KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ TÜRKİYE'DEKİ KANUN TASARISININ AVRUPA BİRLİĞİ VERİ KORUMA DİREKTİFİ IŞIĞINDA DEĞERLENDİRİLMESİ

(An Assessment of the Turkish Draft Law on Protection of Personal Data in Light of the EU Data Protection Directive)

Nurullah Tekin[1]

ÖZ

Kişisel verilerin korunması, birçok uluslararası anlaşmalarda özel hayata ve aile hayatına saygı hakkı ile yakından ilgili ancak ondan farklı olarak, temel hak şeklinde düzenlenmiştir. Avrupa Birliği içerisinde çeşitli direktifler kişisel verilerin kullanımını düzenlemektedir, ancak bunlardan en kapsamlı olanı, bireyin mahremiyetini ve kişisel verilerin kullanımını koruyan 'AB Veri Koruma Direktifi'dir. Kişisel verilerin korunmasına ilişkin giderek fazlalaşan bu hassasiyete rağmen, Türkiye'de kişisel veri gizliliğini düzenleyen bir kanun henüz, bazı mevzuat bölümleri kişisel verilerin korunması ile ilgili olmasına rağmen, yoktur. Adalet Bakanlığı tarafından birkaç yıldır hazırlanan ve geliştirilen ancak başarıya ulaşmamış bir "Kişisel Verilerin Korunmasına Dair Kanun Taslağı" vardır. Bu çalışmamızda, AB Veri Koruma Direktifi ayrıntılı bir şekilde anlatılmakta, Türkiye'deki mevcut durum ve bağımsız bir kişisel verilerin korunması kanununa neden gereksinim duyulduğu açıklığa kavuşturulmaya çalışılmaktadır. Son olarak da, Türkiye'deki 'Kişisel Verilerin Korunmasına Dair Kanun Tasarısı' karşılaştırmalı olarak incelenmekte ve buna göre kritiği yapılmaktadır.

Anahtar Kelimeler: Kişisel Veri, Bilgi, Mahremiyet, AB Veri Koruma Direktifi, Kişisel Verilerin Korunmasına Dair Kanun Tasarısı,

ABSTRACT

The protection of personal data is recognized as a fundamental right in several European and international treaties, closely linked to but different from the right to respect for private and family life. Various directives deal with personal data usage in the European Union, but the most inclusive

1 Menemen Cumhuriyet Savcısı, nurullah.tekin@adalet.gov.tr
*Makale Geliş Tarihi: 14.7.2014, Kabul Tarihi: 24.7.2014

is the EU Data Protection Directive which protects individuals' privacy and personal data use. Despite such gradually increasing sensitivity on protection of personal data, there is not yet a specific law governing personal data privacy in Turkey, though other pieces of legislation refer to the protection of personal data. There is also a draft Law on Protection of Personal Data, which was prepared and developed by the Turkish Ministry of Justice for several years without success. In this the EU Data Protection Directive will be explained in detail. Thereafter, the state of play of this issue in Turkey and the question of why it needs a specific data protection law will be clarified. Finally, the Draft Law on Protection of Personal Data will be comparatively assessed and criticised.

Keywords: Personal Data, Information, Privacy, EU Data Protection Directive, Draft Law on Protection of Personal Data

***

BİRİNCİ BÖLÜM

I. GİRİŞ

Kişisel verilerin korunması, birçok uluslararası anlaşmalarda özel hayata ve aile hayatına saygı hakkı ile yakından ilgili ancak ondan farklı olarak, temel hak şeklinde düzenlenmiştir. Son yıllarda yeni bilgi teknolojilerinin ve özelikle de internetin gelişimi, kişisel verilerin güvenliği konusunda endişeleri artırmıştır. Kişisel verilerin transferi ve depolanması, hiçbir zaman bugünkü kadar kolay olmamıştı. Bu konuda Dünya'da en çok görüş birliği ile dikkatin verildiği Avrupa'da, çözüm "Veri Koruma Kanununda" bulunmuştur. Bu terim, kişisel verilerin bilgi dâhilinde olmasını ve gizlenmesini düzenlemeyi amaçlayan yasal yapıyı ifade etmektedir. Avrupa Birliği (AB) içerisinde çeşitli direktifler kişisel verilerin kullanımını düzenlemektedir, ancak bunlardan en kapsamlı olanı, bireyin mahremiyetini ve kişisel verilerin kullanımını koruyan "AB Veri Koruma Direktifi 95/46/EC"dir. Her ne kadar Direktifin hükümleri, teknolojik gelişmelere ve mahremiyete karşı yeni oluşan tehlikelere ayak uyduramasa da, revizyon aşamasında olan Direktif, dünya çapında veri koruma alanındaki en gelişmiş yasal çerçevelerden birini oluşturmaktadır.

Dünya'da birçok ülkede kişisel bilgilerin hem kamu hem de özel sektör tarafından toplanmasını, kullanımını ve yayınlanmasını açıkça düzenleyen veri koruma kanunları bulunmaktadır. Kişisel verilerin korunmasına ilişkin giderek fazlalaşan bu hassasiyete rağ-

men, Türkiye'de kişisel veri gizliliğini düzenleyen bir kanun henüz, bazı mevzuat bölümleri kişisel verilerin korunması ile ilgili olmasına rağmen, yoktur. Adalet Bakanlığı tarafından birkaç yıldır hazırlanan ve geliştirilen ancak başarıya ulaşmamış bir "Kişisel Verilerin Korunmasına Dair Kanun Taslağı" vardır.

Bu çalışmamızda İlk önce, AB Kişisel Verilerin Korunması Direktifi, kapsamı ve ilkeleri ayrıntılı bir şekilde anlatılmakta, ardından da 'Taslak AB Kişisel Verilerin Korunması Yönetmeliği' genel hatlarıyla açıklanmaktadır. Son bölümde ise, bu konu ile ilgili Türkiye'deki mevcut durum ve bağımsız bir kişisel verilerin korunması kanununa neden gereksinim duyulduğu açıklığa kavuşturulmaya çalışılmaktadır. Son olarak da, Türkiye'deki 'Kişisel Verilerin Korunmasına Dair Kanun Tasarısı' karşılaştırmalı olarak incelenmekte ve buna göre kritiği yapılmaktadır.

II. AB'DE KİŞİSEL VERİLERİN KORUNMASI

20. yüzyıl boyunca AB, kişisel verilere sınırsız erişimin ortaya çıkardığı tehlikelerle karşı karşıya gelmiştir. Otoriter rejimler, tüm Avrupa'da kişisel bilgileri yıkıcı anlamda toplamış ve kullanmışlardır. Bu itibarla, bu deneyimler, hem uluslararası hem de ulusal düzeyde kişisel verilerin kontrolsüz kullanımını önlemeye yönelik yeni çabaları harekete geçirmiştir[2]. Örneğin, AİHS, kişisel verilerin korunmasını genişletmeye yönelik ilk çabalardan birini teşkil etmiştir. AİHS'in 8. maddesine göre "*herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir*." Bu madde, ayrıca, hükümetler tarafından bu hakka karışmanın, demokratik bir toplumun düzgün işleyişi için gerekli olduğu yerler haricinde yasaklandığını vurgulamıştır.

1970'li yıllardan başlayarak bazı Avrupa ülkeleri hem kamu hem de özel sektörü ilgilendiren kapsamlı veri koruma kanunları kabul etmiş ve bu kanunları izlemek ve uygulamak için resmi 'Veri Koruma Kurumlarını' (Data Protection Authorities-DPA-) tesis etmiştir. Örneğin, Alman Hessen eyaleti, gelişmiş teknolojilerin bireyin kişisel verilerinin uygunsuz bir şekilde yönlendirilmesi riskini artırmakta olduğu endişelerinden dolayı 1970 yılında ilk veri işleme düzenlemesini kabul etmiştir. Bunu takiben İsveç, ilk ulusal veri koruma kanununu 1973 yılında çıkarmıştır. Buna benzer bir şekilde Fransa, 1978 yılında bireylere özel hayatın korunmasına yöne-

2 **Kaplan Harvey L, Cowing Mark W, Egli Gabriel P**, *A Primer for Data-Protection Principles in the European Union*, Defense Research Institute, Munich, 2009, s. 39

lik bazı önlemleri sağlayan '*Veri İşleme, Dosyalar ve Özgürlüğe İlişkin Kanunu*' çıkarmıştır[3].

Avrupa'nın veri koruma standartları ve mevzuatı kabul etmesiyle ilgili uzun ve gurur verici bir tarihinin olduğu akıldan çıkarılmamalıdır. Bunlardan bazıları zaman içerisinde tadil edilmiştir ve bazıları gözden geçirilmeye devam edecektir. Mevzuat daima sosyal ve teknolojik gelişmeleri takip etmektedir ve DPA'lar için bu gelişmelere uyum sağlamak ve hızla değişen koşullarda mevzuatı uygulamak ve politika geliştirmek bir zorluk teşkil etmektedir[4]. Bu bağlamda, AB mevzuat planının mihenk taşı, 1995 yılında getirilen 'AB Veri Koruma Direktifi'dir. Bunun ardından, 1997 yılında AB mevzuatının başka bir ana parçası olan, telekomünikasyon sektörü için 97/66/AT Direktifi gelmiştir. Bunun yerine 2002 yılında bu sektör için veri koruma kurallarını güncelleyen 2002/58/AT Direktifi gelmiştir.

III. AB VERİ KORUMA DİREKTİFİ 95/46

A. GENEL OLARAK

1980'li yıllarda çok açık bir şekilde anlaşılmıştır ki, kişisel verileri işleyebilen teknolojik gelişmeler, Avrupa vatandaşlarının bilgi ağlarına tevdi ettikleri veriler konusunda kaygılanmalarına yol açmıştır. Ayrıca, Avrupa Komisyonu, kişisel verilerin ticari sebeplerden dolayı kullanıldığının ve böylelikle Tek Pazar bakımından Topluluk tüzüğüne tabi olduğunun farkına varmıştır[5]. Ne OECD Rehber ilkeleri ne de AK'nin ilgili Sözleşmesi, belirli veri koruma prosedürleri sunmuş ne de ulusal kanunlar arasında uygulama ve standartlaştırma sağlamıştır. Komisyon'un Temmuz 1990'da taslak Direktif'i yayınlaması bu faktörler dikkate alınarak yapılmıştır[6].

11 Mart 1992 tarihinde Avrupa Parlamentosu, Komisyon'un kamu ve özel sektör veri koruması arasında 1990 taslağındaki çelişkileri ortadan kaldırmayı amaçlayan önerisini tadil etmiş ve daha sonra taslak direktifi büyük bir çoğunlukla kabul etmiştir. Komisyon daha sonra tadil edilmiş öneriyi yayınlamış ve Bakanlar Konseyi, "*Kişisel Verilerin İşlenmesi ile İlgili Bireylerin Korunması ve Bu Tür*

3 **Schriver Robert**, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, Fordham Law Review, Cilt: 70, Sayı: 6, 2002, s. 2782

4 **Robinson Neil and others**, *Review of the European Data Protection Directive*, RAND Corporation, sponsored by Information Commissioner's Office, May 2009, s. 4

5 **Kuilwijk Kees Jan**, *Recent Developments in EU Privacy Protection Regulation*, International Trade Law & Regulation, Cilt: 6, Sayı: 6, 2000, s. 200-201

6 **Jay Rosemary and Hamilton Angus**, *Data Protection Law and Practice*, İkinci Baskı, 2003, s. 10

Verilerin Serbest Dolaşımına İlişkin 95/46/AB Sayılı Direktifi" 20 Şubat 1995 tarihinde kabul etmiştir. Direktif resmen 24 Ekim 1995 tarihinde onaylanmış ve üç yıl sonra yürürlüğe girmiştir. 25 Ekim 1998 tarihinde veri koruma kanunu bütün Avrupa'da bariz bir şekilde daha güçlü hale gelmiştir[7].

AB Direktifi'nin temel amacının AB içerisinde kişisel veri akışlarına yönelik engelleri kaldırmak ve tüm Üye Devletlerde kişisel verilerin ortak olarak ve yüksek düzeyde korunmasını tesis etmek olduğu açıktır. Bu, AB'nin iç sınırları ortadan kaldırma ve ekonomik ve parasal birlik kurma amaçlarıyla da uyumludur[8]. AB'nin kanun yapma araçlarından biri olan direktifler, genellikle doğrudan bağlayıcı değildir; ancak birer uyumlaştırma araçlarıdır. Direktifler, Üye Devletlere bu ilkeleri yansıtan ulusal mevzuatı tesis etmesini şart koşmaktadır. Bu bağlamda, AB Direktifinin kabulünü takiben her bir Üye Devlete, ya mevcut kanunlarını tadil ederek ya da Direktifi uygulamak üzere yeni mevzuat getirerek kendi ulusal veri koruma kanunlarını Direktifle uyumlu hale getirme görevi verilmiştir[9].

B. KAPSAM

AB Direktifi; genel hükümler, kişisel verilerin işlenmesinin yasallığı, yargı yolları, sorumluluk ve müeyyideler, kişisel verilerin üçüncü ülkelere transferi, etik kurallar, denetleyici makam, çalışma grubu ve son olarak Birlik uygulama önlemlerini içeren yedi bölüme ayrılmakta ve toplam otuz dört maddeden oluşmaktadır.

Koruma düzeyi, iki sektörde uygulanan kurallar arasında hiçbir fark gözetmeden hem kamu hem de özel sektör için aynıdır. Direktifin 3 (1) maddesi *"bütünüyle veya kısmen otomatik araçlarla, ve ...bir dosyanın parçasını oluşturan veya bir dosyanın parçasının olmasının istendiği kişisel verilerin otomatik araçlarının haricinde her türlü yolla"* işleme arasında ayrım olmadığını öngörmektedir. Elle veri işleme, yalnızca kişisel veri dosyalama sisteminin bir parçasıysa işin içine girer[10]. Bu durum, esasında veri toplamanın bilgisayarla işlenmemiş olması şartıyla, diğer bazı bilgi toplama faaliyetinden önce rastgele toplanan kişisel veriler için güvenli bir pozisyon sağlamaktadır.

