ELEKTRONİK ORTAMDA KİŞİSEL VERİLERİN KORUNMASI, BAZI ÜLKE UYGULAMALARI VE ÜLKEMİZDEKİ DURUM [1*]

Protection Of Personal Data Around The Digital Media, Some Countries' Practices and the Situation in Our Country

Habip Oğuz[2]**

ÖZET

Günümüz teknoloji çağında, bilginin çok hızlı şekilde toplanması, işlenmesi ve aktarılmasının kişinin mahremiyet, rahatsız edilmeme, anonim kalma gibi özellikle manevî varlığına ilişkin haklarını tehdit etmesiyle birlikte, dünya üzerinde kişinin aidiyetini belirleyen kişisel verilerinin korunması gerektiği fikri ortaya çıkmıştır. Elektronik cihazlar ve sistemlerle bilginin otomatik hâlde işlenmesi bu fikrin tohumlarının atılmasına sebep olurken internetin icat edilmesi ve çok hızlı bir şekilde toplumların gündelik yaşamlarında kullanılmaya başlaması ise bu gerekliliği hayatî hâle getirmiştir. Avrupa'da 1960'lı yıllarda atılan ilk adımlardan sonra, 108 sayılı Sözleşme ve 95/46/EC sayılı Yönerge ile kişisel verilerin korunması bağlayıcı yasal bir çerçeveye kavuşturulmuşken ülkemizde 1995 yılında başlayan çalışmalardan halen sonuç alınamamıştır. Ezcümle "*Kişisel Verilerin Korunması Kanun Tasarısı*" üzerinde çalışmalar devam etmektedir.

Anahtar kelimeler: Elektronik Ortam, İnternet Ortamı, Kişisel Veri, Kişisel Verilerin Korunması, Veri Sahibi, Veri Sorumlusu, Veri Koruma Yönergesi

ABSTRACT

Around today's age of technology,while collecting quickly, processing and transfering of knowledge is beginning to threaten especially spiritual entity concerning rights such as a person's privacy rights,undisturbed rights and remaining anonymous rights, the notion of keeping personal data which is a vital necessity and that identifies the person's character and belonging in the world has turned out to be protected. While processing knowledge in an automated maner with a number of electronic devices and systems has led to this idea of laying the foundation, the invention of internet and starting to be used quickly in the daily life of communities has made it a vital necessity. After

1 [*]Bu makale, 25/04/2014 tarihinde Çağ Üniversitesi'nde düzenlenen "Elektronik Ticaret Hukuku Sempozyumu"nda yapılan sunumun genişletilip makaleye çevrilmiş hâlidir

2 [**]Ceyhan Cumhuriyet Savcısı, habip.oguz@adalet.gov.tr

the first steps in Europe in the 1960s, while the protection of personal data was binding in a legal framework with the No.108 conctracting and No.95/46/EC directive, no results could have been achieved from the studies that started in 1995 in our country.Still the studies on "Personal Data Protection Draft Law" continue to work on.

Keywords: Digital Media, Internet Media, Personal Data, Personal Data Protection, Data Owners, Data Management, Data Protection Directive

***

I. GİRİŞ

Günümüz modern hukuk sistemlerinin en önemli hak süjesi insandır. Bu bakımdan hukuk sistemleri temelde insanın kişiliğinin ve kişilik haklarının korunması üzerine kurulmuştur. Çalışmamızın maddî unsurunu oluşturan kişisel veriler ise kişilik haklarının önemli bir bölümünü teşkil eder. Çünkü kişisel verilerin korunması, kişinin şeref ve haysiyeti gibi manevî varlığına ilişkin haklarının korunması ile doğrudan ilgilidir.

Teknolojide yaşanan süratli gelişmeler, bilginin çok hızlı bir şekilde üretilmesine, işlenmesine, depolanmasına ve dağıtılmasına imkân sağlamaktadır. Özellikle bilginin çok hızlı bir şekilde üretiliyor, dağıtılıyor olması bir takım endişeleri ve bazen de problemleri beraberinde getirmektedir. Bugün, dünya üzerinde milyonlarca insan elektronik ortamlara dâhil olmaktadır ve artık sayılamayacak kadar çok bilgiyi bu ortamlara aktarmaktadır. 2012 yılının ikinci yarısında Facebook'un günde beş yüz terabyte veri topladığı, günde ortalama 300 milyon fotoğrafın Facebook'a yüklendiği belirtilmiştir[3]. Bugün 1.23 milyar civarında kullanıcısı olan Facebook'un sosyal medyanın aktörlerinden sadece bir tanesi olduğu göz önüne alındığında kişisel verilerin korunmasının önemi daha iyi anlaşılacaktır.

Kişisel verilerin artık ticarî meta hâline getirilmesi, her geçen gün yeni bir boyut kazanan siber suçlardaki hızlı artış ve buna bağlı olarak toplum psikolojisinde ortaya çıkan kaygılar; izleme, gözetleme, dinleme ve kaydetme imkânlarının olağanüstü derecede artması, yaygınlaşması ve kolaylaşması, bilgisayar ya da diğer mobil cihazlar başında insanoğlunun olağanüstü sosyalleşme çabaları ve buna bağlı olarak sosyal medya aracılığı ile çok fazla

3 Webrazzi, www.webrazzi.com/2012/08/23/facebook-gunde-500-terabyte-veri-topluyor/ (E.T.: 09/03/2014)

miktarlarda paylaşılan kişisel veriler dikkate alındığında kişisel verilerin genel mevzuat hükümlerine göre korumada yetersiz kalacağı açıktır. Ancak yapılacak düzenlemelerin gelişen teknoloji ve değişen toplum düzeni karşısında güncelliğini koruyabilmesi için kazuistik yöntemlerle hazırlanmaması gerekir.

Kişisel verilerin korunması hakkı, insanın temel hak ve özgürlükleri arasında yer almakta olup, kişiliğinin korunması, hukuk devleti ilkesi ve demokrasinin derinlik kazanması açısından hayatî öneme sahiptir[4].

II. ELEKTRONİK ORTAM NEDİR?

Elektronik ortam, sayısallaştırılmış verilerin üzerine kaydedilip saklandığı ortamların genel adıdır. Dolayısıyla anladığımız manada bilgisayarlardan, sayısallaştırılmış veri aktarıp kaydedebildiğimiz flash disklerden tutun akıllı kahve makinalarına, akıllı buzdolaplarına kadar tüm bileşenleri ifade eder.

Elektronik ortam bu denli geniş iken çoğu kez internet ortamı yerine de kullanılır. Oysa internet ortamı, elektronik ortamlardan sadece bir tanesidir. İnternet ortamı, haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan, kamuya açık, İnternet bağlantısı aracılığı ile erişilebilen bütün alanlardır[5]. İnternet ortamı herkese açıktır[6]. Elektronik ortam ise İnternet ortamının dışında kalan haberleşme ile kişisel veya kurumsal bilgisayar sistemlerini de kapsar. Elektronik bir ortam, herkese açık olmayabilir. Kişisel verilerin, bilgi depolama yeteneğine sahip bütün cihazlara kaydedilmesinin, saklanmasının ve bu cihazlardan dağıtılmasının mümkün olduğu göz önüne alındığında en geniş platformda konunun ele alınıp irdelenmesi zorunluluğu ortadadır.

III. ELEKTRONİK VERİ VE KİŞİSEL VERİ KAVRAMLARI

Elektronik veri, bilişim sistemlerinin temelidir ve bilgilerin belirli bir formata dönüştürülmüş hâlini ifade eder[7]. Bilgi depolama ve

4 T.C. Cumhurbaşkanlığı, Devlet Denetleme Kurulu, 27/11/2013 Tarih ve "*Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*" Konulu Denetim Raporu, s.778, http://www.tccb.gov.tr/ddk/ddk56.pdf (E.T.: 09/04/2014)

5 OĞUZ, Habip: İnternet Ortamında Kişilik Haklarının İhlâli ve Korunması, B.2, Ankara 2012, s.45.

6 ÇEKER, Mustafa: "*İnternet Ortamında Yapılan Usulsüzlüklerden Bankaların Hukukî Sorumluluğu*", Prof. Dr. Bilge ÖZTAN'a Armağan, Ankara 2008, s.249.

