, (s. 183- 201).

İnternet Kaynakları

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (Erişim Tarihi: 13.05.2018).

Avrupa İnsan Hakları Mahkemesinin S. ve Marper/Birleşik Krallık Davası (Başvuru No.30562/04 ve 30566/04).

Downloads/CASE%20OF%20S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20%20[Turkish%20Translation]%20by%20the%20COE%20Human%20Rights%20Trust%20Fund.pdf (Erişim Tarihi: 07.11.2018).

Handbook On European Data Protection Law 2018 Edition https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf (Erişim Tarihi: 29.10.2018).

KAYA, Mehmet B./ TAŞTAN Furkan G., **Veri Koruma Hukuku: Mevzuat İçtihat**. http://www.muharrembalci.com/kitaplika/79.pdf 13.05.2018 (Erişim Tarihi: 13.05.2018).

KETİZMEN, Muammer/ÜLKÜDERNER, Çağlar, **E-Devlet Uygulamalarında Kişisel Verilerin Korunma(ma)sı**, s. 2, http://inet-tr.org.tr/inetconf12/bildiri/2.pdf (Erişim Tarihi 11.05.2018).

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf 13.05.2018. (Erişim Tarihi: 13.05.2018).

Kişisel Verileri Koruma Kurulunun 31.10.2018 tarihli ve 2018/10 sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler konulu kararı http://www.resmigazete.gov.tr/eskiler/2018/03/20180307-7.pdf 13.05.2018. (Erişim Tarihi: 13.05.2018).

Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, Kişisel Verileri Koruma Kurulu Yayınları, 2018. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ead8e671-e01e-4ca7-a6a3-bc3c6f79f7c7.pdf (Erişim Tarihi 01.05.2018).

ÖZENÇ, Köksal, **Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması**, Uluslararası Katılımlı Bilgi Güvenliği ve

Kriptoloji Konferansı, 13-14 Aralık, Ankara, 2017. http://www.iscturkey.org/assets/files/2016/03/2007-26.pdf (Erişim Tarihi 13.05.2018).

http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.5b0350a8c86216.44879670; http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b03504c269c89.67813800 (Erişim Tarihi: 08.05.2018).

http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.5b03536c04b525.03378534 (Erişim Tarihi: 08.05.2018).

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b035cae955f04.22462695 (Erişim Tarihi: 08.05.2018).