7 İlgili Direktif için bkz: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, ET: 18.06.2013

8 Bkz, md 1 ve özellikle de Direktifin 1 ve 3. ön maddeleri

9 **Ilana Saltzman**, *The Status of National Implementation of Directive 95/46/EC on the Processing and Free Movement of Personal Data*, European Intellectual Property Review, Cilt: 18, Sayı: 6, 1996, s. 680

10 **Mell Patricia**, *A Hitchhiker's Guide to Trans-border Data Exchanges Between EU Member States and the United States under the European Union Directive on the Protection of Personal Information*, Pace International Law Review, Cilt: 9, Sayı: 1, 1997, s. 160

Direktifin koruması, ses ve görüntüler yoluyla da olsa belirli veya belirlenebilen gerçek bir kişiye ilişkin olarak herhangi bir bilgi olarak tanımlanan 'kişisel veri' ile sınırlıdır. Bankalar tarafından kurulan güvenlik kameraları, dijitalleştirilmiş imzalar veya kayıt sistemleri için (veri öznesinin önceden rıza hükmünün sağlayacağı türden) hiçbir istisna ya da rehber ilke bulunmamaktadır[11].

Direktif, kişisel verilerin kullanımının düzenlenmesine yönelik kapsamlı bir yaklaşımı yansıtmasına rağmen bu, iki durumda uygulanmamaktadır. İlk olarak, Direktifin 3 (2) maddesi uyarınca bu, ceza hukuku alanındaki devlet faaliyetleri ve (işleme faaliyeti devlet güvenlik konularını ilgilendirdiğinde, devletin ekonomik refahı dahil olmak üzere) devlet güvenliği, savunma, kamu güvenliğine ilişkin verilerin işlenmesi için herhangi bir durumda ve AB hukuku kapsamının dışına düşen bir faaliyet esnasında uygulanmayacaktır. Bu örnekler Komisyon'un bu istisnayla kapsamak istediği türdeki kişisel veriler konusunda kılavuzluk sağlamasına karşın, Direktif, Üye Devletler tarafından istisnayı potansiyel olarak farklı yorumlara açık tutarak bu bağlamda AB hukukunun kapsamını sıkı bir şekilde belirlememektedir[12].

İkinci olarak, Direktif bir gerçek kişi tarafından, tamamen kişisel veya ev içi faaliyeti esnasında yapılan veri işlemeye de uygulanmamaktadır. Bu tür faaliyetler, örneğin, mezuniyet partisi davetleri için bir mail listesi hazırlamak için bilgisayarla işlenmiş bir elektronik çizelge kullanımını içermektedir. Yalnızca iki istisnanın varlığı Direktif'in bariz bir şekilde kapsamını göstermektedir[13]. 'Salt kişisel veya ev faaliyeti' ifadesi, bu tür verilerin bir veya daha fazla kişiye değil de belirsiz sayıda kişiye ifşa edildiği, gerçek kişi tarafından kişisel verilerin işlenmesinin Direktif'in kapsamından çıkarmayı mümkün hale getirmemelidir[14].

Avrupa Adalet Divanı (AAD), Direktifin 3 (2) maddesinin uygulanmasına yönelik dar bir yaklaşım benimsemiştir. Mahkeme istisnanın, internette yayına dayanan kişisel veri işlemeyle açık bir şekilde ilgisi olmayan, bireylerin özel veya aile hayatı sırasında yürütülen faaliyetlere ilişkin olarak yorumlanması gerektiğine karar vermiş-

11 **D'afflitto Rosario Imperiali**, *European Union Directive On Personal Privacy Rights And Computerized Information*, Villanova Law Review, Cilt: 41, Sayı: 1, 1996, s. 313-315

12 **Oxman Stephen A**, *Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?* Boston College International & Comparative Law Review, Cilt: 24, 2000, s. 194

13 Kaplan, s. 39-40

14 **Maxeiner James R**, *Freedom of Information and the EU Data Protection Directive*, Federal Communications Law Journal, Cilt: 48, 1996, s. 100

tir[15].

C. ANAHTAR TERİMLER

1. KİŞİSEL VERİ

AB'nin veri koruma kanunu kendine özgü terminolojisiyle doludur. En önemli terimlerden birisi, AB veri koruma kanunu tarafından sağlanan bilgi olan 'kişisel veri'dir. Bu terim, 2 (a) maddesinde belirlenen veya belirlenebilen bir gerçek kişiyle ilgili herhangi bir bilgi olarak tanımlanmaktadır. Buna bağlı olarak, 'belirlenebilir kişi', özellikle bir kimlik numarasına veya kişinin "fiziksel, psikolojik, akli, ekonomik, kültürel veya sosyal kimliğine" özel, bir ya da daha fazla faktöre ilişkin olarak doğrudan veya dolaylı olarak belirlenebilen kişidir.

Kişisel verilerin kapsamı oldukça geniştir ancak sınırsız değildir ve bir bireye uzanabilen hemen hemen her türden veriyi içermektedir[16]. Bu sadece ad, adres veya sosyal güvenlik numarası gibi bireyin kimliğine atıfta bulunan temel gerçeklere dayanan bilgiyi içermemekte, aynı zamanda satın alma kayıtları veya web sitesi ziyaretleri gibi bireyin kişisel tercihlerini açığa çıkaran bilgileri de içermektedir[17].

Direktifin 2 (a) maddesi; bireylerin belirlenemediği durumlarda tüzel kişiler ve kişi grupları hakkında herkesin serbestçe bilgi toplama, işleme ve rapor edebilmeleri anlamına gelmektedir[18]. Bu durum sadece metinsel bilgileri değil aynı zamanda ölü ya da diri olsun belirli veya belirlenebilir bir kişinin fotoğrafları, görsel-işitsel görüntüleri ve ses kayıtlarını da içerecektir[19]. Örneğin, telefon bankacılığında müşterinin bankaya talimat verdiği sesi sisteme kaydedildiği zaman, bu kaydedilen talimatlar kişisel veri olarak düşünülmelidir. Ayrıca, güvenlik kamera sistemi tarafından kaydedilen görüntüler bireylerin tanınabilir olması ölçüsünde kişisel veri olabilir.

2. VERİ İŞLEME

'Veri işleme' terimi de dikkat çekicidir ve AB veri koruma kanununun kapsamını daha da genişletmektedir. İşleme, kişisel verilerin

15 Bkz: C-101/01, *Bodil Lindqvist v. Jönköping*, Davası, [2003] ECR I- 12971, para 47
16 **Johnson Elizabeth H**, *Data Protection Law in the European Union*, The Federal Lawyer, 2007, s. 44
17 Oxman, s. 191
18 Maxeiner (1996), s. 100
19 **Cate Fred**, *The European Data Protection Directive and European-US Trade*, Currents: International Trade Law, Cilt: 7, 1998, s. 62

toplanması ile başlar silinmesine kadar devam eder. Kişisel verilerin işlenmesi, uzun ve birçok işlemi içerir niteliktedir[20]. Direktif bu terimi "*silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi*" olarak tanımlamaktadır. Bu tanım, kişisel verilerin hemen hemen her türlü kullanımını içermektedir. Aslında yalnızca kişisel verileri saklama eylemi Direktifin gerekliliklerine işaret etmektedir[21].

3. VERİ KONTROLÖRÜ (DENETLEYİCİ)

Direktifin 2 (d) maddesi; veri denetleyicisini, tek başına ya da diğerleriyle müşterek olarak kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen kişi olarak tanımlamaktadır. Bu bağlamda, veri kontrolörü bilgisayarda veya yapılandırılmış elle yazılan dosyalarda kişisel verilerin saklanması ve kullanılmasını kontrol eden ve bunlardan sorumlu olan birey ya da tüzel kişidir.

Veri kontrolörleri gerçek kişiler olabildiği gibi şirket, hükümet kurumları veya gönüllü organizasyonlar gibi tüzel kişiler de olabilirler. Veri kontrolörünün bir gerçek kişi olduğu durumlar arasında, hastaları hakkında doktorlar, seçmenleri ile ilgili politikacılar ve müşterileri hakkındaki kişisel bilgileri saklayan bağımsız tüccarlar örnek olarak gösterilebilir. Bir bireye bir şirkette veri koruma sorumluluğu yüklense bile, onlar veri kontrolörü olan şirket adına hareket ederler[22].

4. VERİ İŞLEYİCİ

Direktifin 2 (e) maddesi uyarınca veri işleyici veri kontrolörü adına kişisel verileri işleyen gerçek veya tüzel kişidir; ancak veri işleyicisi, çalışması sırasında bu tür verileri işleyen bir veri kontrolörünün çalışanını kapsamamaktadır.

Uygulamada, veri kontrolörleri, zaman ve maliyet tasarrufu sağlamak için verilerini işlemek üzere sıklıkla üçüncü taraf yani harici kişi ya da şirketleri kullanmaktadırlar. Üçüncü taraf, yalnızca veri kontrolörünün emri üzerine hareket ettiği, ancak veri işleme-

20 Ö**zdemir Hayrunnisa**, *Haberleşmenin Gizliliği ve Kişisel Veriler*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XIII, Sayı: 1–2, 2009, s. 291

21 Kaplan, s. 40

22 *Key definitions of the Data Protection Act,* online at: http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions, ET: 26.06.2013

nin amacını kendisi belirlemediği için, bu kişi veri işleyici olacaktır. Veri işleyicilerine örnek olarak, başkası adına kişisel bilgi saklayabilen veya işleyebilen sigorta şirketleri, muhasebeciler veya pazar araştırma şirketleri gösterilebilir[23].

Belirtmek gerekir ki, bir şirket ya da bireyin kişisel verilerin belirgin grupları bakımından hem veri kontrolörü hem de veri işleyicisi olması mümkündür. Örneğin, bir sigorta şirketi kendi çalışanı hakkındaki veriler açısından 'veri kontrolörü' olacaktır; ancak müvekkil şirketler için işlediği çalışan bordrosuna ilişkin olarak 'veri işleyicisi' olacaktır.

İlgili anahtar terimleri açıklığa kavuşturmak için bir örnek vermek yararlı olacaktır. Mayflowers Ltd adli bir şirket ulusal bir gazetede mutfak ürünlerinin reklamını yapmaktadır. Robert reklamı görüp bir broşür için şirkete telefon eder. İsmini, telefon numarasını, doğum tarihini ve adresini verir. Telefon operatörü bu bilgileri Robert konuşurken şirketin bilgisayar veri tabanına girer. Bu örnekte, Direktifin terminolojisi aşağıdaki gibi uygulanır:

Kişisel veriler: Robert'ın adı, telefon numarası, doğum tarihi ve adresi hakkında bilgi.

İşleme: Bu, kişisel verilerin bilgisayar sistemine girildiği, elektronik ortamda saklandığı, ekranda okunduğu veya basılı materyalde kullanıldığı yerde meydana gelir.

Veri öznesi: Robert.

Veri kontrolörü: Mayflowers Ltd şirketi.

D. VERİ KORUMA İLKELERİ

Veri koruma ilkeleri mevzuatın belkemiğini oluşturmaktadır. İlkelerin çoğu mahremiyeti koruma ve bireylerin özel hayatına uygunsuz ve gereksiz müdahaleleri önleme ihtiyacıyla bağlantılıdır. İlkeler, Avrupalı veri kontrolörlerinin kişisel verileri işlerken uyması gereken birtakım yükümlülüklerden oluşmaktadır. Bu ilkelerin, kişisel verilerin işlenmesi hususunda veri kontrolörleri ve veri özneleri arasında çakışan çıkarları dengelemede Direktifin arabulucu rolünde kilit nokta olduğu söylenebilir[24].

23 **Carey Peter**, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Second Edition, 2004, , s. 19

24 **Wong Rebecca and Savirimuthu Joseph**, *All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, Journal of Computer & Information Law, Cilt: 25, 2008, s. 243

1. VERİ KALİTESİNE İLİŞKİN İLKELER

a. Adil ve Yasal

Direktifin 6 (1) (a) maddesi uyarınca, kişisel veriler adil ve yasalara uygun bir şekilde işlenmelidir. Yasalara uygunluk gereksinimi nispeten açık olmasına karşın, adillik gereksinimi kısmen belirsizdir. Aslında veri işlemenin adil olması gereksinimi temel bir yasal genellemedir. Bazı ülkeler adillik gereksinimini tanımlamak için adımlar atmış olmasına karşılık, diğerleri bunu DPA'ların takdirine bırakmaktadır[25].

b. Amaç Sınırlamalı

6 (1) (b) maddesi kişisel verilerin "*belirli, açık ve meşru amaçlar için toplanması gerektiği ve bu amaçlarla uyumsuz bir şekilde daha fazla işlenmemesi gerektiğini*" belirtmektedir. Maddeden açıkça anlaşılacağı üzere, 'belirli' ve 'açık' olan bir amaç aynı zamanda 'meşru' olmalıdır. Bu, kanunilik ilkesi ile aynı değildir. Belli faaliyetler teknik olarak kanun içerisinde olabilir ancak meşru olmayabilir. Bu ilkenin bir uzantısı olarak, gelecekte olası kullanıma olanak yaratılması için kişisel verilerin toplanması da mümkün değildir[26].

c. İlgili ve Orantılı

Kişisel verilerle ilgili üçüncü ilke, 6 (1) (c) maddesinde belirtildiği üzere, orantılılık veya yeterlilik ilkesidir. AB Direktifi kişisel verilerin "toplandığı ve/veya daha fazla işlendiği amaçlarla ilişkin olarak yeterli, ilgili olması ve aşırı olmaması" gerektiğini şart koşarak, toplanabilen verilerin niteliğini ve miktarını sınırlamaktadır. Esasen bu, veri kontrolörlerinin bu tür verileri işlemek için veri kontrolörünün amacı için gerekli olan bilgileri veri öznelerinden almalarını zorunlu kılmaktadır. Ancak bu, belli bir zaman süresinden sonra veya veri öznesinin talebinin hemen ardından bir kişinin kişisel verilerinin silinmesini talep etmek için somut ve icra edilebilir yasal bir hak sağlamamaktadır.