7 YAZICIOĞLU, R. Yılmaz: Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukuki Boyutları İle,

işlemede araç olan elektronik ortamlar ve bir bölümünü oluşturan internet, fonksiyonlarını yerine getirebilmek için bazı kişisel verileri kullanıcının bilgisi ve/veya onayı olmaksızın toplayabilmektedir[8]. Her şeyden önce biz istemesek de internet ortamına bağlandığımız bilgisayar, tablet, mobil telefon gibi cihazların IP adresleri trafik kayıt günlüklerine işlenmektedir. Bu itibarla tek başına bir IP adresi bile, en azından kamusal internet bağlamında, çoğu kez bir kişisel veridir[9]. Çünkü buradan internet hattının sahibi, bu itibarla çoğu kez internet hattını kullanan kişi, tespit edilebilir[10].

Kişisel veri, 15/03/2013 tarihli Kişisel Verilerin Korunması Kanun Tasarısında "*kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Yapılan tanım dikkate alındığında kişi hakkında toplanan her bilgi, doğrudan ya da dolaylı olarak belirli bir kişiyi işaret ediyorsa artık kişisel veri olarak kabul edilecektir. Yani kişi; adının, e-posta adresinin verilmesi gibi doğrudan belirlenebileceği gibi fiziksel, psikolojik, ekonomik, kültürel veya sosyal kimliğine ait özellikler işaret edilmek suretiyle dolaylı olarak da tespit edilebilir[11]. Tasarının bu hâlinde, sadece gerçek kişiye ait bilgiler kişisel veri olarak kabul edilmiştir.

IV. KİŞİSEL VERİLERİN ELDE EDİLME YÖNTEMLERİ

İnsanlar elektronik ortamlara dâhil oldukları anda bir takım kişisel verilerini de kullanıma açmış olurlar. Bu gün veri toplayabilen birçok elektronik sistem, kullanıcı ile etkileşime geçtiği ilk anda, hiçbir bilgi kaydedemese dahi kullanıcının benzersiz numarasını ve sisteme bağlandığı zamanı, sistem günlüğüne[12] kaydeder. Her ne kadar, yazılım uzmanları kişisel verileri kaydetmeyi, güvenlik gerekçesi ile ortaya çıkan bir ihtiyaç olarak açıklamaya çalışsalar

İstanbul 1997, s.29; ERGÜN, İsmail: Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara 2008, s.6.

8 TOPALOĞLU, Mustafa: Bilişim Hukuku, Adana 2005, s. 163.

9 SMITH, Graham J. H.: Internet Law and Regulation, B.4, Londra 2007, s.679.

10 IP adreslerinden, internet servis sağlayıcısının internet hizmeti sağladığı aboneye ulaşılabilir. Ancak bu, interneti bizzat kullanan kişiye ulaşılmayacağı anlamına gelmez. Zira mevzuatımızda toplu kullanım sağlayıcıları olarak yer alan İnternet kafelerde dahi iç IP dağılımı yapma, her bilgisayarı görecek şekilde kamera kaydı tutma ve bunları belirli bir süre saklama yükümlülüğü vardır. (İnternet kafelere ilişkin daha detaylı inceleme için bkz: OĞUZ, 208 vd.)

11 TOPALOĞLU, 165.

12 Her ne kadar "*logfile*" ifadesi dilimize "*sistem kütüğü*" olarak çevrilmekte ise de kütüğün fonksiyonunun daimi kayıt ve belgelendirme, günlüğün ise belirli bir zaman dilimi sonuna kadar kayıt ve analiz olduğu göz önüne alındığında "*günlük*" ifadesinin kullanılmasının daha doğru olacağı kanaatindeyiz.

bile kanaatimizce bu, insanoğlunun karşısındaki kişi hakkında daha fazla şey öğrenme merakından başka bir şey değildir. Zira hangi türden bir elektronik ortam olursa olsun, çoğu zaman ihtiyaç duyulandan çok daha fazla kişisel veriye erişme eğilimindedir. Bunun en güzel örneği, bugün çok popüler olan Android uygulamalarıdır. Bir Android uygulamayı mobil cihazlarınıza yüklemek istediğiniz zaman telefon rehberi, görüşme detayları, mesajlar dâhil, olabildiğince çok veriye erişim için izin istemekte, kullanıcılar ise uygulamayı yükleyebilmek ve kullanabilmek için istemeseler de erişim isteğini kabul etmektedirler.

Zaman içerisinde kişisel verilerin elde edilme yöntem ve yoğunluğu farklılık gösterse de bugün devletlerin kendi mevzuatında kişisel verileri koruma gayretleri ile paralel olarak ilgilinin rızası doğrultusunda kişisel verilerin elde edilme yöntemi yaygındır. Yukarıda da belirtildiği üzere, kişi, bir programı, bir siteyi kullanabilmek ya da sunulan bir hizmetten yararlanabilmek için istemese de bir takım kişisel verilerinin elde edilmesine rıza göstermekte ya da bizzat bilgi girişi yapmak suretiyle kişisel verilerini karşı tarafa iletmektedir.

Elektronik ortamda yapılan ticaretin çok yaygın olduğu günümüzde, kullanıcı hangi türden bir alışveriş sitesine girerse girsin, alışveriş yapmak istediği zaman adı, soyadı, eposta adresi, T.C. Kimlik Numarası, kredi kartı bilgileri gibi bilgileri istenmekte, bu bilgiler verilmediği zaman işlem gerçekleşmemektedir.

İstenen bu bilgiler arasında T.C. Kimlik Numarasının önemi üzerinde durmak gerekir. VUK'un 230. maddesi, 157 numaralı VUK Tebliği ve 3 numaralı Vergi Kimlik Numarası Genel Tebliği göz önüne alındığında nihai tüketicilere yapılan satışlar için düzenlenecek faturalarda nihai tüketicinin T.C. Kimlik Numarasının belirtilme zorunluluğu bulunmamaktadır. Buna rağmen bütün alışveriş sitelerinde, fatura düzenlenirken ihtiyaç olduğu gerekçesiyle kullanıcıların T.C. Kimlik Numaraları istenmekte, verilmediği zaman ya da yanlış verildiği zaman alışveriş süreci devam ettirilemediğinden işlem gerçekleştirilememektedir.

Günümüzde halen kişisel verilerin korunması kanunu olmadığı gibi maalesef e-devlet sistemimizde de bir bütünlük bulunmamaktadır. Bugün her kamu kurumu, bir diğerinden bağımsız ve çoğu kez birbiri ile entegre edilemez şekilde kendi e-devlet sistemini kurmuştur. Bu

siteler ziyaret edildiği zaman bir takım bilgiler istenir, bu bilgilerle kişinin yetkili kişi olup olmadığı kontrol edilmeye çalışılır, kişinin yetkili kişi olduğu kanaatine varılırsa[13] kişi ile ilgili sistemdeki diğer bilgiler gösterilir. Bu dağınık yapının en büyük sakıncası, bir kişiye ait kişisel verilerinin tamamının kötü amaçlarla kullanmak için parça parça toplanma olanağıdır. "*Kişisel veri zinciri kurma*" olarak tabir edebileceğimiz bu yöntemde, kişinin bilinebilir adı ve soyadının yanına önce T.C. kimlik numarası eklenir, sonra çalışmış olduğu kurum sicil numarası, anne baba adı derken her e-devlet sisteminden elde edilen fazladan bir bilgi ile sonuçta kişinin hiç de istemeyeceği şekilde A'dan Z'ye tüm bilgisine ulaşılabilir.

Kişisel verilerin elde edilmesine ilişkin diğer yöntemler ise çerezlerdir. Çerezler (cookiees), web sunucuları tarafından tarayıcı marifetiyle kullanıcıların bilgisayarlarına sonraki kullanımlar için yerleştirilen bilgi parçacıklarıdır[14]. Kullanıcı siteyi her ziyaret ettiğinde, site kullanıcının bilgisayarına istemi dışında bırakılan çerezi kontrol eder. Böylece daha kullanıcının daha önceki işlemleri hakkında bilgi sahibi olur. Bu yöntem kullanıcıların internet ortamındaki eğilimlerini analiz için en garanti sonuç veren yöntemlerden bir tanesidir. Çerezlerin bu kadar popüler hâle gelmesinin nedenlerin bir tanesi, kuşkusuz, kullanıcıların çerezlerin bilgisayarında saklanmasından rahatsız olmuyor olmalarıdır[15]. Çerezler virüs de taşıyamazlar herhangi bir kod da çalıştıramazlar. Genel olarak sonraki ziyaretler, kullanıcıyı çabuk tanıma ve kullanıcı tercihleri hakkında bilgi almak için gönderilirler. Silinmeleri ve engellenmeleri mümkündür[16].

Kişisel verileri ele geçirmenin sayısız yolu olmasına rağmen, son günlerde ülkemizde yaşanan gelişmelere bağlı olarak kullanıcılara zarar vermesi muhtemel bir yöntemden bahsetmek gerekir: VPN[17].