Örneğin, Magdalen İstihdam Şirketi işe başvuranların kendi sürücü belgesi numaralarını belirtmelerini standart müşteri detayları formunda gerekli kılsın. Şoförlük mesleği ile ilgili olmayan bir işe başvurmayı isteyen David, kendi sürücü belgesinin detaylarını içeren

25 **Korff Douwe**, *Data Protection Laws in the European Union*, the Direct Marketing Association, 2005, s. 37-38

26 **Uygun Murat**, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010, s. 55

formu doldursa, bu durumda şirket, David'in sürücü belgesinin detaylarını işleyerek bu ilkeyi ihlal etmiş olur.

d. Doğru

Doğruluk terimi verilerin temel niteliklerinden birisidir. Yanlış kimlik tespiti gibi en basit türdeki bir hata, kavramsal olarak üstesinden gelinebilecek en basit hatadır[27]. 6 (1) (d) maddesi kişisel verilerin "*doğru ve gerekli olduğu yerde güncellenmesi gerektiğini; toplandıkları ve daha fazla işlendikleri amaçları dikkate alarak doğru olmayan veya noksan olan verilerin silinmesini veya düzeltilmesini sağlamak üzere makul her adımın atılması gerektiğini*" belirtmektedir.

Bu maddenin uygulamadaki zayıflığı veya eksikliği, veri toplamanın niteliğini yeterince tanıyamamasıdır. Veri toplayıcılarının her zaman sahip olamayacağı odaklanmış bir amacın olduğunu var saymaktadır. İş adamları ve bilim profesyonelleri bazen doğruluğundan veya amaca uygunluğundan emin olmadan önce bir takım bilgiler elde ederler. Sadece bu tür verileri kullandıktan sonra kullanıcı, bilginin doğruluğu veya kullanılabilirliğini belirleyebilmektedir[28].

e. Zaman Sınırlamalı

6 (1) (e) maddesi uyarınca kişisel veriler, "*bu verilerin toplandığı veya daha fazla işlendiği amaçlar için gerekenden fazla olmayacak şekilde veri öznelerinin kimliğinin tespitine izin veren bir şekilde saklanmalıdır*." Artık gerekli olmayan bilgiler ise yok edilmelidir. Eğer yok edilmezse, ya da bilginin ilk toplandığı veya işlendiği amaç dikkate alındığında artık gerekmeyecek şekilde saklanırsa, bu ilke ihlal edilmiş olacaktır. Verilerin saklanması, erişilmek istenen amacın gerçekleşmesine kadar hukuka uygun olacaktır[29].

2. MEŞRU VERİ İŞLEME KRİTERLERİ

a. Rıza

Kişisel verilerin "*veri öznesinin rızasını açık bir biçimde verdiğinde*" işlenebildiği belirtmektedir[30]. Ayrıca Direktifin 2 (h) maddesinde, rızanın hem bilgilendirilmiş hem de gönüllü olması gerektiği ifade edilmektedir. Bu koşul açık görünmesine rağmen, bazen uygula-

27 **Karst Kenneth L**, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 Law and Contemporary Problems, 1966, s. 353

28 **Maxeiner James R**, *Business Information and Personal Data: Some Common-Law Observations about the EU Draft Data Protection Directive*, Iowa Law Review, Cilt: 80, 1995, s. 634

29 **Başalp Nilgün**, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara, 2004, s. 39

30 Bkz: Direktifin 7 (a) maddesi.

mada sorunlar olabilmektedir[31]. Buradaki irade açıklaması, dışarıya vurulan, muhatap taraf açısından objektif bir değerlendirme ile onay şeklinde anlaşılabilen bir davranıştır. İlgilinin susması ise rıza olarak değerlendirilemez[32].

b. Sözleşme

Direktifin 7 (b) maddesi uyarınca, kişisel veriler "*bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi amacıyla*" işlenebilir. Bu, bir sözleşmenin belirli bir amacına ulaşmak için gerekli olan verilerin işlenmesine uygulanmaktadır. Problem, örneğin, devredilemez bir sözleşme içerisinde veri işlemenin gerektiği, ancak bu sözleşmenin amacını karşılamak için sıkı bir şekilde gerekli olmayan durumlarda görülmektedir[33]. Aslında bu durumlarda hükümlerin icrası, duruma özgü veri koruma kanununa dayanabilir. Bu bakımdan vurgulanmalıdır ki, bu koşul veri öznesinin taraf olduğu bir sözleşmeye atıfta bulunmaktadır. Bu nedenle, veri kontrolörünün veri öznesiyle beraber sözleşmeye taraf olması gerekli değildir[34].

c. Yasal Yükümlülükler

Kişisel verilerin "*veri kontrolörünün tabi olduğu bir yasal yükümlülüğe uyum için gerekli olduğu*" zaman işlenebileceği Direktifin 7 (c) maddesinde belirtilmektedir. Bu hüküm açık bir şekilde ifade edilmesine karşılık, bazı yasal yükümlülüklerin kişisel verilerin işlenmesini haklı göstermeyebileceği muhtemeldir. Hükmün, AB sınırları içerisinde ortaya çıkan yasal yükümlüklere kesinlikle uygulanacağı belli olmasına rağmen, bunun başka yerde ortaya çıkan yasal yükümlülüklere uygulandığı tam olarak açık değildir[35].

d. Hayati Menfaat

Bu kriter 7 (d) maddesinde "*kişisel verilerin veri öznesinin hayati menfaatlerini korumanın gerekli olduğu*" zaman işlenebildiği şeklinde belirtilmektedir. 'Hayati' ifadesi bu koşulun kilit noktasıdır ve Direktifin Önsözünün 31. fıkrasında veri öznesinin hayatı için gerekli olan bir menfaatin korunmasına atıfta bulunduğundan dolayı dar bir biçimde yorumlanabilir. Bu nedenle, sadece acil bir durum kapsam içinde olacaktır. 'hayati menfaatlerin' yalnızca ölüm kalım

31 **Kosta Eleni**, *Consent in European Data Protection Law*, 2013, s. 110
32 Şimşek Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınları, İstanbul, 2008, s. 45
33 Kaplan, s. 41
34 Carey, s. 74
35 **Kinton John D**, *Managing the EU-US Discovery Conflict*, Law 360, 2008, bkz: http://www.law360.com/articles/72082/managing-the-eu-us-discovery-conflict, ET: 29.06.2013

durumlarında uygulanması kuvvetle muhtemeldir[36].

Örneğin, İspanya vatandaşı olan Susan, kayak tatili için Avusturya'ya gidiyor. Pist dışında kayarken bir çığa yakalanıyor ve acil olarak hastane tedavisine ihtiyaç duyuyor. Avusturya'daki hastane Susan'ın tıbbi kayıtlarının İspanya'dan transfer edilmesini istiyor. Ancak Susan'ın bilinci açık olmadığı için buna rıza gösteremiyor. Bu durumda, Susan'ın fiziksel sağlığı yani hayatı için gerekli olduğu gerçeğinden hareketle, Susan'ın doktorunun veri işlemesi bu durumda meşru olmaktadır.

e. Kamu Menfaati

Kişisel veriler, "*verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu otoritesinin uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekli olduğu zaman*" işlenebilir[37]. 'Kamu menfaati' terimi belirsizdir ve yapılan yorumlar AB'de farklılık gösterebilir. Örneğin, Belçika'da epidemiyolojik[38] amaçlar için veri işlemenin kamunun menfaatine olduğu varsayılmaktadır ve bu nedenle ön rıza olmadan da veriler işlenebilmektedir. Buna benzer bir şekilde, 'resmi bir otoritenin görevi sırasında' ifadesi Üye Ülkeler arasında farklı olarak yorumlanabilir. İç mevzuat yalnızca devlet kurumları veya kamu hukuku ve özel hukukuna tabi, gerçek veya meslek dernekleri gibi tüzel kişilerin bu istisna altında nitelendirilip nitelendirilmeyeceğini belirleyecektir[39].

f. Meşru Menfaat

Kişisel veriler "İşleme, bu tür menfaatlerin, madde 1 (1) kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çiğnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen *meşru menfaatlerin amaçları için gerekli olduğu zaman*" işlenebilir[40]. Bu hüküm tarafından ileri sürülen çıkarları dengeleme türü, Üye Devletlere, veri işlemeye izin verildiği zaman bunu belirleme konusunda dikkate değer bir esneklik sunmaktadır. Bu anlamda, bireysel veri koruma kanunları bu tür bir veri işlemenin 'gerekli' ol-

36 Carey, s. 75

37 Bkz: Direktifin 7 (e) maddesi ve Önsözün 32. maddesi.

38 Epidemiyoloji, toplumdaki hastalık, kaza ve sağlıkla ilgili durumların dağılımını, görülme sıklıklarını ve bunları etkileyen belirteçleri inceleyen bir tıp bilimi dalıdır.

39 **Bergkamp Lucas and Dhont Jan**, *Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*, The EDI Law Review, Cilt: 7, 2000, s. 82

40 Bkz: Direktifin 7 (f) maddesi.

duğu zamanki kapsamın ana hatlarını net bir şekilde çizmektedir[41].

Direktif, meşru menfaat terimini tanımlamamaktadır. Ancak Direktifin 30. Beyanı (Önsözü) "şirketler ve diğer organların meşru olağan iş faaliyetlerine" atıfta bulunmaktadır. Sonuç olarak, meşru menfaatler muhtemelen doğrudan pazarlamayı içerebilen 'meşru iş çıkarlarını' kapsamaktadır[42]. "Bu hükmün sınırlamalar veya müdahalelerin demokratik bir toplumda gerekli olması şartıyla meşru bir amaç için bu tür haklara, kısıtlama veya müdahaleye izin veren, AİHS'deki temel somut maddelerin yapısını yansıttığını belirtmek yeterli olmalıdır. AİHM, bu yaklaşım temelinde ayrıntılı testler geliştirmiştir. Böylece bu testler, Direktif uyarınca bu kriterlerin uygulanmasında da geçerlidir"[43].

3. HASSAS VERİ

AB Direktifi, 8 (1) maddesinde özellikle hassas olduğu düşünülen kişisel verilerin korunmasına ek bir koruma daha eklemektedir. Belli başlı kişisel veriler şayet "ırksal veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliği*, ve...sağlık veya seks hayatını*" içeriyorsa daha yüksek liyakate sahiptir. Bu doğrultuda, Direktif, Üye Devletleri istisnai bazı durumlar dışında tüm hassas verilerin işlemesini yasaklamaya zorlamaktadır[44]. Bu sınırlı ve istisnai haller aşağıdaki durumlarda söz konusudur:

- bir veri öznesi açık rıza göstermişse,
- veri öznesinin (veya başka bir kişinin) hayati menfaatlerini korumak gerekliyse ve bu durumda veri öznesi fiziksel veya hukuken rıza veremiyorsa,
- veri işleme, amacı hassas verilerin çeşitlerinden birine ilişkin bir gündemi yürütmek olan kar amacı gütmeyen bir kuruluş tarafından yürütülüyorsa,
- işleme; yalnızca amaçlarıyla bağlantılı olarak düzenli iletişimde oldukları kişileri veya kuruluş mensuplarını ilgilendirmesi koşuluyla bir vakıf, dernek veya siyasi, felsefi, dini veya ticaret birliği amaçlı başka bir kar amacı gütmeyen kuruluş tarafından

41 Kaplan, s. 42

42 Bergkamp, s. 81

43 **Korff Douwe**, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, 2010, bkz: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, ET: 28.06.2013, s. 68

44 D'afflitto, s. 314

uygun teminatlı meşru faaliyetler esnasında yapılıyorsa,

- veri, veri öznesi tarafından açık bir şekilde aleni hale getirilmekteyse,
- kanuni hakların tesisi, yerine getirilmesi veya savunulması için gerekliyse ve
- sağlık sebeplerinden dolayı gerekliyse,

Pratik açıdan, hassas verilerin işlenmesi, listelenen tüm diğer durumların ticari bir ortamda nadiren mevcut olmasından dolayı veri öznesinin açık bir rızasını neredeyse her zaman gerektirmektedir. Açık rıza gereksinimi bireyin veri işlenmesine yönelik onayını açık bir şekilde belirtmesini ifade etmektedir[45]. Bu, aşağıda açıklanan 'opt-in' ve 'opt-out' rızanın yeterli olmadığı anlamına gelmektedir[46]. Hassas olmayan verilerin bazen hassas verilerle bağlantılı olmasından dolayı rıza gereksiniminin sonuçları, salt hassas verinin kapsamı dışına çıkabilmektedir[47].

Belirtmek gerekir ki, bu kriterleri karşılamak, Direktif tarafından getirilen diğer gereksinimleri uygulamamak anlamına gelmemektedir. Bazı Üye Devletlerde pazarlama amaçlarından dolayı kişisel verilerin işlenmesi, hiçbir rıza alınmamasına rağmen meşruiyet testini geçebilir. Ancak rıza, bu amaçlarla hassas verileri işlemek için her zaman gerekmektedir. Dolayısıyla tıbbi veya farmakolojik ürünleri ve hizmetleri sunan bir web sitesini ziyaret eden veri öznelerine sunulan doğrudan pazarlama amaçlarına yönelik bir opt-out düzenlemesi yeterli varsayılmayacaktır. Sağlık verileri doğrudan pazarlama hedefleri için işlendiği zaman, sadece bir opt-in formülü yeterli olacaktır[48].

AB'de rıza göstermenin en yaygın yolu, opt-out ya da opt-in metodunu kullanmaktır. Bu tür bir şart, bir kullanıcının verilerini özel olarak belirtilmiş bir amaç için kullanılmasını istemediğine dair bir işareti tik atarak belirtmesini sağlayan bir kutuyla (opt-out) ya da

45 **Kuner Christopher**, *European Data Privacy Law and Online Business*, Oxford University Press, 2003, s. 70

46 Dünyada istek dışı haberleşme konusunda; alıcının ilk elektronik postadan sonra reddetme hakkı olarak tanımlanan "opt-out" ve elektronik iletilerin ilkinde dahi önceden izin alma şartı getiren ve "opt-in" sistemi olarak adlandırılan iki farklı düzenleme bulunmaktadır. İlk yöntem, Amerika Birleşik Devletleri ve Uzak Doğuda; ikinci yöntem ise Avrupa Birliğine üye ülkelerin genelinde uygulanmaktadır. (Türkiye uygulaması için bkz, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı, http://www2.tbmm.gov.tr/d24/1/1-0488.pdf, ET: 17.02.2014)

47 **Corien Prins**, *When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?* SCRIPT-ed, Cilt: 3, Sayı: 4, 2006, s. 291

48 Bergkamp, s. 82-83

kullanıcının özel olarak belirlenmiş veri işlemeyi kabul etmesini gösteren bir kutuyla (opt-in) birlikte verilerin istenilen kullanım beyanından meydana gelir[49].

Örneğin, bir şirket Michael'a spor ürünlerine dair bilgi gönderiyor. Şayet 'bu şekilde irtibata geçilmesini istemiyorsanız lütfen kutuya tik atın' yazan bir ibare mevcutsa o halde bu opt-out şartıdır. Diğer taraftan, şayet şirket seçili bir iş ortağına verilerini kullanılabilir hale getirmek istiyorsa ve 'bu şekilde irtibata geçilmesini istiyorsanız lütfen kutuya tik atın' yazan bir ibare mevcutsa, o halde bu bir opt-in şartıdır.

Direktifteki hassas veri tanımı oldukça geniş olmasına karşılık, bazı Üye Devletler bu tür verileri diğerlerinden daha geniş bir biçimde tanımlamaktadır. Örneğin, Portekiz, tüketici ve ev alışkanlıklarına ilişkin verilerin toplanmasına yönelik açık rıza gerektirecek tanım içerisinde bireyin 'özel hayatı' hakkında verileri içermekteyken; İngiltere'de bu tür veriler kesinlikle 'hassas olmayan veriler' olarak muamele görecek ve dolayısıyla daha düşük seviyede koruma gerektirecektir[50]. Benzer şekilde, Direktiften farklı olarak, örneğin, genetik bilgilere (Polonya, Estonya), ten rengine (İzlanda), dernek üyeliğine (İtalya), özür durumuna (Estonya), alkol, tıbbi ilaç ve uyuşturucu kullanımına (İzlanda) ilişkin veriler de veri koruma kanunlarında hassas veri olarak kabul edilmiştir[51].

E. DENETLEME MERCİLERİ

Direktif, herkesin kendi sınırları içerisinde Direktifin uygulanmasını gözetmek için tüm AB Üye Devletleri'nin bağımsız bir kamu mercisi oluşturmasını zorunlu kılmaktadır. Denetleme mercilerinin, bu bağlamda, minimum seviyede, veri koruma konularını araştırma, rehberlik sağlama, ulusal kanunların ihlal edildiği yargılamalara dâhil olma ve yargı mercilerinin dikkatini ihlallere çekme konularında geniş görevleri bulunmaktadır. Olası veri koruma etkisi ile düzenlemeler için taslak oluşturulduğunda bu mercilere danışılmalıdır. Bağımsız denetlemeye olan bu vurgu, veri koruma ile ilgili Avrupa yaklaşımının vazgeçilmez bir özelliğidir[52]. Direktif, aynı zamanda, '29. Madde Çalışma Grubu' olarak bilinen kurumu

49 Carey, s. 254

50 **Charlesworth Andrew**, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?* Hastings Law Journal, Cilt: 54, 2003, s. 940

51 **Kaya Cemil**, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul *Ü*niversitesi Hukuk Fakültesi Mecmuası, Cilt: LXIX, Sayı: 1 - 2, 2011, s. 319

52 Robinson, s. 21

da oluşturmuştur. Bu, kısmen her Üye Devlet tarafından belirlenen denetleme mercilerinin temsilcilerinden oluşmaktadır[53].

AAD, denetleme mercisinin bağımsız olmasının, denetlenen kurumlar tarafından gerçekleştirilen her türlü etkiyi önleyeceğini ifade etmiştir. Bu bağımsızlık olgusu, özel hayat hakkının korunması ve kişisel verilerin serbest dolaşımı arasındaki adil dengeyi kurmakla görevli mercilerin performansının doğruluğunu sorgulayan, doğrudan ya da dolaylı her türlü dış etkiyi de engellemektedir. Mahkeme, aynı zamanda özel hayat hakkının koruyucusu olan bu merciler tarafından benimsenen rolün amaçlarına yönelik olarak, almış oldukları kararların ve böylece mercilerin kendilerinin, her türlü yanlılık şüphesinden uzak kalmasının önemli olduğunu belirtmiştir[54]. Bir denetleme mercisi, Direktif'in ilkeleri ile uyumlu olmalıdır. "Veri konusu (veri sahibi), yetkili mercinin kararlarına itiraz etmek istediğinde ya da mahremiyet hakkının üçüncü taraflarca ihlalinin devamı halinde, veri sahibi, her zaman yargıya başvurabilir"[55].

Belirli kurumsal düzenlemeler ülkeden ülkeye farklılık gösterebilir. Mesela, Hollanda'da, sağlık ve telekomünikasyon gibi alanlarda diğer sektörlerle birlikte genel sorumluluk verilmiş bir Veri Koruma Mercisi bulunmaktadır. Merkezi olmayan bölgesel kuruluşlar ile Almanya gibi federal devletler, bölgesel düzeyde hizmet veren görevli devlet-altı ajanslar ile ulusal kuruluşlar kabul etmişlerdir. Örneğin Romanya gibi diğer devletler, mahremiyet haklarını gözetmeleri ile sorumlu Ombudsman kuruluşlarını kullanmakta iken, Finlandiya'daki eş değer kuruluşlar sadece kişisel verileri korumaktadır[56].

F. ÜÇÜNCÜ ÜLKELERE KİŞİSEL VERİLERİN TRANSFERİ

AB Direktifi'nin belki de en ihtilaflı hükümleri, kişisel verilerin üçüncü ülkelere transferine ilişkin olanlarıdır. Bu bağlamda 25. madde, geniş çapta tartışmaların temelini oluşturmaktadır. Çünkü bu madde, AB'nin düzenleme kapsamını dış hukuka kadar genişlettiği çok nadir durumlardan birini teşkil etmektedir[57]. Bir kez daha belirtmek gerekir ki, AB sistemi Direktif'in ikili amacını, serbest bil-

53 **Garrie Daniel, Duffy-Lewis Maureen and Wong Rebecca**, *Data Protection: The Challenges Facing Social Networking*, International Law & Management Review, Cilt: 6, 2010, s. 130

54 Bkz: C-518/07, *Commission v Germany* Davası, [2010] ECR I- 1885.

55 D'afflitto, s. 320

56 *Data Protection in the European Union: the Role of National Data Protection Authorities*, 2010, s. 19, bkz: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, ET: 19.06.2013

57 **Koutsias Marios**, *The International Reach of European Union Data Protection Law and the United States: is International Trade in a Safe Harbour?* International Trade Law & Regulation, Cilt: 18, Sayı: 2, 2012, s. 32

gi akışı ve etkin veri korumayı, gerçekleştirmeyi amaçlamaktadır[58]. Ancak AB ülkelerindeki veri koruma seviyelerindeki farlılıklar, kişisel verilerin bir ülkeden diğerine olan akışını engelleyebilir. Bu farklılık, Birlik düzeyinde birçok ekonomik faaliyet arayışına engel teşkil edebilir. Bu yüzden Direktif, Üye Ülkeler arasında korumaya yönelik katı standart kurallar koymakta ve Birlik içerisinde sınıraşırı veri akışı önündeki engelleri ortadan kaldırmaktadır[59].

Esasen Direktifin temel amacı, kişisel verilerin Avrupa Birliğine üye ülkeler arasında serbest dolaşımına katkıda bulunmaktır. Ancak bu veri trafiğinin kişilerin temel hak ve özgürlüklerine zarar vermesini engellemek için üye ülkelerin mevzuatları birbiriyle uyumlu hale getirilmeye çalışılmaktadır. Ancak Birliğe üye olmayan ülkeler bakımından Direktifle sağlanan korumanın bir anlamı bulunmamaktadır[60].

Direktif, aynı zamanda, AB dışına veri transferini de düzenlemekte ve sınırlı şartlar haricinde üçüncü ülkelere (üye olmayan) bu transferi açık bir şekilde engellemektedir. Ancak AB dışında Direktif'in bu gibi bir etkisinin olmadığını ve koruma düzeyinin ulusa göre daha fazla bir şekilde farklılık gösterdiğini de belirtmek gerekir. Direktif'in 25 (1) maddesine göre bu gibi bir transfer ancak, alıcı ülkede yeterli seviyede veri koruma sağlanıyorsa, kabul edilebilir[61]. Yukarıda bahsedilen kısıtlamalar, Direktif'e kendi sınırları dışında fiili bir etki sağlamaktadır. Kişisel verilerin AB dışına transferinin engellenmesinin istisnaları, aşağıda belirtildiği üzere üçe ayrılabilir[62].

1. DURUMA ÖZGÜ İSTİSNALAR

Kişisel verilerin AB dışına transferinin engellenmesine olan duruma özgü istisnalar, kişisel verilerin ne zaman işlenebileceğini belirleyen durumlara benzemektedir. 26 (1) maddesinde Direktif, mahremiyete yönelik olarak yeterli koruma sağlayamayan üçüncü ülkelere veri transferi engellemesinden sapma öngörmektedir. Bu istisnalar; daha önceden açıklanan meşru veri işleme kıstasları ile

58 Bainbridge David, *Processing Personal Data and the Data Protection Directive*, Information & Communications Technology Law, Cilt: 6, Sayı: 1, 1997, s. 17

59 **Kong Lingjie**, *Data Protection and Trans-Border Data Flow in the European and Global Context,* European Journal of International Law, Cilt: 21, 2010, s. 443

60 **Atak Songül**, *Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri*, Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi, Sayı: 59-60, 2009, s. 214

61 **Swire Peter and Litan Robert**, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998, s. 31

62 Kaplan, s. 43

aynı şekilde, rıza, sözleşme, kamu menfaati, hayati menfaat ve meşru menfaattir.

2. ÜLKEYE ÖZGÜ İSTİSNALAR

a. Yeterli Koruma Seviyesi

Direktif'in 25. Maddesi[63], eğer üçüncü ülke 'yeterli seviyede koruma' sağlıyorsa, verilerin transfer edilebileceğini hüküm altına almaktadır. Ancak Direktif, yeterlilik hakkında durum bazında "veri transferini çevreleyen tüm durumların ışığında değerlendirilmelidir" tespitini yapmaktan başka, yeterliliğin nasıl tanımlanacağı ya da tespit edileceği konusunda bize çok fazla yardımcı olmamaktadır[64]. 'Yeterli seviyede koruma' ilkesi ile neyin kastedildiğinin tam olarak açıklanmamasından dolayı, AB Üye Ülkeleri içerisinde farklı uygulamaların ortaya çıkma riski bulunmaktadır. Veri kontrolörü, verilerin dışa transferi için en düşük veri koruma seviyesine sahip olan ülkeyi ihtimal dâhilinde seçebilir. İşte bu nedenledir ki, Direktif karar verme konusunda uyumlu bir uygulama sunmaktadır[65].

Ancak, Avrupa Komisyon'una 'yeterli seviyede koruma' sağlayan olarak bazı ülkeleri belirleme görevi verilmiştir. Çoğu ülkenin, kişisel verilerin korunmasına ilişkin kanunları bulunmasına rağmen, şu ana kadar bunlardan çok azının AB tarafından yeterli kanunlara sahip olduğu belirtilmiştir[66]. Bunu gerçekleştiren ülkeler arasında üç Avrupa Ekonomik Alanı'nın (AEA) AB üyesi olmayan ülkeleri; Norveç, Lihtenştayn ve İzlanda'dır. Bunun yanında Komisyon'un yeterli seviyede koruma sağladığını belirlediği diğer ülkeler; İsviçre, Kanada, Arjantin, İsrail ve Avustralya'dır[67].

63 İlgili maddeye göre; "Üye Devletler, bu Direktifin diğer hükümleri uyarınca benimsenen ulusal hükümlere uyuma zarar vermeksizin, yalnızca söz konusu üçüncü ülke yeterli koruma seviyesi sağlarsa, transfer sonrası işleme için istenen veya işlemeye tabi olan kişisel verilerin bir üçüncü ülkeye transferinin gerçekleşebilmesini sağlayacaktır. Bir üçüncü ülke tarafından sağlanan koruma seviyesinin yeterliliği, veri transfer faaliyetlerinin dizisinin veya bir veri transfer faaliyetini çevreleyen tüm koşulların ışığında değerlendirilecektir."

64 **Hobby Seth**, *The EU Data Protection Directive: Implementing A Worldwide Data Protection Regime and How The U.S. Position Has Progressed*, International Law & Management Review, Sayı: 1, 2005, s. 173

65 **Zinser Alexander**, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, Tulane Journal of Technology & Intellectual Property, Cilt: 6, s. 172-173

66 **Bond Robert**, *International Transfers of Personal Data - an Update*, Business Law International, Cilt: 5, No: 3, 2004, s. 424

67 Kişisel verilerin korunması ile ilgili gerekli yeterliliğe sahip olan ülkelerin tümünün listesi için bkz: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, ET: 07.07.2013

b. Güvenli Liman

AB Direktifi, AB'nin mahremiyet koruma yeterlilik standardını karşılamayan ve AB üyesi olmayan ülkelere kişisel verilerin aktarılmasını engellemektedir. Bu tür bir koruma ülke düzeyinde ya da kurumsal düzeyde olabilir. Amerika Birleşik Devletleri (ABD) ve AB, vatandaşları için mahremiyet korumasını geliştirmeyi amaçlamaktayken; ABD, mahremiyete AB'den farklı bir perspektiften bakmaktadır. Yaklaşımlardaki bu farklılığı gidermek ve ABD kuruluşlarının Direktif ile uyumlu olmalarını sağlamaya yönelik geliştirilmiş yöntemler sağlamak için ABD Ticaret Bakanlığı, Avrupa Komisyonu ile istişare ederek, Güvenli Liman çerçevesini oluşturmuştur[68].