13 Bazen gerçek durum, sanılanın aksidir.

14 TOPALOĞLU, 164.

15 TIPTON, Harold F., KRAUSE, Micki: Information Security Management Handbook, B.6, Northwest 2007, s.2134.

16 EC-Council: Ethical Hacking and Countermeasures: Web Applications and Data Servers, New York 2010, Bl.5, s.4.

17 VPN (Virtual Private Network, Sanal Özel Ağ), İnternet üzerinden başka bir ağa bağlanmayı sağlayan bağlantı çeşididir. VPN istemcisi, TCP/IP (tünel protokolleri) tabanlı sanal bir bağlantı noktasına sanal bir arama gerçekleştirir. VPN istemcisi, İnternet üzerinden bağlantı kurmak istediği kaynakla sanal bir noktadan noktaya bağlantı kurar, kaynak ya da uzaktan erişime geçmek istediği sunucu kimlik bilgilerini kontrol eder ve doğruladıktan sonra VPN istemcisiyle uzaktan erişime geçtiği sunucuyla veri akışı gerçekleşir. (Wikipedi, tr.wikipedia.org/wiki/VPN, E.T.: 25/03/2014)

Özellikle sitelere erişim yasağı uygulanmaya başladıktan sonra internet kullanıcılarının DNS[18] değiştirerek sitelere girmeye devam ettikleri 5651 sayılı Kanun'un yürürlüğü süresince biliniyordu. Ancak IP bazlı site engelleme yöntemi uygulanmaya başladıktan sonra DNS adreslerini değiştirerek sitelere bağlanmak mümkün olmadığında kullanıcılar VPN servislerini veya programlarını kullanmaya başladılar. VPN servisleri temelde ücretlidir. Ancak ücretsiz olduğu bildirilen birçok VPN servis veya programı, sitelere erişim engellendikçe, binlerce Türk internet kullanıcısı tarafından bilgisayarlarına, mobil telefonlarına indirilmiş ve kullanılmıştır. Bu programlara eklenebilecek çok küçük yazılımlarla kullanıcıların kişisel verilerinin ele geçirilmesi mümkün olduğu gibi kullanıcıların bilgisayar ve mobil cihazları DOS[19] saldırılarında birer araç olarak da kullanılabilir[20]. Bu sebeple kullanılması düşünülen bu tür program ve servislerin kullanımına başlanmadan önce mutlaka güvenirliğine dikkat edilmeli, program ve servisler hakkında detaylı bilgilere ulaştıktan sonra ilgili program veya servis kullanılmalıdır.

V. AVRUPA'DA KİŞİSEL VERİLERİN KORUNMASI

A. OECD

14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi'ne dayanılarak, 1961'de kurulan ve savaş yıkıntıları içindeki Avrupa'nın Marshall Planı çerçevesinde yeniden yapılandırılması amacıyla 1948 yılında faaliyete başlayan Avrupa Ekonomik İşbirliği Örgütü'nün (OEEC) doğrudan mirasçısı olan İktisadi İş Birliği ve Kalkınma Teşkilatı'nın üyelerinin büyük bir bölümü AB üyeleridir[21] ve 1980 yılında

18 DNS (Domain Name System, Alan Adı Sistemi), internet uzayını bölümlemeye, bölümleri adlandır-maya ve bölümler arası iletişimi organize etmeye yarayan bir sistemdir. İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri, *"www.siteadi.com"* gibi kullanıcıların kolay hatırlamalarına yarayacak URL adreslerine dönüştürülür. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır. (Wikipedi, tr.wikipedia.org/wiki/DNS, E.T.: 25/03/2014)

19 DoS (Denial of Service) Attack olarak bilinen yöntemlerle sunuculara aşırı istek gönderilerek sunucu-lara erişim güçleştirilir ve ileri safhalarda sisteme ağır zararlar verilir (OĞUZ, 137).

20 DoS saldırılarının birçok bilgisayardan aynı anda yapılmasına DDoS (Distributed Denial of Service) denir. DDoS saldırıları "*kaptan*" olarak tabir edilen az sayıdaki bilgisayarları kullanan kişilerin saldırılarıyla başlar. Kaptan bilgisayarlar kullanıcı ağlarını tararlar ve kullanıcının bilgisayarına küçük kod ya da servis kurmak için sistem açıklarını (genellikle en iyi bilinenlerini) kullanırlar. Bu bilgisayarlar artık birer "*zombi*" hâline gelir ve kaptan bilgisayarlar tarafından İnternetteki diğer bilgisayar veya ağlara saldırıda kullanılmak için tetiklenir (HENMI, Anne/LUCAS, Mark/SINGH, Abhisbek/CANTRELL, Chris: Firewall Policies and VPN Configurations, Canada 2006, s. 322.).

21 http://tr.wikipedia.org/wiki/OECD (E.T.: 09/04/2014)

"*Gizliliğin ve Sınır Aşan Kişisel Veri Trafiğinin Korunmasına Dair Kurallar*"ı benimsemişlerdir[22]. Bu kuralların bağlayıcılığı yoktur ve tavsiye niteliğindedir. Kurallar, 2013 yılında "*2013 OECD Gizlilik Kuralları*[23]" olarak yeniden düzenlenmiştir.

B. Avrupa Konseyi

Avrupa Birliğinden farklı bir yapıda, 1949 yılında, insan hakları, demokrasi ve hukukun üstünlüğünü savunmak amacıyla Avrupa çapında kurulmuş hükümetlerarası bir kuruluş olan Avrupa Konseyi'nin 28/01/1981 tarihli, "*Kişisel Verilerin Otomatik İşleme Tâbi Tutulma Sürecinde Şahısların Korunması*"na ilişkin 108 sayılı sözleşmesi, Avrupa'da kişisel verilerin korunmasına dair ilk uluslararası hukuk belgesi olarak karşımıza çıkmaktadır[24]. 1985 yılında yürürlüğe giren Sözleşme güçlü bir koruma yapısı içermemekle birlikte kişisel verilerin korunması konusunda kabul edilmiş bağlayıcılığı olan ilk uluslararası belge olması bakımından önemlidir[25].

Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Şahısların Korunmasına ilişkin bu sözleşme, kişisel verilerin kullanılması ve depolanması yanında, kişilerin başkaları tarafından toplanan verileri üzerinde kontrolünü belirlemeyi amaçlar ve bu konuda bir takım kurallar getirir[26]. Bu sözleşme Konsey üyesi diğer devletlerle birlikte Türkiye tarafından da imzalanmıştır ancak Türkiye sözleşmenin onaylanabilmesi için bir kanun çıkarma zorunluluğunu henüz yerine getirmemiştir.

C. Avrupa Birliği

Malların, kişilerin, hizmetlerin ve sermayenin serbestçe dolaşması düşünceleri üzerine kurulu Avrupa Birliği'nde, bu hedeflerin yerine getirilmesinde kişisel verilerin işlenmesi ve korunmasının zorunlu olması sebebiyle, Avrupa Birliği'nde kişisel verilerin korunmasını amaçlayan kurallar, bilgi teknolojilerinin gelişimi ile beraber

22 www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (E.T.: 09/04/2014)

23 http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (E.T.: 09/04/2014)

24 BAŞALP, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s.24.

25 ATAK, Songül: "*Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler*", TBB Dergisi, S.87, y.2010, s.90.

26 BEYLİ, Ceylin: "*Bilgi Toplumunda Kişisel Veriler - Kişisel Verilerin Korunması Kanun Tasarısı Üzerine Eleştiriler*", Bilişim Hukuku, der. Mete Tevetoğlu, İstanbul 2006, s.71.

Avrupa Birliği içinde ortak pazarının gereklerini dikkate alma ve serbest veri trafiğini temel haklara uygun işleme düşüncesiyle yürürlüğe konulmuştur[27]. Bu anlamda, 24/10/1995 tarihinde 95/46/EC sayılı "*Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi*" kabul edilmiştir[28].

Yönerge ile üye devletlerin kişisel verilerin korunmasına ilişkin mevzuatlarında yeknesaklığı ve Avrupa Birliği sınırları içerisinde kişisel nitelikli verilerin serbest dolaşımının sağlanması hususlarında üye devletlerin düzenlemeleri arasında uyumu sağlamaları[29] amacıyla kişisel verilerin korunmasına ilişkin temel ilkeler ortaya konulmuştur. Kişisel verilerin korunmasının dayanağı olan hakların, kişilik hukukundan doğduğu düşüncesiyle Yönerge sadece gerçek kişilerle sınırlı tutulmuştur. Tüzel kişilerin kişisel verilerinin korunması Yönerge kapsamında değildir. Hâl böyle olmakla birlikte yönergede tüzel kişilerin kişisel verilerinin korunmasına ilişkin düzenlemelere üye devletlerin kendi iç hukuklarında yer verebilecekleri belirtilmiştir.