AB ve ABD Ticaret Bakanlığı, kendilerini resmen Güvenli Liman olarak sertifikalandıran ABD'deki kuruluşlara AB'den gelen kişisel verilerin transferine izin veren hükümleri belirleyen görüşmelere 2000 yılında başlamışlardır. Bu süreç, bir ABD şirketine ya da ona bağlı olan bir şirkete, verileri Direktif'in belirttiği şekilde işleme koymayı kabul ettiğinde, AB'den kişisel veri alabilmelerini sağlamaktadır. Güvenli Liman kuruluşuna transfer edilen kişisel veriler, örneğin, maaş bordrosu verilerini, çalışanların değerlendirmelerini, müşteri listelerini, fatura bilgilerini ve Güvenli Liman sürecinin bir parçası olarak ABD içerisinde davası süren bir eser için toplanan belgeleri içerebilir. Sonuç olarak; Güvenli Liman Anlaşması, Direktifin yerine getirilebilmesi için (Direktif'in gereklilikleri veri transferinin alıcısına üçüncü ülkeler tarafından teklif edilen 'yeterli' seviyede korumaya ilişkin) gerekliydi.

3. İŞLETMEYE ÖZGÜ İSTİSNALAR

Halen şirketlerin, AB dışına kişisel veri transferine karşı yasaklamadan kaçınmak için başvurabileceği iki yöntem vardır. Bu yöntemler, Standart Sözleşme Maddeleri (SSM) ve Bağlayıcı Şirket Kuralları (BŞK) dır. Bunların önemi her geçen gün artabilir, çünkü DPA'lar kişisel verilerin sınıraşırı transferi için daha katı uygulama rejimleri başlatmaktadır.

a. Standart Sözleşme Maddeleri

Komisyon, Standart Sözleşme Maddelerinin (SSM) AB Direktif'inin 26 (2) maddesinde öngörüldüğü üzere, yeterli koruma teklif etmeye karar verme yetkisine sahiptir. Mahremiyetin korunması ve temel

68 ABD ve AB Güvenli Liman İlkeleri için bkz; http://export.gov/safeharbor/eu/index.asp, ET: 07.07.2013

hak ve özgürlükler konusunda ve mutabık hakların kullanılması hususunda da yeterli koruma sağlamaktadır. Böyle bir kararın etkisiyle, SSM'leri sözleşmeye dâhil ederek, kişisel veriler, herhangi bir AB ülkesinde ve üç AEA üye ülkesinde bulunan veri kontrolöründen, yeterli seviyede veri koruma sağlamayan bir ülkede bulunan veri kontrolörüne aktarılabilir. Çok özel durumlar haricinde ulusal DPA'lar böyle bir transferi engelleyemez[69].

b. Bağlayıcı Şirket Kuralları

İşletmeye özgü ikinci istisna, Bağlayıcı Şirket Kuralları'na (BŞK) dayanır. Bu istisna, Direktif ile uyumlu olan ve şirket çapında uygulanan davranış kuralları çıkaran çok uluslu şirketler için geçerlidir. BŞK'ler onaylandığında, şirkete tüm kuruluşlarda serbestçe kişisel veri transferi yapabilme imkânı sağlayacaktır[70].

IV. TASLAK AB VERİ KORUMA YÖNETMELİĞİ

Öncelikle kabul edilmelidir ki, mevcut Veri Koruma Direktifi internet öncesi bir dönemde uygulamaya konulmuştur. Ancak bugün Avrupa'da her gün 250 milyon kişi internet kullanmaktadır. Bu da Direktifin 21. yüzyılın zorluklarıyla başa çıkamayacağı anlamına gelmektedir. Hızlı teknolojik gelişmeler ve küreselleşme, veri koruma tartışmaları hakkında önemli etkileri ile birlikte yeni zorluklar da getirmiştir ve böylece insanların, temel hak ve özgürlüklerinin etkin korunmasına yatırım yapmaları gerekmektedir[71].

AB Üye Devletleri; var olan kuralları, farklı şekillerde uygulamışlardır. Bu da birçok yasal belirsizliğe neden olmak kadar, uygulama ve yorumlamada ciddi derecede farklılığa da yol açmıştır. Bu sadece sınıraşırı durumlarda vatandaşlar için veri koruma kaybı değil, aynı zamanda gereksiz masraf anlamına da gelmektedir. AB içerisinde tutarlılığın yaygınlaşması gerekmektedir. Son olarak, Lizbon Anlaşması temel hak olarak veri korumanın önemini vurgulamış ve tüm AB politika alanlarında yatay kurallar için hukuki temeli oluşturmuştur. Bu durum, mevcut kanunların gözden geçirilmesini ve daha geniş bir yaklaşımı gerektirmektedir[72].

Sonuç olarak, Avrupa Komisyon'u 25 Ocak 2012'de Veri Koruma Yönetmeliği önerisini yayınladı. Önerilen düzenleme, 1995 Direk-

69 *Model Contracts for the transfer of personal data to third countries*, at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm, ET: 07.07.2013
70 **Lambert Paul**, *A User's Guide to Data Protection*, Bloomsbury Professional Ltd, 2013, s. 401
71 **Kuschewsky Monika**, *Sweeping Reform for EU Data Protection*, European Lawyer, Cilt: 112, 2012, s. 12
72 **Hustinx Peter**, *Streamlining Data Protection*, European Lawyer, Cilt: 112, 2012, s. 4

tifi'nin yerine geçmek üzere ve kişisel verilerin kullanımına ilişkin olarak bireylerin mahremiyetlerinin korunmasına odaklanmıştır. Kabul edildiğinde, Yönetmelik tüm AB Üye Devletleri'nde doğrudan yürürlüğe girecektir. Taslak Yönetmelik kapsamlı bir çalışma gerektirmesine rağmen, makalemiz Yönetmeliğin sadece birkaç önemli hususunu ele alacaktır.

- Yönetmeliğin Direktif'in yerine geçmesi büyük bir yeniliktir, belki de en önemlisidir. Yönetmelik doğrudan uygulanabilir olduğu için, AB'nin veri koruma kuralları tüm AB Üye Devletleri'nde tamamen aynı olacaktır[73].
- Veri öznelerinin haklarına bu Yönetmelikle netlik kazandırılmış ve özellikle sanal dünyada sosyal ağlar ve diğer servisler için, 'silme hakkı ya da unutulma hakkına' özel bir önem verilmiştir. Kişiler, verilerinin artık işlenmesini istemezlerse ve bunu muhafaza etmek için de yasal bir zemin yoksa veriler silinecektir[74].
- Veri işleme için onay gerektiğinde, bu onayın sadece serbest olarak, belirli ve bilgilendirici olması yetmemekte, aynı zamanda açık, yani beyana ya da net bir onaylayıcı harekete dayanması gerekmektedir. Yönetmelik; 'rıza tanımında' bu onayın açık olmasını gerektiren bir takım unsurlar eklemekte, böylece hassas verilerin işlenmesine ilişkin Yönetmelik hükümleri, artık 'açık' onay anlamına gelmemektedir[75].
- Yönetmelik aynı zamanda; bireylere, verilerinin elektronik kopyasını bulundurma hakkı ve bir kuruluştan diğer bir kuruluşa transfer etme talebi hakkı veren 'veri taşınabilirliği hakkı' vermektedir. Bu hak, kolayca hizmeti değiştirme olanağı sağlayarak müşterileri güçlendirmeyi amaçlamaktadır.
- AB Veri Koruma Kanununun uluslararası kapsamı genişletilecektir. Bu kapsam, sadece AB içinde bulunan kontrolör bağlamında kişisel verilerin işlenmesine uygulanmayacak, aynı zamanda AB içinde veri öznelerine mal ya da hizmet tekliflerine ya da onların davranışlarının izlenmesine ilişkin işlemelere de uygulanacaktır[76].

Bu reformlar, kişisel veri işleme ile ilgili konuların merkezinde

73 **De Waele Henri**, *Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective*, Privacy & Data Protection, Cilt: 12, Sayı: 4, 2012, s. 4

74 Bkz: Taslak Yönetmeliğin 17. maddesi.

75 Kosta, s. 147

76 Hustinx, s. 14

bulunan sorumluluk ve hesap verebilirlik konularına değinmeyi amaçlamıştır. Yönetmeliğin Direktif'in yerine geçmesi açıkça, Yönetmeliğin ciddi şekline bakılmaksızın, AB içerisinde uygulanabilir, standart, erişilebilir ve şeffaf kurallara ve usullere doğru atılmış önemli bir adımdır[77].

V. TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Uluslararası bakış açısına göre, Avrupa Konseyi'nin bir üyesi olarak Türkiye, AİHS'i onaylamış, hem 1981 yılında 'Kişisel Verilerin Korunmasına ilişkin Avrupa Konseyi Sözleşmesini' hem de 2001 yılında denetleyici otoriteler ve sınır aşan veri transferlerine ilişkin Sözleşme'nin Ek Protokol'ünü imzalamıştır, ancak henüz bunları onaylamamıştır. Bu nedenle, Türkiye'nin iç hukuku açısından bunlar 'kanun' statüsünde değildir.

Türkiye, kişisel verilerin korunması alanında ilk uluslararası belge olan Avrupa Konseyinin 28.01.1981 tarihinde imzaya açtığı 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmeyi imzaya açıldığı gün imzalayan ilk ülkelerden birisidir. Bunun dışında, 2001 yılında denetleyici otoriteler ve sınır aşan veri transferlerine ilişkin Sözleşme'nin Ek Protokol'ünü imzalamıştır, ancak henüz bunları onaylamamıştır. Günümüz itibariyle ise San Marino, Sözleşmeyi imzalamayan, Türkiye ise imzalamasına rağmen onay surecini işletmemiş tek ülke konumundadır[78].

Kişisel verilerin korunması alanında ilk başvurulabilecek kaynak Türk Anayasasıdır[79]. Türkiye'de bu haktan, Türkiye Cumhuriyeti Anayasasında, Ceza ve Medeni Kanunu gibi mevzuatın çeşitli kısımlarında bahsedilmekte ancak tanımı yapılmamaktadır. Aslına bakılırsa, 2010 yılından önce '*kişisel veri veya kişisel verilerin korunması*' terimi, Anayasada özel hayatın korunması kapsamında kabul edilmesine karşın açık bir şekilde belirtilmemiş idi. Daha sonra, 12 Eylül 2010 tarihinde, Anayasa'ya değişiklikler getiren reform pa-

77 De Waele, s. 5

78 **Cumhurbaşkanlığı Devlet Denetleme Kurulu**, *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*'na ilişkin 27 Kasım 2013 tarihli Denetim Raporu, s. 780, bkz: http://www.tccb.gov.tr/ddk/ddk56.pdf, ET: 13.02.2014

79 Özkan Ayşegül, *Türkiye'nin Kişisel Verilerin Korunması Hukuku Alanındaki Durumu Ve Almanya İle Türkiye Arası Olası Bilgi Aktarımı*, bkz: http://www.datenschutzbeauftragter-online.de/tuerkiye-nin-kisisel-verilerin-korunmasi-hukuku-alanindaki-durumu-ve-almanya-ile-tuerkiye-arasi-olasi-bilgi-aktarimi/4878/, ET: 14.02.2014

ketine ilişkin bir referandum gerçekleştirildi. Değişiklik sonucunda, Anayasa'nın 20. maddesinde detaylandırılan kişisel verilerin korunması hakkı desteklenmiş ve hesap verilebilirliğin kapsamı artırılmış ve kişisel verilerin korunmasına yönelik daha bağlayıcı gereksinimler getirilmiştir. Aşağıdaki paragraf, Türk Anayasası'nın 20. maddesine 3. fıkra olarak eklenmiştir:

"*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*."

Söz konusu düzenleme, kişisel verilerin korunması hakkının temel ilkelerini ve bireylerin haklarını açıkça belirtmesi açısından önemlidir. Ancak, Anayasa ile güvence altına alınan bu hakkın etkin bir şekilde korunması açısından; kişisel veri, açık rıza ve benzeri tanımların, kişisel verilerin işlenmesinin genel ilke ve esaslarının, kişilerin haklarını korumalarına yardımcı olacak mekanizmaların ve ilgili kurum ve kuruluşların kişisel verilerin işlenmesi sırasında bu hakkın korunmasına aykırı davranışta bulunmamalarını sağlamak amacıyla gerekli ikincil düzenlemeleri ve denetimleri yapacak, *şikayetleri* değerlendirecek, idari yaptırım uygulama yetkisine sahip kurumsal yapılanmanın ne şekilde olacağını belirleyen çerçeve bir kanunun bir an önce hukuk sistemimize kazandırılması ihtiyacı bulunmaktadır[80].

Aslında kişisel veriler ilk defa, 2005 tarihli Türk Ceza Kanunu (TCK) ve Ceza Muhakemesi Kanununda (CMK) *özel hayatın gizliliğinden ayrı, bağımsız bir yasal kavram olarak* düzenlenmiş ve korunmuştur. Ceza Kanununda, 135 ila 140. maddeler kişisel verilerin korunmasına ilişkin hükümler ihtiva etmektedir. Yeni maddeler, hukuka aykırı bir şekilde veya rıza olmaksızın kişisel verileri toplamayı, yaymayı ve işlemeyi, yüksek hapis cezalarıyla birlikte, bir suç haline getirmiştir. 135. maddede suçun işlenme şekli ve alanı sınırlandırılmamıştır. Suçun en çok işlenebileceği yer bilişim alanı olmakla beraber yalnız bu alanla da sınırlı değildir[81]. Kişisel verilerin, gerekli güvenlik önlemleri alamamanın bir sonucu olarak, başkaları

80 Cumhurbaşkanlığı Devlet Denetleme Kurulu Raporu, s. 781, bkz: http://www.tccb.gov.tr/ddk/ddk56.pdf, ET: 13.02.2014

81 **Karagülmez Ali**, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayınları, Ankara, 2005, s. 231

tarafından alıkonulmasına, bozulmasına ve zarar görmesine neden olmak, cezayı müeyyideyi gerektiren bir suç olarak görülmektedir. TCK'nın 135 (2) maddesi uyarınca, "*kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse*", hapis cezasıyla cezalandırılır.