Yönergede kişisel veri yanında hassas veri kavramlarına da yer verilmiştir. Buna göre, etnik ve ırksal köken, politik, dinî ve felsefî görüş, sendika üyeliği, sağlık ve cinsel yaşama ilişkin bilgiler hassas veriler olarak kabul edilmiştir. Kural olarak, hassas verilerin işlenmesi yasaklanmıştır. Ancak istisnaî olarak, veri sahibinin açık rızası, verilerin umuma açıklanmış olması, iş hukukundan kaynaklanan yükümlülükler, üstün nitelikli bir hakkının korunması, adlî makamlarda iddia ve savunma, suçla mücadele gibi konularda bu hassas veriler işlenebilir.

Yönergede bir takım ilkeler benimsenmiştir. Buna göre, veri sahibinin veri işlemesi konusunda bilgilendirilmesi gerekir, veri sahibinin eksik ve hatalı verileri düzeltme, verilerinin işlenmesini engelleme ve verilerinin işlenmesine itiraz etme hakları vardır. Verilerin işlenebilmesi için hukuka uygun yollardan elde edilmiş olması gerekir. Veriler ancak yasal amaçlar doğrultusunda işlenebilir ve toplanma amacını aşan mahiyette kullanılamaz, toplanma amacının gerektirdiği süreden daha uzun süre saklanamaz[30].

15/12/1997 tarihinde 97/66/EC sayılı "*Telekomünikasyon*

27 BAŞALP, 25.

28 Çalışmamızın bundan sonraki bölümlerinde bu düzenleme "*Yönerge*" şeklinde ifade edilecektir.

29 SAVAŞ, F. Burcu: "*İş Hukukunda 'Siber Gözetim'*", Çalışma ve Toplum Dergisi, S.22, y.2009, s.103.

30 http://bilgitoplumuhukuku.blogspot.com.tr/ (E.T.: 10/04/2014)

Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi" yürürlüğe girmiştir. Bu düzenleme Yönergenin tamamlayıcısı niteliğindedir[31]. 31/07/2002 tarihinde yürürlüğe giren 2002/58/EC sayılı "*Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi*" de Yönergenin tamamlayıcısıdır. Bu düzenleme Yönergeden farklı olarak tüzel kişilerin kişisel verilerinin de korunmasını amaçlamaktadır.

D. Avrupa Birliği Veri Koruma Yönergesi

07/02/1992 tarihinde imzalanan Maastricht Anlaşması ile Avrupa Ekonomik Topluluğu, Avrupa Topluluğu'na dönüştürülmüştür. Daha sonra Lizbon Anlaşması ile Avrupa Topluluğu[32] terimi Avrupa Birliği terimine dönüştürülmüştür[33].

Veri Koruma Yönergesi ile üye devletler arasında kişisel verilerin serbest dolaşımının sağlanması hedeflenmiştir. Gerçek kişilerin haklarının korunması ve özellikle özel hayatın korunması gibi sebeplerle veri trafiğinin engellenmesinin önüne geçilmesi amaçlanmıştır. Zira birliğe üye ülkelerdeki veri koruması düzenlemeleri arasındaki farklılıklar, ortak pazarın oluşumu ve işleyişi açısından bir engel oluşturacaktır[34]. Bu sebeple Yönerge ile bir taraftan kişisel verilerin serbest dolaşımının sağlanması

31 BAŞALP, 27.

32 "*Çoğu zaman Avrupa Birliği, her birine 'sütun' adı verilen görev alanlarına bölünmüş olarak tanımlanır. Avrupa Topluluğu Yönergeleri birinci sütunu oluştururken, ikinci sütun ortak dışişleri ve güvenlik politikasını ele alır. Üçüncü sütunda ilk olarak adalet ve içişleri konuları ele alınmışsa da Amsterdam ve Nice antlaşmalarında yapılan değişiklik ve eklentilerle bu sütunun görev alanı günümüzde yalnızca güvenlik güçleri ve adalet alanında iş birliğini kapsar. Bu bağlamda, ikinci ve üçüncü sütunlar devletler arasındaki işlemler olarak tanımlanabilir çünkü Komisyon, Parlamento ve Adalet Divanı gibi uluslar üstü kurumlar bu işlemlerde ya hiç rol oynamazlar ya da konuya çok az dâhil olurlar. Avrupa Birliği'nin yürüttüğü etkinliklerin çoğu birinci sütun çatısı altında gerçekleştirilir. Bu etkinlikler çoğunlukla ekonomik merkezlidir ve uluslar üstü kurumlar bu sütunun konularında daha etkilidir.*" (BİLGEN, Mustafa: "Uluslararası Birlikler - 2 Avrupa Birliği (AB)", http://www.tv5haber.com/yazar_6906_618_ab.html, E.T.: 10/04/2014)

33 Lizbon Anlaşması ile Avrupa Topluluğu ve Avrupa Birliği arasındaki ayrım ortadan kalktığı için üç sütunlu yapı da artık tek çatı altında toplanmıştır.

34 Üye Devletlerde uygulanan kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere bireylerin hakları ve özgürlüklerinin korunma seviyesindeki farklılıklar, bir Üye Devlet toprağından diğer Üye Devlete bu tür verilerin iletilmesini engelleyebilir; bu nedenle bu fark, Topluluk seviyesindeki birtakım ekonomik faaliyetlerin takibi için bir engel oluşturabilir, rekabeti bozabilir ve Topluluk hukuku kapsamında makamların sorumluluklarını yerini getirmesini engelleyebilir; koruma seviyesindeki bu fark, çok çeşitli ulusal kanunlar, yönetmelikler ve idari hükümlerin varlığından dolayıdır. (Yönergenin 7 numaralı gerekçesi.) (http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf, E.T.:10/04/2014); BAŞALP, 30.

amaçlanırken diğer taraftan da kişisel verilerin işleme usul ve yöntemleri belirlenerek kişilerin mağdur olmalarının önüne geçilmeye çalışılmıştır.

E. Almanya

Dünyanın ilk veri koruma kanunu, Almanya'nın Hesse Eyaletinde 1970 yılında kabul edilmiştir[35]. 1977 yılında ise Federal Veri Koruma Kanunu yürürlüğe girmiştir. 23/05/2001 tarihinde de Yönerge, Federal Veri Koruma Kanununda yapılan değişiklikle uygulanmıştır. Son olarak 2009 yılında bazı değişiklikler yapılmıştır.

Federal Veri Koruma Kanunu'na ek olarak verilerin korunmasına dair kurallar Sosyal Güvenlik Kanunu, Tele Medya Kanunu[36], Telekomünikasyon Kanunu gibi kanunlarda da mevcuttur[37].

Federal Veri Koruma Kanunu, gerçek ve tüzel kişilerin, şirketler, dernekler – vakıflar ile diğer özel kuruşların yanı sıra kamu otoritelerinin ve organlarının hem federal hem sınırlı olarak eyalet düzeyinde kişisel verileri toplamasına, işlemesine ve kullanmasına her iki sektör için farklı şekilde uygulanır[38]. Kanunda, Yönergeden faklı olarak kamu sektörüne ve özel sektöre uygulanacak kurallar birbirinden ayrılmıştır. Tüzel kişiler ve ölüler kanun kapsamına dâhil değildir. Ancak tek kişilik ticarî faaliyetlere ilişkin bilgiler kişisel veri olarak kabul edilmiştir. Hastanelerle ilgili özel kanunlarda ve meslekî gizlilik kurallarında ölümlerin kişisel verilerinin korunmasına ilişkin hükümler mevcuttur[39].

Yönergeden farklı olarak, Federal Veri Koruma Kanunu veriden uzak durma ve veri minimizasyonu ilkesine yer verilmiştir. Buna göre veri sorumluları, yeter düzeydeki asgarî kişisel veriden fazlasının toplanmaması ve kişisel verilerin mümkün olduğunca anonim hâlde ya da maskelenmiş (*psodonim*) şekilde tutulmasını sağlayacak tedbirleri almakla yükümlüdürler. Seçilen veri

35 RODRIGUES, Roberto/WILSON, J, Petra/SCHANZ, Stephen J.: The Regulation of Privacy and Data Protection in The Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to personal-Identifiable Health Databases, Washington 2001, s.76.

36 Kanunun 1. bölümünde, bu kanunun tüm elektronik bilgi ve iletişim servisleri hakkında uygulanacağı belirtilmiştir.

37 KUSCHEWSKY, Monika: Data Protection and Privacy: Jurisdictional Comparisons, "*Germany*", Londra 2012, s.169.

38 Kuschewsky, 170.

39 DDK, 123.

işleme yöntem ve tasarımı, kişisel verilerin tamamını toplamaya, işlemeye ve kullanmaya yönelmemelidir[40]. Bu ilkenin Yönergedeki "*verilerin ilgili olması ve aşırı olmaması*" ilkesine karşılık geldiği düşünülse de Federal Veri Koruma Kanunu daha sıkı bir koruma sağlamaktadır. Yine Federal Veri Koruma Kanununa göre kural olarak kişisel verilerin veri sahibinden alınması esastır. Diğer kaynaklardan verilerin toplanması istisnadır. Diğer kaynaklardan verilerin toplanması, kanunda açıkça gösterilmesi, kişisel verilerin veri sahibinden toplanmasının orantısız bir çabayı gerektirmesi, kişisel veri sahibinin yasal çıkarlarının zarar göreceği bir duruma yol açmaması, verilerin toplanmasının ilgili ticarî amaç için ya da kamu görevi için gerekli olması gibi hâllerde mümkündür[41].

Federal Veri Koruma Kanununda yer alan kurallar Yönergenin iç hukuka aktarılmış şeklidir. Ancak Almanya'da veri koruma ilkeleri Yönergeden daha önce şekillenmeye başlaması sebebi ile kısmen farklı ifadeler içermektedir[42]. Kişisel veriler ile hassas verilerin hangi durumlarda işlenebileceği gibi hususlar Yönerge ile paralel düzenlenmiştir.

Almanya'da veri kütüğü sahipleri üzerindeki devlet denetimi, farklı otoriteler tarafından yerine getirilmektedir. Federal Veri Koruma Komiseri, federal düzeydeki kamu kurumları tarafından yürütülen veri işleme faaliyetlerinde yetkilidir. Federe düzeyindeki Veri Koruma Komiserleri de yetki alanlarında işlem yaparlar. Komiserlerin bağımsızlıkları güçlü bir teminat altındadır. Özel sektörde veri işleme faaliyetleri de Federal Veri Koruma Kanununa tâbi olmakla birlikte bazı eyaletlerde denetleme yetkisi içişleri bakanlığına verilirken bazı eyaletlerde de oluşturulan Eyalet Veri Koruma Otoritelerine verilmiştir[43].

F. Fransa

Fransız veri koruma ve gizlilik ilkelerinin yasal çerçevesi, 2004-801 sayılı Kanunla değişen veri işleme, veri dosyaları ve bireysel özgürlükler ile ilgili hükümlerin yer aldığı 78-17 sayılı Kanunla sağlanmıştır. Bu Kanun daha sonra Yönerge ile uyumlu hâle getirilmiştir. Buna ek olarak, Medenî Kanun (özellikle 9. maddesi), İş Kanunu, Ceza Kanunu, 82-689 sayılı İş Kanunu, güvenlikle ilgili

40 FISCHER-HUBNER, Simone: IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms, Heidelberg 2001, s.17.

41 DDK, 124.

42 DDK, 122.

43 DDK, 131.

95-73 sayılı Kanun gibi diğer yasal kaynaklar gizliliğin korunması ve kişisel veriler ile ilgili hükümler içermektedir[44].

Kanunda kişisel veri, bir kişi ile ilişkilendirilebilecek, onu bir kimlik numarası ya da bir veya birden fazla özellik ile doğrudan ya da dolaylı olarak tanımlayan, her türlü bilgi olarak ifade edilmiştir. Veri öznesi ise, işleme kapsamındaki veri ilgilisi gerçek kişidir. Kanunda rızanın tanımı yapılmamıştır. Bu konudaki yorumlar Fransız Medenî Kanununa bırakılmıştır. Kanun da hassas verilerden ve ek olarak "*adlî veriler*"den de bahsedilmiştir[45]. Tanımlar dikkate alındığında tüzel kişiler Kanun kapsamında değildir.

Kanun, Avrupa Birliği dışında kurulu bulunan ve Fransa'da faaliyette bulunan veri kütüğü sahiplerine temsilci bulundurma zorunluluğu getirmiştir ve Kanunun uygulanmasında veri kütüğü sahibi adına ülkedeki temsilciyi sorumlu tutmuştur[46].

1978 yılında çıkarılan kanunla "*bağımsız bir idarî otorite*" olarak düzenleme yetkisine sahip CNIL (Bilişim ve Özgürlükler Ulusal Komisyonu/Commission Nationale de l'informatique et des Libertés) kurulmuştur. Bu Komisyon, Fransa'da hükümetten yasal olarak bağımsız kurulan idarî kuruluştur. Komisyon, Fransız Veri Koruma Kanununun uygulanmasını veri işleme faaliyetlerinin Kanuna uygun gerçekleştirilmesini sağlamakla yükümlüdür ayrıca belirli bilgi sistemleri otoritelerinin talepleri ile ilgili cevaplar verir ve bu konuda kararlar alır[47].

G. İngiltere

İngiltere'de, ilk olarak 1984 yılında kabul edilen Veri Koruma Kanununda, Yönergenin sonucu olarak yeni bir takım düzenlemeler yapılmış ve 1998 yılında kabul edilmiştir ve halen yürürlüktedir. Veri Koruma Kanunu, kişisel verilerin adil, yasalara uygun olarak ve belirtilen amaçlar için işlenmesi, belirli süre saklanması, kişisel verileri doğru ve güncel tutma, kişisel verileri koruma, veri sahibinin hakları, bilgi güvenliği ve kişisel verileri Avrupa Ekonomik Bölgesi'nin dışına gönderme olmak üzere sekiz bölümden oluşur[48].

44 DANA, Raphaël/TAVELLA, Ramiro: Data Protection and Privacy: Jurisdictional Comparisons, "*France*", Londra 2012, s.149.

45 DANA/TAVELLA, 151.

46 DDK, 112.

47 U.S. Congress, Office of Technology Assessment: Federal Government Information Technology: Electronic Record Systems and Individual Privacy, Washington 1986, s.151.

48 CUNHA, Mario Viola de Azevedo: Market Integration Through Data Protection: An Analysis of

1998 Veri Koruma Kanununda kişisel veri tanımı büyük ölçüde Yönergeye benzemektedir. İngiliz Temyiz Mahkemesinin 2003 yılında "*Durant v. FSA*" davasında yaptığı "*kişisel veri*" tanımı, veri kontrolörlerinin sorumluluklarının kapsamın belirlemede kaynak olmuştur[49]. Temyiz Mahkemesi, "*bireylerin kişisel ya da aile yaşantıları, iş veya meslekî kapasiteleri yönünden özel hayatını etkileyen bilgiler*" olması hâlinde bireyle ilişkilendirilebileceğini belirtmiştir. Mahkemeye göre, bir bilginin kişisel veri sayılabilmesi için, "*kişinin birlikte olduğu diğer kişiler veya yer aldığı faaliyetlerden ziyade kendisini odağına almış olması*" gerekmektedir. Bir belgede kişinin tek başına bulunan adı, kişisel veri sayılmaz[50]. Bu tanımlamalardan, kişisel veri kavramının İngiliz Hukukunda oldukça dar yorumlandığı anlaşılmaktadır.

İngiltere'de kişisel verilerin korunması ile ilgili kurum, ICO (*The Information Commissioner's Office*/Bilgi Komiserliği Ofisi) adlı, malî yönden Adalet Bakanlığı'na bağlı bir kurumdur. Bu durum ICO'nun oldukça sıkı bir şekilde hükümetin kontrolü altında olduğunu sonucu doğurmaktadır ve bu hâliyle Yönergede belirtilen bağımsızlık ilkelerini taşıdığı söylenemez[51].

VII. TÜRKİYE'DE KİŞİSEL VERİLERİN KORUNMASI

Ülkemizde henüz başlı başına bir "*Kişisel Verilerin Korunması Kanunu*" bulunmamaktadır. Hâl böyle olmakla birlikte, başta Anayasamız olmak üzere bir takım kanun ve yönetmeliklerin ilgili hükümleri ile kişisel veriler koruma altındadır.