TCK, ayrıca kişisel verilerin yetkili olmayan kişilere ifşa edilmesi ve verilmesini de düzenlemiştir. Buna ek olarak, kanunların belirlediği süreler geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmemeleri yani verileri yok etmemeleri durumunda, bu kişiler hapis cezasıyla cezalandırılmaktadır. Son olarak, Kanun, bu tür ceza gerektiren suçların verilerin tutulduğu her sisteme uygulanabilir olduğunu söylemekte ve tüzel kişilerin sorumluluğunu yani tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağını vurgulamaktadır.

CMK'ya gelince, ilk olarak şunu belirtelim ki, ceza bilimi, cezai kovuşturmayı başlatmaya yetecek delil elde etmek amacıyla büyük bir önem taşımaktadır. Bu bağlamda, kan, parmak izleri, ses ve kokunun hepsi birden kişisel veri olarak kabul edilmektedir. CMK, vücuttan veya suç mahallinden elde edilen örneklerin incelenmesi için bir koruma öngörmektedir ve bunları ilk kez kişisel veri olarak ele almıştır. Bu tür örneklerin analizinden elde edilen bilgiler de kişisel veri olarak görülmektedir, ancak bu bilgiler başka amaçlar için kullanılmamalıdır. Bunun dışında, dosyalara erişimi bulunan kişiler yetkili olmayan kişilere bu bilgileri ifşa etmemelidir[82].

Bu ana kanunlardan önce, kişisel verilerin işlenmesine dair tanımlar "*Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*" adı verilen bir yönetmelikte ayrıntılarıyla verilmiştir. Burada kişisel veri belirli veya belirlenebilir gerçek ve/veya tüzel kişiye ilişkin herhangi bir bilgi anlamına gelecek şekilde tanımlanmıştır. Belirlenebilir bir kişi belirleme numarasına veya kişinin fiziksel, fizyolojik, akli, ekonomik, kültürel veya sosyal kimliği, sağlık, genetik, etnik, dini ve siyasal bilgilerine atıfta bulunarak doğrudan veya dolaylı bir şekilde ilgili yönetmelik uyarınca belirlenebilen kişidir. Bu tanım AB Direktifine oldukça yakındır.

Özel Hukuk alanında, özellikle de Medeni Kanun ve Borçlar Kanunu alanında kişisel hakların korunmasına ilişkin bazı hükümler

82 Bu bilgiler için bkz, CMK'nın 80. maddesi.

bulunmaktadır. Bireylerin hakları, kişisel verilerin kanuna aykırı işlenmesi halinde, bu hükümler aracılığıyla korunabilir. Medeni Kanunun 24. maddesi uyarınca, kişisel hakları adil olmayan bir şekilde ihlal edilmiş olan bir birey, bu tür bir ihlale karşı korunmaya ve/veya bu tür ihlalden doğan zararların tazminine yönelik hukuk davası açabilir. Kişisel ve/veya gizli bilgileri ifşa etme veya kötüye kullanma, kişisel hakların korunmasına yönelik bu genel kurallar uyarınca kişisel hakların bir ihlali olarak düşünülmektedir. Mağdur taraf, Borçlar Kanunu'nun 49. maddesi uyarınca dava açabilir ve maddi ve manevi zararların tazminini elde edebilir. Dolayısıyla kişilik hakkı ihlali ve bunun sonuçlarıyla ilgili Medeni Kanun ve Borçlar Kanunu maddeleri, kişilik ihlali hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin uygulama alanına sahiptir; zira ceza hukukuna hâkim olan suçta ve cezada kanunilik ilkesi özel hukukta geçerli değildir[83]. Bunun dışında, kişisel veriler ve onların korunmasına yönelik hükümler, İş Kanunu, Bilgi Edinme Hakkı Kanunu ve Nüfus Hizmetleri Kanunu gibi diğer kanunların metinlerinde de yer almaktadır.

B. VERİ KORUMA KANUNU'NA DUYULAN İHTİYAÇ

Taslak Kanunun değerlendirilmesinden önce daha genel bir soruya cevap verme ihtiyacı bulunmaktadır: Türkiye'de bu tür bir kanunu kabul etmek gerekli midir? Türkiye'nin insan haklarına saygı duyan demokratik bir devlet olduğunu akılda tutmak gereklidir. Türkiye, Avrupa Konseyi, BM ve OECD gibi birçok uluslararası örgüte üyedir. Bununla birlikte, Türkiye veri koruma alanında bu örgütler tarafından kabul edilen ilkeleri kendi iç hukukuna dâhil etmeyi başaramamıştır. Türkiye halen kişisel verilerin işlenmesine ilişkin açık, uygun bir yasal düzenlemeden yoksundur. Kişisel verilerin korunması yaklaşık kırk yıldır Avrupa ülkelerinin çoğunda yasal sistemin bir parçası olmuştur. Aslında bu alanda en eskiye dayanan düzenlemeler Avrupa'dadır. ABD'yi ayıracak olursak, hemen hemen tüm modern demokratik ülkeler bu konuda bir düzenleme kabul etmiştir[84].

Türk Ceza Kanunu'nun 135 ve devamı maddelerinde, kişisel verilerin kanuna aykırı bir şekilde işlenmesi suç olarak kabul edilmiştir. Ancak bunun hangi koşullarda kanuna aykırı olduğunu ve hangi şartlarda kanuna aykırı olmadığını açıklığa kavuşturan bir düzenleme bulunmamaktadır. 2010 yılında Anayasada yapılan değişik-

83 **Dülger Murat Volkan,** *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004, s.265

84 **Kuzeci Elif**, *Kişisel Verilerin Korunması*, Turhan Kitabevi, Ankara, 2010, s. 351

likle kişisel verilerin korunması temel bir hak olarak güvence altına alınmıştır ve diğer detayların kanunca düzenlemesi gerektiği ifade edilmiştir.

Kişisel verilerin korunması ve düzenleyici ve denetleyici bir kurumun kurulması hakkında yasal bir düzenleme yapmanın 'Müktesebat Fasılları'nın 4'ü ile ilgili olduğunu burada belirtmek de ayrıca önemlidir. Bu Fasıllar 23. Fasıl (Yargı ve Temel Haklar), 24. Fasıl (Adalet, Özgürlük ve Güvenlik), 10. Fasıl (Bilgi Toplumu ve Medya) ve 28. Fasıl'dır (Tüketicinin ve Sağlığın Korunması). Bu doğrultuda, Türkiye'nin katılım sürecinde bu tür bir kanunu kabul etmesi de bir gereklilik teşkil etmektedir.

Böyle bir kanunun yürürlüğe girmemiş olması; İlerleme Raporu'nda, Katılım Ortaklığı Belgesi'nde ve 23. Fasıl Tarama Sonrası Raporları'nda da önemli bir eksiklik olarak değerlendirilmiştir. Dahası, Türkiye'de kişisel veriler korunmadığı gerekçesiyle Avrupa Polis Teşkilatı (EUROPOL) ile operasyonel işbirliği anlaşmaları yapılamamaktadır. Mevcut işbirliği ve bilgi belge değişimi elektronik iletim hattından yapılamamakta ve bu sebeple gecikmeler ve başarısızlıklar yaşanmaktadır. Bunun da ötesinde, Türkiye Schengen Bilgi Sistemi ve Ulusal Girişlerde Tamamlayıcı Bilgi Talebi (SIRENE)[85]'nin sağladığı imkânlardan yararlanamamaktadır.

Yukarıda bahsedilen tüm konular dikkate alındığında, mümkün olduğunca hızlı bir şekilde bağımsız ve kapsamlı bir kanunun yürürlüğe girmesi konusu tartışmasız bir gerekliliktir.

VI. KİŞİSEL VERİLERİN KORUNMASINA DAİR KANUN TASARISI

A. TARİHÇE

Kişisel Verilerin Korunması Kanun Tasarısı ile ilgili ilk çalışmalar 1989 yılında başlamış ve 2000'li yıllara kadar çeşitli tasarılar Adalet Bakanlığınca hazırlanmış, ancak çalışmalar sonuçlandırılamamıştır. 2000 yılında kurulan bir komisyonun da tasarı çalışmalarını tamamlayamaması üzerine 2004 tarihli Bakan Oluru ile Prof. Dr. Bahri Öztürk başkanlığında yeni bir Komisyon oluşturularak Tasarı hazırlık çalışmalarına devam edilmiştir. Bu Komisyon tarafından hazırlanan Tasarı, kamu kurumları, üniversiteler ve sivil toplum örgütleri de dâhil olmak üzere toplam 53 kuruluşa görüşe gönde-

85 Bu sistem, çalıntı araçlar, pasaportlar, Avrupa tutuklama kararları, aranan kişiler ve istenmeyen kişiler (persona non grata) hakkındaki bilgilerin paylaşılmasına olanak sağlamaktadır.

rilmiş, Başbakanlık aşamasında da tekrar görüş alınmıştır. Gelen görüşler üzerinde çalışmalarını tamamlayan Adalet Bakanlığı, Tasarıyı 2006 tarihinde Başbakanlığa göndermiştir.

Tasarı, Başbakanlık tarafından 2008 yılında Türkiye Büyük Millet Meclisi'ne (TBMM) sevk edilmiştir. Daha sonra, 2 Mayıs 2008 tarihinde esas komisyon olarak Adalet Komisyonuna gönderilmiştir. 7 Mayıs 2008 tarihinde de Meclis Adalet Komisyonu tarafından alt komisyona havale edilmiştir. Alt Komisyon tasarı ile ilgili birkaç toplantı yaptıktan sonra yoğun gündem nedeniyle çalışmalarına ara vermiş ve Adalet Alt Komisyonunda bulunan tasarı, araya TBMM Seçimlerinin girmesi nedeniyle yasalaşamayınca İçtüzüğünün 77. maddesi gereğince hükümsüz sayılmıştır. Ardından da Başbakanlığa iade edilmiştir[86]. 2012 yılının Mart ayı içerisinde Başbakanlıkta yapılan toplantıda Tasarının yenilenmesinin istenilmesi üzerine Adalet Bakanlığı bünyesinde yeni bir çalışma grubu oluşturulmuştur. Çalışma grubu tarafından mevcut Tasarı, yapılan eleştiri ve öneriler doğrultusunda yeniden kaleme alınmış ve Tasarıya son şekli verilerek 8 Haziran 2012 tarihinde 'Kişisel Verilerin Korunması Kanun Tasarısı' adı altında Başbakanlığa sevk edilmiştir[87].

B. DEĞERLENDİRME VE ELEŞTİRİLER

Kişisel Verilerin Korunması Kanun Tasarısı, Avrupa Komisyonu ve EUROJUST gibi birçok AB kurumuna görüş alınması amacıyla sunulmuştur. Bu eleştiriler önemli değişikliklere sebep oldu, gerçi metnin meclis onayı almadığının ve resmi kanun tasarısı olmadığının da altı çizilmelidir. Bu, denetim kurulunun yapısı gibi birçok hükmün bakanlıkça incelenmesi sırasında halen değiştirilebileceği anlamına gelmektedir. Ancak, önerilen Kanun Tasarısı Avrupa Konseyi Sözleşmesi'ne ve AB Direktifi'ne uygundur. Genel veri koruma sisteminin terimleri, tanımları ve kurumları, çoğunlukla aynı harf ve kelimelerle benimsenmiştir. Ancak doğaldır ki, Türkiye'ye ve onun hukuk sistemine özgü bazı değişiklikler vardır.

Aşağıdaki eleştiri ve değerlendirmelerimiz, Kanun Tasarısının mevcut haline ilişkin 8 ana konuyu özetlemektedir. Her başlık, kısa bir özetle başlamaktadır ve ardından, eğer uygulanabilirse ve mümkün olduğu kadar, nelerin yapılabileceğine dair öneriler sunmaktadır.

86 **Ünsal Çağrı Zeybek**, *Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi*, Hacettepe Hukuk Fakültesi Dergisi, Cilt: 3, Sayı: 1, 2013, s. 101 99–124

87 Adalet Bakanlığı, Kanunlar Genel Müdürlüğü tarafından hazırlanan bilgi notu (yayımlanmamıştır)

1. Tasarıdaki bazı kavramların tanımları, AB Direktifindeki kavramlardan farklı, daha kapsamlı ya da daha bağlayıcıdır.

Tasarının 3 (g) maddesi uyarınca, veri kontrolörü, veri kayıt sisteminin tesis edilmesinden ve yönetilmesinden sorumlu gerçek veya tüzel kişidir. Bu tür bir tanım AB Direktifinden daha bağlayıcıdır. Dahası, 'kişisel verilerin işlenmesinin amaçlarını, koşullarını ve araçlarını belirler' ifadesi cümlenin sonuna eklenmelidir. Ayrıca, 'veri öznesinin rızası', 'temsilci', 'üçüncü taraf'[88]ve 'alıcı' tanımları Taslakta yer almamaktadır. Bunlar, AB Direktifi doğrultusunda eklenmelidir.

Kişisel verilerin tanımı bir önceki 2008 Tasarısında tüzel kişileri kapsayacak şekilde genişletilmişti. Oysa AB Direktifi, gerçek kişilerin kişisel verilerinin korunmasıyla sınırlıdır. Tüzel kişileri dahil etmek üst düzey idari yüke yol açacak ve etkili icranın zor olacağı ölçüde kanunun kapsamını genişletecektir. Bu nedenle, AB'den gelen eleştirileri ve özellikle Türk Anayasasının 20 (3) maddesini dikkate alarak, Adalet Bakanlığı, yenilenmiş Taslakta 'tüzel kişiler' terimini kaldırma kararı almıştır.

2. Tasarı ile öncelikle kişisel verilerin işlenmesi sorunu düzen altına alınmakta, buna ilişkin genel ilkeler belirlenmektedir.