Anayasamızın ikinci kısmının ikinci bölümünde "*Özel Hayatın Gizliliği ve Korunması*" başlığı altında yer alan 20. maddesine göre, "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*" Yine aynı fıkranın devamında kural olarak hâkim kararı olmaksızın kimsenin üstünün, özel kâğıtlarının ve eşyasının aranamayacağı ve bunlara el konulamayacağı belirtilmiştir.

Anayasamızın anılan maddesine 2010 yılında yeni bir fıkra eklenmiştir. Ek fıkrada herkesin, kendisiyle ilgili kişisel verilerin

---

the Insurance and Financial Industries in the EU, Dordrecht 2013, s.101.

49 TAYLOR, Mark: Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge 2012, s.119.

50 DDK, 136.

51 DDK, 147.

korunmasını isteme hakkına sahip olduğu, bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenleneceği belirtilmiştir. Bugün, bir türlü kanunlaşamayan tasarının anayasal dayanağını bu madde oluşturmaktadır.

4721 sayılı Türk Medenî Kanunumuzda da kişisel verilerin koruma altına alındığında tereddüt bulunmamaktadır. Türk Medenî Kanunumuz "*Kişiliğin Korunması*" başlığı altında 24. maddesinde hukuka aykırı olarak kişilik hakkına saldırılan kimsenin, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebileceği belirtilmiştir. Devamında kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırının hukuka aykırı olduğu belirtilmiştir. Yine 25. madde de kişilik haklarına saldırı hâlinde ne tür davaların açılabileceği belirtilmiştir.

Konunun takdiminde de belirtildiği üzere, kişisel veriler, kişilik haklarının bir bölümünü teşkil etmektedir ve kişisel verilerin korunması, kişinin şeref ve haysiyeti gibi manevî varlığına ilişkin haklarının korunması ile doğrudan ilgilidir. Bu bakımdan, kişisel verilerin hukuka aykırı olarak toplanması, işlenmesi ve dağıtılması durumlarında en azından şu aşamada, Medenî Kanun hükümlerine göre koruma istenmesi gerektiği açıktır.

Mevzuatımızda konunun ceza hukukuna ilişkin düzenlemeleri ise 5237 sayılı Türk Ceza Kanununun ikinci kitap, ikinci kısmında bulunan "*özel hayata ve hayatın gizli alanına karşı suçlar*" başlıklı dokuzuncu bölümünde yer almaktadır. Kişisel verilerin korunması gerektiği hususunda farkındalığın artmasına paralel olarak 06/03/2014 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren 6526 sayılı Kanunla, Türk Ceza Kanununda yer alan kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ile verileri yok etmeme suçlarında cezaların alt sınırları artırılmıştır.

5271 sayılı Ceza Muhakemeleri Kanunumuz, soruşturma ve

kovuşturma yürütülürken, şüpheli, sanık, mağdur ve müştekinin haklarını, bu arada kişisel verilerini ve özel hayatının gizliliğini, korumak ve için birçok düzenlemeye yer vermiştir. CMK'da düzenlenen, gözlem altına alma, şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması, diğer kişilerin beden muayenesi ve vücuttan örnek alınması, moleküler genetik incelemeler ve bunların gizliliği, fizik kimliğin tespiti, eşya veya kazancın muhafaza altına alınması ve bunlara el konulması, el konulamayacak mektuplar, belgeler, taşınmazlara, hak ve alacaklara el koyma, postada el koyma, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma, iletişimin tespiti, dinlenmesi ve kayda alınması gibi hükümler kişisel verilerin ve özel hayatın gizliliğinin korunması ile ilgilidir.

213 sayılı Vergi Usul Kanunun "*Vergi Mahremiyeti*" başlıklı 5. maddesinde; vergi muameleleri ve incelemeleri ile uğraşan memurların, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay'da görevli olanların, vergi kanunlarına göre kurulan komisyonlara iştirak edenlerin, vergi işlerinde kullanılan bilirkişilerin görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine müteallik olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları ifşa edemeyecekleri ve kendilerinin veya üçüncü şahısların yararına kullanamayacakları belirtilmiştir. Maddenin devamında açıklama ve ifşa yasağının istisnaları sayılmış ve açıklanan bu bilgiler ele alınarak dahi mükelleflerin haysiyet, şeref ve haklarına tecavüz edilemeyeceği belirtilmiştir.

5809 sayılı Elektronik Haberleşme Kanununda Bilgi Teknolojileri ve İletişim Kurumu'nun görev ve yetkileri arasında "*abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak*" sayılmıştır. Kuruma, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisi verilmiştir. Yine işletmecilere de kişisel veri ve gizliliğin korunması yükümlülüğü getirilmiştir.

6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanunda, 5490 sayılı Nüfus Hizmetleri Kanunda, sağlık alanındaki birçok kanun ve yönetmelikte, sosyal sigortalar ve genel sağlık sigortası ile ilgili mevzuatta, tapu-kadastro mevzuatında, Adli Sicil Kanununda,

Bankacılık Kanununda da kişisel verilerin korunması, bilgi güvenliği, özel hayatın gizliliğinin ve mahremiyetinin korunması ile ilgili birçok hüküm mevcuttur.

5809 sayılı Kanundan önce yürürlükte olan Telgraf ve Telefon Kanunu ve yine bazı maddeleri yürürlükten kaldırılan Telsiz Kanununa dayanarak "*Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*" yayımlanmıştır. Daha sonra 5809 sayılı Kanunun yürürlüğe girmesi ile Yönetmelik de güncellenmiştir. 24/07/2012 tarih ve 28363 sayılı Resmî Gazete'de yayımlanan "*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*" telekomünikasyon alanında Avrupa Birliği tarafından çıkarılan direktifler göz önüne alınarak güncellenmiş ve kişisel verilerin korunması ile ilgili olarak, arayan numaranın gizlenmesi ve gizli numaradan gelen aramaların kabul edilmemesi, kişisel verilerin, trafik verilerinin işlenmesi gibi hükümlere yer vermiştir.

VII. KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISI

A. Genel Olarak

28/01/1981 tarihinde kabul edilen ve 1985 yılında yürürlüğe giren Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Şahısların Korunmasına İlişkin 108 Sayılı Sözleşmesi Türkiye tarafından imzalanmış ancak onaylanamamıştır.

Avrupa Birliği çevresinde kişisel verilerin korunması konusunda yaşanan gelişmeler karşısında Adalet Bakanlığı tarafından Avrupa Birliği uyum yasaları çerçevesinde uzun zamandır kişisel verilerin korunmasına ilişkin tasarı çalışmaları yürütülmektedir. Özellikle bilişim alanında yaşanan hızlı gelişmeler, artık bu alanda bir kanunun çıkarılması gerektiği hususunda hem toplumda bir algı hem yasama üzerinde bir baskı oluşturmaktadır.

Kişisel verilerin korunması kanun tasarısı çalışmaları kapsamında 13/09/1995 yılında kurulan komisyon çalışmalarını tamamlayamadan 2000 yılında yeniden oluşturulmuştur. 2003'te hazırlanan bir tasarı, 2008'de yeni hâli ile meclise sunulmuş ancak kanunlaşamamıştır. Bazı değişiklikler yapılmak suretiyle Tasarı, 2012 yılında Adalet Bakanlığı Kanunlar Genel Müdürlüğü'nce

Başbakanlık'a gönderilmiştir. 2013 yılına gelindiğinde ise bu kez 2012 yılındaki tasarı üzerinde yine değişiklikler yapılmıştır. Çalışmamızın bundan sonraki bölümlerinde "*15/03/2013 tarihli Kişisel Verilerin Korunması Kanun Tasarısı*" dikkate alınacaktır[52].

B. Amacı

Tasarıda, kanunun amacı, "*kişisel verilerin işlenmesinde kişinin hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemek*" olarak belirtilmiştir. Tasarının önceki yıllardaki hâllerinde ise kanunun amacı "*kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddî ve manevî varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemek*" olarak belirtilmiştir. Kanunun amacında böyle bir değişikliğe gidilmesi bizce de isabetlidir. Zira temel hak ve özgürlüklerinin içerisinde kişinin dokunulmazlığının, maddî ve manevî varlığının da bulunduğu açıktır.