Buna göre kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi, belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi gerekmektedir. Ayrıca bu veriler, toplandıkları amaçla bağlantılı, yeterli ve orantılı olmalı, doğru olmalı ve gerektiğinde güncellenmelidir. Tam bu noktada, 'gerektiği zaman' ibaresi gereksiz bir eklemedir, çünkü kişisel veriler her zaman güncel olmak durumundadırlar. Eğer değişiklik yapılması gerekli değilse, o zaman veri günceldir.

3. Kişisel veriler istisnalar haricinde ancak ilgili kişinin açık rızasıyla işlenebilecektir.

Öncelikle belirtmek gerekir ki, veri öznesi istediği zaman rızasını geri çekme hakkına sahiptir. Rızanın geri çekilmesi, bu geri çekmeden önce rızaya dayalı işlemenin meşruluğunu etkilemeyecektir[89]. Kural olarak, kişisel veriler ancak ilgili kişinin açık rızasıyla ve kanunda açıkça öngörülen hallerde işlenebilecektir. İlgili kişinin bir itirazda bulunması halinde, kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, veri işlenemeyecektir. Bu kuralın

88 İşin garip tarafı, 'üçüncü taraf' terimi daha önce 2008 Kanun Tasarısında tanımlanmıştı.
89 Lambert, s. 98

istisnaları Tasarının 5. maddesinin ikinci fıkrasında; kanunlarda açıkça öngörülme, rızasını açıklayamayacak durumda olan kişinin hayati çıkarları, sözleşmenin kurulması ve ifası, ilgili kişi tarafından alenileştirilmiş olma ve veri sorumlusunun hukuki yükümlülüklerinin yerine getirilmesi, şeklinde sayılmıştır.

Bu maddeye ilişkin olarak, hukuki veri işlemeyi meşrulaştırma gerekçelerinin farklı olduğu görülebilir. Tasarı, rıza temeline dayalı veri işleme ile diğer gerekçelerle veri işleme arasında bir ayrım yapmaktadır. Esasında bu tür bir ayrım Direktifte yapılmamaktadır. Aslında bu, önemli bir kategoridir çünkü bu yolla, çıkarların dengelenmesine imkân tanınmaktadır. Bunlara ek olarak, rızayı ayrı bir gerekçe ya da sebep olarak değil, diğerlerine eşit bir gerekçe olarak dâhil etmek uygun olacaktır. Bundan ayrı olarak, hayati menfaat ibaresi, 'veri öznesinin rızasını veremeyeceği yerde başka bir kişinin' korunmasını da kapsamasından ötürü AB Direktifinden daha kapsamlıdır.

4. Özel nitelikteki kişisel veriler için işlem yasağı getirilmektedir.

Tasarı ile kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve cinsel hayatlarından[90] oluşan özel nitelikteki kişisel veriler (hassas veriler) için işlem yasağı getirilmekte, bu kuralın sınırlı istisnaları da 6. maddede fıkralar halinde sayılmaktadır.

6 (2) (a) maddesi uyarınca, hassas veriler, ancak veri öznesi 'tam' rızasını verirse işlenebilir. Bu tür bir rıza, AB'deki 'tam' rızadan daha güçlü olmasından dolayı 'açık rıza' ile değiştirilmelidir[91]. Bir istisna, veri öznesi (sahibi) tarafından alenileştirilen verilere de uygulanır. Bu durumda, AB Direktifi uyarınca 'alenileştirmiş olmasının' önüne 'açıkça' ibaresi yerleştirilmelidir. Dolayısıyla, işlenecek hassas veriler için veri öznesinin verinin kamuya açık hale getirilmesini istediğini açık hale getirmek istediği kesinlikle belirgin olmalıdır.

5. Tasarı ile verileri işlenen kişilere bilgi edinme, düzeltme gibi bir takım haklar tanınmaktadır.

Tasarının 9. maddesine göre, veri sorumluları (kontrolör); ilgili kişileri; veri sorumlusunun kimliği, verilerin işlenme amaç ve şekilleri ile bilgi edinme ve düzeltme haklarının bulunduğu hususlarında bilgilendirmekle yükümlü olacaktır. İlgili kişiler de, veri sorumlu-

90 2008 yılında Meclise gönderilen Tasarıda, 'cinsel hayat' hassas veri olarak düşünülmemişti, bu terim özel hayatın kapsamı içinde varsayılmıştı.

91 2008 Kanun Tasarısı, özel kategorideki kişisel verilerin işlenmesi için 'yazılı rızayı' aramaktaydı.

suna başvurarak; kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenmek, işlenmişse bunları talep etmek, verinin içeriğinin eksik veya yanlış olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesi ile buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini istemek hakkına sahip olacaktır.

7 (2) maddesi uyarınca, Kişisel veriler ilgili mevzuattan kaynaklanan bir zorunluluğun bulunmaması veya sözleşmeden kaynaklanan edimlerin karşılıklı olarak tamamen ifa edilmesi kaydıyla, ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir. Bu hüküm eleştirilebilir.

İlk olarak, silme ve yok etme arasındaki fark nedir? Zira, AB Direktifinde 'düzeltme, silme veya bloke etme' terimleri kullanılmasına rağmen, Tasarı, bu tür terimleri kullanmayı tercih etmektedir. Tasarının önsözüne göre, 'silme', örneğin, kişisel verilerin belgelerden, dosyalardan, CD'lerden ve hard disklerden silinmesi anlamına gelmektedir. 'yok etme' ibaresine gelince bu, örneğin, belge, dosya, CD ve hard disk verileri gibi materyallerin yok edilmesine atıfta bulunmaktadır. Bu tür bir ayrımın yapılmasına karşın bu ayrım hala kafa karıştırıcıdır ve AB Direktifindeki terimlerle aynı doğrultuda olmalıdır. İkinci olarak, kişisel veriler işleme amacıyla artık gerekli olmadığı durumlarda da silinmelidir. Başka bir deyişle, bu, yalnızca veri öznelerinin isteklerine bağlı olmamalıdır. Bu nedenle, 'artık' ifadesi 'gerekli' teriminin önüne eklenmelidir[92].

6. Tasarı ile yurt dışına veri aktarımı da sınırlandırılmaktadır.

Kişisel verilerin yurt dışına transferi Tasarının 8. maddesinde belirtilmiştir. Kişisel veriler, kural olarak, verinin istendiği yabancı ülkede yeterli koruma bulunması ve bu Kanunda belirtilen şartların gerçekleşmesi halinde yurtdışına aktarılabilecektir. Bu kuralın istisnaları 8. maddenin üçüncü fıkrasında bentler halinde sayılmıştır. 'İlgili verilerin veri öznesi tarafından aleniyete vurulması' ana kuralın sapmaları arasındadır. Bu bir nevi garip bir ilavedir. Bu, internette yayınlanan verilere yönelik midir? Bu istisna Direktifte bulunmamaktadır. Bu nedenle, bu ifade maddeden çıkarılmalıdır.

Tasarının 8 (5) (b) maddesinde 'kişisel veriyi talep eden ülke ile Türkiye arasında veri transferine ilişkin karşılıklılık durumunun' üçüncü bir ülkenin koruma düzeyinin yeterliliğini değerlendirme

92 Adalet Bakanlığının talebi üzerine, bu Tasarı hakkında Eurojust Kurumu tarafından hazırlanan rapor (yayımlanmamıştır)

kriterlerinden birisi olduğu da kabul edilmektedir. Ancak bu, hiçbir şekilde veri koruma unsuru değildir. Kanaatimizce bu ibare maddeden silinmelidir.

Ayrıca, Tasarının 8 (7) maddesinde; "Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlarla ilgili kişisel veriler, ilgili kişinin 'rızası' dışında üçüncü kişilere ve yurtdışına aktarılamaz" ifadesi yer almaktadır. Böyle bir kullanım yerine, bu tür bir transferin gerekliliğini ve orantılılığını dikkate alarak ya rızanın ya da yeterli garantilerin bulunması halinde ifadesini söylemek daha iyi olacaktır. Aynı şekilde, tekrar vurgulamak gerekir ki, hassas kişisel veriler söz konusu olduğunda, bunun her zaman 'açık rıza' ile olması gerekir.

Son olarak, "sağlık ve cinsel hayat" ibaresi, hassas verilerin üçüncü ülkelere transferi ile ilgili olan bu bölümde belirtilmemiştir. Tasarıda "sağlık ve cinsel hayat"a ilişkin kişisel veriler ile diğerleri arasında bir ayrım yapılmadığını anlamak güçtür. Tasarıdaki hassas verilere ilişkin diğer hükümler ile uyumu sağlamak için bunun dâhil edilmesi gerekmektedir.

7. Tasarıda belirlenen hükümlere aykırılıklar hakkında idarî ve cezaî yaptırımlar öngörülmüştür.

AB Direktifi'ne göre, Üye Ülkeler bu Direktif'e istinaden kabul edilen ulusal hükümlerin ihlali durumunda uygulanacak tedbirleri ortaya koymak zorundadır. Bu anlamda, Tasarı ile burada öngörülen yükümlülüklere aykırı hareket edilmesi halinde, 5237 sayılı Türk Ceza Kanununa paralel bir şekilde adli ve idari yaptırımlar öngörülmüştür. Örneğin, 26 (3) maddesine göre, 7. maddeyi ihlal ederek kişisel verileri silmeyen ya da anonimleştirmeyen bir veri kontrolörü, altı aydan bir yıla kadar hapis cezası ile cezalandırılır. Burada, 'yok etme' terimi geçmemektedir. Dolayısıyla diğer ilgili hükümlerle uyumu yakalamak için bu terimin buraya dâhil edilmesi gerektiğini düşünmekteyiz.

8. Tasarı ile bağımsız bir Kurul kurulmaktadır.

Tasarı ile tespit edilen ilkelere gerçek ve tüzel kişilerin uyumunu denetlemek, bu konuda yapılacak şikâyetler hakkında karar vermek, veri sorumluları sicilini tutmak ve konuyla ilgili düzenleyici işlemler yapmak üzere "Veri Koruma Kurumu" kurulmaktadır. Devamlı surette faaliyet gösterecek olan Veri Koruma Kurumu; Veri Koruma Kurulu ve Genel Sekreterlik olmak üzere iki birimden

oluşmakta, Veri Koruma Kurulu, Kurumun karar organı olarak görev yapmaktadır. Kurul, görevleri ile ilgili konularda veri sorumlularından, devlet sırları hariç olmak üzere, her türlü belge ve bilgiyi isteyebilecek olup, veri sorumlusu olan kurum ve kuruluşları ile gerçek ve tüzel kişiler söz konusu isteğe cevap vermek ve Kurulun görevlilerine gereken kolaylığı göstermekle yükümlü olacaktır.

İlgili kişiler, veri sorumlularına yaptıkları başvurudan netice alamazlarsa, otuz gün içinde Kuruma şikâyette bulunabilirler. Kurum da gelen şikâyetleri üç ay içinde karara bağlamak zorundadır. Kurul kararları, idari yargı denetimine tabidir. Veri Koruma Kurulları mahremiyet düzenlemeleri alanında, temel haklar ve tüketici haklarını inceleyerek güvence altına alan ve veri koruma politikaları ile uyumu zorunlu kılan en önemli aktörlerden bir tanesi olarak faaliyet göstermektedir. Söz etkin düzenlemeye geldiğinde, Veri Koruma Kurulunun 'tam bağımsızlığı' konusu kişisel verilerin korunması bakımından hayati önem arz etmektedir[93]. Genel olarak, öncelikle üç bileşenin gerekliliği kabul görmektedir. Bunlar: Kurumsal, İşlevsel (emir ve talimat almadan görevlerini yerine getirme) ve Mali (bütçe ve bütçe planlama) Bağımsızlıktır.

Veri Koruma Kurulunun işlevsel açıdan bir bakanlığa veya bir kamu kurumuna bağlı, onun denetim ve gözetimi altında ve onun talimatına göre hareket eden bir kurum olması düşünülemez. Avrupa uygulamasındaki veri koruma otoriteleri incelendiğinde bunların bağımsız bütçeli, sekretaryası ve kadrolu personeli olan, idari ve mali özerkliğe sahip bağımsız kurumlar olduğu açıkça görülmektedir[94]. Nitekim AB Komisyonu'nun Almanya aleyhine açtığı davada, Avrupa Birliği Adalet Divanı 2010 yılında verdiği bir kararda, Direktif'in 28 (1) maddesini ihlal ettiğini Almanya'da özel sektör için oluşturulan makamların devletin denetiminde olmasının Direktifin 28 (1) maddesi ile bağdaşmadığını ifade etmiş ve ihlal kararı vermiştir[95].

Yukarıda bahsi geçen kriterlere ve AAD kararlarına ilişkin olarak, eski 2008 Kanun Tasarısı, Avrupa Komisyonu Sözleşmesi ve AB Direktifinde belirtildiği üzere tam bağımsızlık sağlamamaktaydı.

93 Aslında, AB Direktifinde 'tam bağımsız' ifadesi kullanılmış ise de; kabul etmek gerekir ki, hiçbir kurum, şirket ya da kişi tam manasıyla bağımsız değildir. Ne var ki, bu yazılış tarzı AB'nin bu tür kurulların özerk olması gerektiğine dair görüşünün bir yansımasını göstermektedir.

94 Adalet Bakanlığı Avrupa Birliği Genel Müdürlüğü tarafından hazırlanan bilgi notu (yayımlanmamıştır)

95 Bkz: C-518/07 *Commission v. Germany* Davası, para 56. Mahkeme benzer bir ihlal kararını da Avusturya hakkında 16 Ekim 2012 tarihinde vermiştir. (Bkz: C-614/10 *Commission v. Austria* Davası)

Bu yüzden AB Komisyonu, mevcut tasarıya ilişkin görüşlerinde yukarıda bahsedilen hususları özellikle belirtmiş ve oluşturulacak denetim makamının tam bağımsız olarak kurulması gerektiğini ifade etmiştir.