C. Kapsamı

Tasarıda, bu hükümlerin, kişisel verileri işlenen gerçek kişileriler ile bu verileri kısmen veya tamamen işleyen gerçek kişiler ve tüzel kişiler hakkında uygulanacağı belirtilmiştir. Tasarının ilk hâllerinde Avrupa Konseyi Sözleşmesi'nden ve 95/46/EC sayılı Yönergeden farklı olarak tüzel kişilerin korunmasından bahsedilmekte idi. Daha sonra yapılan değişiklikle tüzel kişilerin kişilik haklarının korunması kapsam dışında bırakılmıştır. Bu yaklaşım, kişisel verilerin çoğu kez kişinin manevî varlığına ilişkin hakları arasında yer alması dolayısıyla, tüzel kişilerin manevî tazminat isteme hakkının olup olmadığı tartışmalarını[53] akıllara getirmektedir. Tasarının kapsamı dikkate alındığında hukuka aykırı olarak ele

52 Bugüne kadar kaç tane "Kişisel Verilerin Korunması Kanun Tasarısı" hazırlandığını söylemek güçtür. Zira ortada taslak halinde bir metin vardır ve bu metin her gün, gelen talimatlarla, yapılan toplantılarla değişebilmektedir. Bu sebeple tasarının incelemesinde, madde madde tasarıdan bahsetmek yerine, elde edebildiğimiz son tasarı olan 15/03/2013 tarihli Tasarı'da yer alan kavramlar, Tasarı'ya hâkim olan genel ilkeler üzerinde durulacaktır. Ancak kavramlar ve ilkeler anlatılırken 15/03/2013 Tasarı'nın madde numaralarından bahsedilmesinde bir sakınca görülmemiştir. Bu metin bundan sonra "*Tasarı*" olarak anılacaktır.

53 Doktrin ve uygulamada, genel olarak, tüzel kişilerinin manevi haklarının olduğu ve manevi haklarının ihlali halinde yetkili organları aracılığı ile kişilik haklarında meydana gelen azalmaların giderilmesi için dava açabilecekleri kabul edilmektedir. (OĞUZ, 181; EREN, Fikret: Borçlar Hukuku Genel Hükümler, B.11, Ankara 2009, s.765; UYGUR, Turgut: Açıklamalı - İçtihatlı Borçlar Kanunu – Sorumluluk ve Tazminat Hukuku, B.2, C.2, Ankara 2003, s.2271)

geçirilen veriler nedeniyle kişilik hakları ihlâl edilen tüzel kişiler, Medenî Kanun ve Borçlar Kanundaki genel hükümlere göre koruma talep edeceklerdir.

Kişisel verilerin korunmasına ilişin bir kanuna sahip 99 ülkeden 86'sının kanunlarının hem özel hem kamu sektörünü kapsadığı göz önüne alındığında, Tasarının kapsam açısından genel eğilimlerle uyumlu olduğu söylenebilir[54].

D. Temel Kavramlar

1. Anonim Hâle Getirme

Tasarının "*Tanımlar*" alt başlığı altında anonim hâle getirme, "*kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*" olarak tanımlanmıştır. 2008 yılında TBMM'ye sunulan tasarıda ise "*kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hâle getirilmek suretiyle işlenmesi*" olarak tanımlanmıştır.

24/07/2012 tarih ve 28363 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 3/1.c maddesinde anonim hâle getirme, "*kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek ya da tüzel kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hâle getirilmesi*" olarak tanımlanmıştır[55].

Tasarı ile Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik arasında önemli bir fark vardır. Şöyle ki, kaynağın belirlenemeyecek hâle getirilmesi zaten "*kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi*" ile aynı düşünceyi ifade etmesi sebebiyle tasarının son hâlinde çıkarılan bu ifadenin Yönetmelikten de çıkarılması gerektiği kanaatindeyiz.

2. İlgili Kişi

İlgili kişi, kişisel verisi işlenen gerçek kişidir. Buna göre artık tüzel kişilerin kişisel verilerin işlenmesi hâlinde çıkarılması plânlanan

54 DDK, 289.

55 Bu tanım, 11/07/2013 tarih ve 28708 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik 1. Maddesi ile değiştirilmiş hâlidir.

kanun çerçevesinde korunmayacaktır. Bunun yerine tüzel kişiler, kişilik hakları ihlâl edildiğinde, Türk Medenî Kanunu ve Türk Borçlar Kanunundaki önleme, durdurma, tespit, maddî - manevî tazminat, vekâletsiz iş görme gibi davaları açabilirler.

3. Kişisel Veri

Çıkarılması plânlanan kanunun korumayı hedeflediği ana unsur kişisel veridir. Tasarıda, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" kişisel veri olarak tanımlanmıştır[56]. Bu bağlamda kişinin adı, soyadı, doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, cihaz kimlikleri, hobiler, tercihler, iletişimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişisel veri sahibini doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır[57]. Yine Yargıtay, kamu oyunda çokça tartışılan bir kararında kimlikleri tespit edilemeyen mağdurelerin uygunsuz fotoğraflarının çekilmesini kişisel verilerin kaydedilmesi kapsamında değerlendirmemiştir[58].

56 Yargıtay, "*...suçun maddî konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği, iddiaya konu olayda, mağdurenin çıplak vaziyetteki görüntü ve fotoğraflarının kaydedilmesinden ibaret eylemin, "Kişisel verilerin kaydedilmesi" suçunu oluşturmayacağı...*" şeklinde verdiği bir kararında, bir kişinin görüntü ve fotoğraflarının kaydedilmesinin özel hayatın ihlâli kapsamında değerlendirilmesi gerektiğini vurgulamıştır (Y. 12 C.D., 11/09/2012 T., 2012/17703 E., 2012/18222 K.).

57 DDK Raporu, 778.

58 *"...sanığın, resim çekme sistemi çalışır vaziyetteki taşınabilir telefonunu, kimlikleri tespit edilemeyen mağdurelerin, etek altına ve bacak, göğüs gibi erojen bölgelerine odaklayarak, onların bilgi ve rızaları dışında, fotoğraflarını çekmesi şeklinde gelişen eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturacağı, anılan suçun aynı Kanunun 139/1. maddesi uyarınca soruşturulması ve kovuşturulması şikâyete bağlı olup, mağdurelerin tespit edilememiş ve sanık hakkında usulüne uygun şikayette bulunulmamış olması karşısında, sanık hakkında açılan kamu davasının şikayet yokluğu nedeniyle 5237 sayılı TCK'nın 139/1, 73/1 ve 5271 sayılı CMK'nın 223/8. maddeleri uyarınca düşmesine karar verilmesi*

4. Kişisel Verilerin İşlenmesi

Tasarıda, "*kişisel verilerin tamamen veya kısmen, otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" kişisel verilerin işlenmesi olarak tanımlanmıştır.

Tanıma göre verilerin toplanmaya başlamasından itibaren verilerin yok edilmesine kadar tüm işlem adımları kişisel verilerin işlenmesi kapsamında değerlendirilmiştir. Yine kişisel veriler, bilgisayar gibi otomasyon sistemlerinin kullanılması yöntemiyle işlenebileceği gibi, otomasyon sistemleri kullanılmadan, örneğin, defter tutmak suretiyle, işlenmesi hâli de tanım kapsamındadır.

5. Veri Kayıt Sistemi

Tasarıda, "*kişisel verilere ulaşımı kolaylaştıracak şekilde, belirli bir kritere göre yapılandırılmış kayıt sistemi*" olarak tanımlanmıştır. Böylece belirli bir kritere göre yapılandırılmamış sistemler, veri kayıt sistemi olarak nitelenemeyecektir. Kişisel verilerin rastgele bir metin dosyasında saklanmasından sonra her zaman bu verileri, belirli bir sistem dâhilinde işlemek mümkündür. Bu bakımdan "*belirli bir kritere göre yapılandırılmış olma"* şartı uygulamada sorunlara neden olabilir.

6. Veri Sorumlusu

Veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. Bu kişiler, verilerin saklanmasını, işlenmesini kontrol eden ve bundan sorumlu olan örneğin bir web sitesinin sahibi gibi gerçek kişi olabileceği gibi, kamu kurumları veya ticarî şirketler, dernek - vakıflar gibi tüzel kişiler de olabilir.

---

gerektiği gözetilmeden, suç vasfında yanılgıya düşülerek, sanığın yazılı şekilde mahkumiyetine karar verilmesi..." karşısında hükmün bozulmasına karar vermiştir (Y. 12 C.D., 11/09/2012 T., 2012/16872 E., 2012/18221 K.). Her ne kadar Yargıtay verdiği karar sebebiyle çokça eleştirilere maruz kalmış ise de, gerçekten de fotoğrafların kişisel veri sayılabilmesi için öncelikle kime ait olduklarının belirlenebilir olması gerekir. Diğer bir husus ise, kimliği belirli ya da belirlenebilir kimseye ait fotoğraf ya da video görüntülerinin kişisel verilerin kaydedilmesi mi özel hayatın gizliliğini ihlâl mi olduğunu failin yöneldiği amaç belirleyecektir. Yani failin amacı, kişinin özel hayatına müdahale ederek mağdurun özel yaşamına vâkıf olma amacı taşıyorsa özel hayatın gizliliğini ihlâlden, kişisel verilerini bir sistem dâhilinde toplama ve/veya işleme iradesi taşıyorsa kişisel verilerin kaydedilmesinden sorumlu tutulabilecektir.