AB'de DPA üyeleri belirli usullerle ve sıklıkla da Parlamento'nun da dahil ve etkili olduğu bir sistemle atanmaktadır. Kurulun bazı üyeleri, İrlanda, Lüksemburg ve İngiltere'de olduğu gibi hükümet tarafından atanmakta iken, örneğin Danimarka ve Hollanda'da gibi ülkelerde Adalet Bakanı tarafından atanmaktadır[96]. Bundan farklı olarak, Polonya'da olduğu gibi, DPA'ların temsilcileri Senato'nun onayı ile Parlamento tarafından seçilir ve yalnızca yine Parlamento tarafından görevden alınabilirler[97].

Tüm bu eleştirilere rağmen, Tasarı uygun kriterleri karşılamaya oldukça yakındır. Tasarıya göre, Veri Koruma Kurumu, kendisine verilen görevleri yerine getirmek için idari ve mali özerklik tanınmış kamu kurumu olarak oluşturulmuştur. Kurum, Adalet Bakanlığı'na bağlanmıştır ancak yetkilerini bağımsız olarak kullanacaktır. Hiçbir organ, makam, merci veya kişi Kurumun kararını etkilemek amacıyla emir ve talimat veremez. Merci, Veri Koruma Kurulu ve Genel Sekreterlikten oluşmaktadır. Veri Koruma Kurulu, yedi üyeden oluşur. Kurulun dört üyesi Bakanlar Kurulunca; iki üyesi Yargıtay ve Danıştay Genel Kurullarınca kendi üyeleri arasından, bir üyesi ise Yükseköğretim Genel Kurulunca öğretim üyeleri arasından üye tamsayılarının salt çoğunluğunun gizli oyu ile seçilir. Bakanlar Kurulu, Kurul üyelerinden birisini Başkan olarak seçer[98].

Parlamento'nun bu usullere, özellikle üyelerin atanmasında ve görevden alınmalarında müdahil olmadığı savunulabilir. Bu tür bir müdahil olma, bağımsızlık hükmüne yönelik önemli bir adım olacaktır. Bir diğer eleştiri de Kurul Başkanı'nın Hükümet (Bakanlar Kurulu) tarafından seçilmesine ilişkindir. Kanaatimizce Kurul, başkanını kendi içinden seçmelidir.

96 Korff (2010), s. 104
97 Polonya'nın ilgili kanunu için bkz: http://www.giodo.gov.pl/144/id_art/171/j/en/, ET: 25.07.2013
98 Bkz: Direktifin 12. maddesi.

SONUÇ

Veri koruma mevzuatı, kendi kişisel bilgilerinin kullanımını kontrol edemeyen bireylerin çıkarlarını, mahremiyetini ve kimliğini korumak için gereklidir. Uluslararası beklentiler, veri koruma mevzuatı bulunmayan ülkelere, şayet uluslararası bilgi toplumunun bir parçası olarak kalmayı istiyorlarsa, bu tür bir mevzuatı kabul etmeleri yönünde baskı yapmaktadır.

Veri işleme uygulamalarına ilişkin AB Direktifi, inanılmaz ölçüde etkili olmaktadır. İlkeleri uluslararası düzenleyici yanıtlar için zemin sağlamıştır. Kişisel verilerin yasal tanımları için standart oluşturmuştur. Ayrıca, mevcut düzenlemeleri başarılı bir şekilde uyumlaştırmış, bilgi mahremiyetine yönelik bireysel hakları korumuş ve ayrıca verilerin serbestçe ve güvenli bir şekilde transfer ve değiş tokuş edilebileceği ortak bir Avrupa sistemi yaratmıştır. Ancak tabiidir ki bazı hataları bulunmaktadır. Önemli biçimde, gelecekte veri işleme ve mahremiyet ihtiyaçlarına uygun sağlam yasal bir çerçeve yaratamamıştır. Bunun dışında, bilgilerin nasıl toplandığı, saklandığı, iletildiği, kullanıldığı, değiş tokuş edildiği ve satıldığıyla ilgili hızlı ve değişen değişiklikleri ele almada başarısız olmuştur.

Şu anda Türkiye'de kişisel verilerin korunması ile ilgili bağımsız bir kanun bulunmamaktadır. Bunun yerine, kişisel verilerin korunması diğer bir takım kanun ve yönetmelik maddelerinde genel hatlarıyla ve sadece bahsedilerek düzenlenmiştir. Başbakanlığın önünde bekleyen bir 'Kişisel Verilerin Korunması Kanun Tasarısı' bulunmasına rağmen, aslında bu, AB Direktifini çok yakından izlemektedir. Zayıf ve güçlü yanları zaten Tasarıda açık bir şekilde göze çarpmaktadır.

Esasında, Türkiye'nin böyle bir kanunu kabul etme dürtüsü, Avrupa Birliğine üye olmak istek ve ihtiyacından kaynaklanmaktadır. Ülkemiz buna ilişkin bir Tasarı hazırlamış ama maalesef bunu henüz bir mevzuat olarak kabul edememiştir. Bu durum aslında bir taraftan Tasarının ilk ortaya çıktığı tarihlerde bu konunun öneminin yeterince anlaşılamamasından, diğer taraftan kanunlaşma süreci ve yönteminden kaynaklanmaktadır. Zira yaklaşık 30 yıldır böyle bir kanunun yasalaşması mümkün olamamıştır. Bütün bunlara rağmen ülkemiz, kişisel verilerin korunması ile ilgili kanunu kabul etmeyi istemekte ve bu yönde de vaatte bulunmuştur.

Özellikle güvenlik, göç, askeri ve cezai konularla ilgili Avrupa kurumları ile yapılan bilgi alışverişi ve değişiminin gerekliliği, bu ka-

nunun kabul edilmesinin önemini bir kez daha ortaya koymaktadır. Türkiye'de mahremiyet ve kişisel verilerin korunmasının başarılı olması ya da başarısızlığı salt bir kanun metninin kabul edilmesiyle ölçülemez. Burada ayrıca, kanunun etkin şekilde uygulanması da önem arz etmektedir. Her an kişisel verileri toplanan, işlenilen ve aktarılan bireylerin karşı karşıya oldukları tehdidin farkında olması ve verilerine, mahremiyetlerine sahip çıkmaları, bu yönde bilinçlenmeleri ve talepte bulunmaları en az yasal düzenlemelerin varlığı kadar önemlidir. Son olarak belirtelim ki, Türkiye, kişisel verilerin korunması ve bunun düzenlenmesi hususunda gerek uluslar arası arenada, gerek Avrupa ülkelerinden kazandığı tecrübe, gerekse kendi iç dinamiklerinin zenginliğinden yararlanma imkânına sahip bir ülkedir. Dolayısıyla bu fırsat iyi kullanılmalıdır.

KAYNAKÇA

KİTAP VE MAKALELER

Adalet Bakanlığı, Kanunlar Genel Müdürlüğü tarafından hazırlanan bilgi notu (yayımlanmamıştır)

Atak, Songül, *Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri*, Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi, Sayı: 59-60, 2009, ss.200-222

Başalp Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınevi, Ankara, 2004

Bergkamp Lucas and Dhont Jan, *Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web*, The EDI Law Review, Cilt: 7, 2000, (ss. 71-114)

Bond Robert, *International Transfers of Personal Data - an Update*, Business Law International, Cilt: 5, No: 3, 2004, (ss. 423-432)

Bainbridge David, *Processing Personal Data and the Data Protection Directive*, Information & Communications Technology Law, Cilt: 6, Sayı: 1, 1997, (ss. 17-40)

Carey Peter, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, Second Edition, 2004

Cate Fred, *The European Data Protection Directive and European-US Trade*, Currents: International Trade Law, Cilt: 7, 1998, (ss. 61-80)

Charlesworth Andrew, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?* Hastings Law Journal, Cilt: 54, 2003, (ss. 931-969)

Corien Prins, *When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter*? SCRIPT-ed, Cilt: 3, Sayı: 4, 2006

D'afflitto Rosario Imperiali, *European Union Directive On Personal Privacy Rights And Computerized Information*, Villanova Law Review, Cilt: 41, Sayı: 1, 1996, (ss. 305-323)

De Waele Henri, *Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective*, Privacy & Data Protection, Cilt: 12, Sayı: 4, 2012, p.3-5, (ss. 3-5)

Dülger Murat Volkan, *Bilişim Suçları*, Seçkin Yayınevi, Ankara, 2004

Garrie Daniel, Duffy-Lewis Maureen and Wong Rebecca, *Data Protection: The Challenges Facing Social Networking*, International Law & Management Review, Cilt: 6, 2010, (ss. 127-152)

Hobby Seth, *The EU Data Protection Directive: Implementing A Worldwide Data Protection Regime and How The U.S. Position Has Progressed*, International Law & Management Review, Sayı: 1, 2005, (ss. 155-190)

Hustinx Peter, *Streamlining Data Protection*, European Lawyer, Cilt: 112, 2012

Ilana Saltzman, *The Status of National Implementation of Directive 95/46/EC on the Processing and Free Movement of Personal Data*, European Intellectual Property Review, Cilt: 18, Sayı: 6, 1996, (ss .680-683)

Jay Rosemary and Hamilton Angus, *Data Protection Law and Practice*, İkinci Baskı, 2003

Johnson Elizabeth H, *Data Protection Law in the European Union*, The Federal Lawyer, 2007

Kaplan Harvey L, Cowing Mark W, Egli Gabriel P, *A Primer for Data-Protection Principles in the European Union*, Defense Research Institute, Münih, 2009

Karagülmez Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayınları, Ankara, 2005

Karst Kenneth L, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 Law and Contemporary Problems, 1966, (ss. 342-376)

Kaya Cemil, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul ***Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LXIX, Sayı: 1 - 2,*** 2011, ss. 317-334

Kinton John D, *Managing the EU-US Discovery Conflict*, Law 360, 2008, bkz: http://www.law360.com/articles/72082/managing-the-eu-us-discovery-conflict, ET: 29.06.2013

Kong Lingjie, *Data Protection and Trans-Border Data Flow in the European and Global Context*, European Journal of International Law, Cilt: 21, 2010, (ss. 441-456)

Korff Douwe, *Data Protection Laws in the European Union,* the Direct Marketing Association, 2005

Korff Douwe, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments,* 2010, bkz:

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, ET: 28.06.2013

Kosta Eleni, *Consent in European Data Protection Law*, 2013

Koutsias Marios, *The International Reach of European Union Data Protection Law and the United States: is International Trade in a Safe Harbour?* International Trade Law & Regulation, Cilt: 18, Sayı: 2, 2012, (ss. 31-45)

Kuilwijk Kees Jan, *Recent Developments in EU Privacy Protection Regulation*, International Trade Law & Regulation, Cilt: 6, Sayı: 6, 2000, (ss. 200-212)

Kuner Christopher, *European Data Privacy Law and Online Business*, Oxford University Press, 2003

Kuschewsky Monika, *Sweeping Reform for EU Data Protection*, European Lawyer, Cilt: 112, 2012

Kuzeci Elif, *Kişisel Verilerin Korunması*, Turhan Kitabevi, Ankara, 2010

Lambert Paul, *A User's Guide to Data Protection*, Bloomsbury Professional Ltd, 2013

Maxeiner James R, *Business Information and Personal Data: Some Common-Law Observations about the EU Draft Data Protection Directive*, Iowa Law Review, Cilt: 80, 1995, (ss. 619-638)

Maxeiner James R, *Freedom of Information and the EU Data Protection Directive*, Federal Communications Law Journal, Cilt: 48, 1996, (ss. 93-104)

Mell Patricia, *A Hitchhiker's Guide to Trans-border Data Exchanges between EU Member States and the United States under the European Union Directive on the Protection of Personal Information*, Pace International Law Review, Cilt: 9, Sayı: 1, 1997, (ss. 147-183)

Oxman Stephen A, *Exemptions to the European Union Personal Data*

Privacy Directive: Will They Swallow the Directive? Boston College International & Comparative Law Review, Cilt: 24, 2000, (ss. 191-203)

Özdemir Hayrunnisa, *Haberleşmenin Gizliliği ve Kişisel Veriler*, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XIII, Sayı: 1–2, 2009, ss. 285-303

Özkan Ayşegül, Türkiye'nin Kişisel Verilerin Korunması Hukuku Alanındaki Durumu Ve Almanya İle Türkiye Arası Olası Bilgi Aktarımı, bkz: http://www.datenschutzbeauftragter-online.de/tuerkiyenin-kisisel-verilerin-korunmasi-hukuku-alanindaki-durumu-ve-almanya-ile-tuerkiye-arasi-olasi-bilgi-aktarimi/4878/, ET: 14.02.2014

Robinson Neil and others, *Review of the European Data Protection Directive*, RAND Corporation, sponsored by Information Commissioner's Office, May 2009

Schriver Robert, *You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, Fordham Law Review, Cilt: 70, Sayı: 6, 2002, (ss. 2777-2818)

Swire Peter and Litan Robert, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998

Şimşek, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınları, İstanbul, 2008

Uygun Murat, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010

Ünsal Çağrı Zeybek, *Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi*, Hacettepe Hukuk Fakültesi Dergisi, Cilt: 3, Sayı: 1, 2013, (ss. 99–124)

Wong Rebecca and Savirimuthu Joseph, *All or Nothing: This is The Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet*, Journal of Computer & Information Law, Cilt: 25, 2008, (ss. 241-266)

Zinser Alexander, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, Tulane Journal of Technology & Intellectual Property, Cilt: 6, (ss. 171-179)

İNTERNET KAYNAKLARI

Data Protection in the European Union: the Role of National Data Protection Authorities, 2010, bkz: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf, ET: 18.06.2013

Key definitions of the Data Protection Act, bkz: http://www.ico.org.uk/for_organisations/data_protection/the_guide/key_definitions, ET: 26.06.2013

Model Contracts for the transfer of personal data to third countries, bkz:

http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm, ET: 07.07.2013

http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, ET: 07.07.2013

http://www.tccb.gov.tr/ddk/ddk56.pdf, ET: 13.02.2014

DAVALAR

Case C-101/01, *Bodil Lindqvist v. Jönköping*, [2003] ECR I- 12971

Case C-518/07, *Commission v Germany*, [2010] ECR I-1885

Case C-614/10 *Commission v. Austria*, 16 October 2012