7. Veri İşleyen

Veri sorumlusundan aldığı yetkiye dayanarak, onun adına kişisel verileri işleyen gerçek veya tüzel kişidir. Tasarının tanımlar başlıklı 3. maddesinde, önce veri işleyen, sonra veri sorumlusu tanımlanmıştır. Veri işleyen kişinin de veri sorumlusundan aldığı yetkiye dayanarak işlem yaptığı belirtildiğine göre öncelikle veri sorumlusunun tanımlanması gerektiği kanaatindeyiz.

Kişisel verilerin, her zaman veri sorumlusu adına işlenmesi söz konusu olmayabilir. Buna en güzel örnek UYAP sistemidir. UYAP ortamında herhangi bir dosyaya taraf dâhil edilmek istendiğinde kişinin daha önceden UYAP kayıtlarında kimlik ve adres bilgileri varsa dosyanın sistem kütüğüne oradan eklenir. Ancak daha önceden UYAP kaydı yoksa sistem, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün veri tabanına (Mernis'e) bağlanır ve oradan kimlik ve adres bilgilerini alarak UYAP ortamına aktarır. UYAP kullanıcısının Mernis'e erişmesinde, veri sorumlusu olarak nitelendirilmesi mümkün olan Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün erişim yetkisi verdiği açıktır. Ancak bu bilgilerin Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü adına işlendiğini söylemek güçtür. Bu bakımdan tanımdan "*onun adına*" ibaresinin çıkarılması gerektiği kanaatindeyiz.

Tasarıda, veri işleyen ve veri sorumlusu ayrı ayrı tanımlanmakla birlikte, bazı yerlerde "*veri işleyen*" ifadesinin hem veri işleyen hem veri sorumlusu yerine kullanıldığı görülmektedir. Örneğin, kanunun kapsamıyla ilgili maddesinde, "*kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemek*" ifadesinde kastedilen, hem veri sorumlusu hem veri işleyendir. Aksi, veri sorumlularının kanun kapsamında olmadığı anlamına gelir ki bu yorum kanunun, temel amacı ile de örtüşmez.

E. Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

1. Genel Olarak

Kişisel verilerin işlenmesine ilişkin genel ilkeler, Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tâbi Tutulma Sürecinde Şahısların Korunmasına ilişkin 108 sayılı sözleşmesi ve Yönergede yer alan "*verilerin kalitesine dair ilkeler*" ile paralel olarak düzenlenmiştir.

2. Hukuka Ve Dürüstlük Kurallarına Uygun Olma

Her şeyden önce kişisel veriler hukuka ve dürüstlük kuralına uygun olarak işlenebilir. Zaten hukuka ve dürüstlük kurallarına uygun olma hukukun genel ilkelerindendir. Bu ilkeler objektif niteliktedir ve herkesin göstermesi gereken davranış modelini çizer[59].

Toplum içinde orta zekâda, makul, mantıklı bir insanın kişisel verileri işlerken göstereceği davranış modeli, dürüstlük kurallarına uygun bir davranış modeli olacaktır.

Veri işleyen kimse, veri işleme amacını açık ve kesin bir biçimde belirlemelidir. Yani veri işleyen, kişisel verileri neden topladığını, ne şekilde topladığını, hangi amaçlarla ve hangi biçimde kullanacağını kişisel verilerle temas kurmadan önce veri sahibine bildirmelidir. Bu itibarla verilerin toplandığının, işlendiğinin kişisel veri sahibi tarafından biliniyor olması gerekir. Bu, dürüstlük kuralının ve hukuka uygunluğun bir gereğidir.

3. Doğru Olma

Kişisel veriler işlenirken, ilgili verilerin doğru olduğunun denetlenmesi gerekmektedir. Doğru olmayan verilerin, veri işleyen kimseye vermesi muhtemel zararları bir yana, özellikle verilerin üçüncü kişilere aktarıldığı durumlarda, kişisel veri sahibini de zarar tehlikesi ile karşı karşıya bırakma ihtimali mevcuttur.

4. Güncel Olma

Bu ilke kişisel verilerin doğru olması gerektiği ilkesi ile doğrudan irtibatlıdır. Zira bir kişisel veri güncel değilse, güncelliğini yitirmişse doğru olduğundan da söz edilemez. Dolayısıyla güncel olmayan bir kişisel verinin, kişisel veri sahibini zarar tehlikesi ile karşı karşıya bırakma ihtimali de aynı şekilde mevcuttur.

5. Belirli, Açık Ve Meşru Amaçlar İçin İşlenme

Hukuka ve dürüstlük kurallarına uygun olarak toplanan verilerin, hukuka aykırı bir biçimde kullanılması tâbi ki düşünülemez. Bu açıdan kişisel verilerin hangi amaçlarla işleneceği, tereddüt bulunmayacak biçimde açık ve net olmalıdır.

59 ZEVKLİLER, Aydın/ACABEY, M. Beşir/GÖKYAYLA, M. Emre: Zevkliler Medeni Hukuk, B. 6, Ankara 2000, s.32.; EDİS, Seyfullah: Medenî Hukuka Giriş ve Başlangıç Hükümleri, B. 6, Ankara 1997, 290 vd.

6. Amaçla Bağlantılı, Sınırlı Ve Ölçülü Olma

Kişisel veriler, açık ve net bir şekilde belirlenen amaçlarla bağlantılı, bu amaçların çizdiği sınırlar dâhilinde ve ölçülülük genel kuralı çerçevesinde toplanabilir ya da işlenebilir. Örneğin sadece belli bir okuldan mezun olan kişileri bir araya getirmeyi amaçlayan bir mezunlar derneğinin, kişinin etnik kökenini, cinsel eğilimlerini, mensup olduğu siyasî, felsefî görüşlerini toplaması ya da işlemesi karşısında elbette ki amaçla bağlantılı, sınırlı ve ölçülü davrandığı söylenemez. Ancak aynı türden kişisel verilerin, bir arkadaş bulma sitesinde toplanması ya da işlenmesi hâlinde, toplama veya işlemenin amaçla bağlantılı, sınırlı ve ölçülü olduğu söylenebilir. Zira kişinin yakınlık kurduğu diğer kişi ile ilgili olarak, onun etnik kökenini, cinsel eğilimlerini, mensup olduğu siyasî, felsefî görüşlerini bilme hakkı vardır.

7. Amaç İçin Gerekli Süre Kadar Saklanma

Kişisel veriler ilanihaye saklanmamalıdır. Toplandıkları ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Kişisel verilerin, veri sahibinin teşhis edilmesine imkân sağlayacak şekilde toplandığı veya işlendiği amaçlar için gerekli olan süreden daha fazla saklanmaması gerekir. Söz konusu amaca ulaşıldıktan sonra veriler anonim hâle getirilmeli veya silinmelidir. Yönergenin 6/1. maddesinde de paralel düzenlemeler mevcuttur.

F. Kişisel Verilerin İşlenme Şartları

Tasarının 5. maddesinde kişisel verilerin işlenme şartları belirtilmiştir. Buna göre, kural olarak, kişisel veriler ilgili kişinin rızası olmaksızın işlenemez. Rızaya bağlanmamış işlem hukuka aykırıdır[60]. İlgilinin rızası, bir hukuka uygunluk nedenidir. Rıza tek taraflı hukuki bir işlemdir ve bu itibarla işlemin geçerlilik şartlarına sahip olması gerekir[61]. Buna göre, veri sahibinin fiil ehliyetinin bulunmaması, veri sahibinin rızası alınırken iradesinin fesada uğratılması gibi hâllerde geçerli bir rızadan bahsedilemez.

Ancak kanunlarda kişisel verilerin rıza aranmaksızın işlenebileceğinin açıkça öngörülmesi, fiilî imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya fiil ehliyeti bulunmayan kişinin kendisinin veya bir başkasının hayatı

60 BAŞALP, 39.

61 OĞUZ, 124; EREN, 563.

veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olmak kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması, kişisel verinin, veri sahibi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumlarının birinin varlığı hâlinde veri sahibinin rızası olmaksızın kişisel verileri işlenebilir.

G. Özel Nitelikli Kişisel Veriler

Tasarının 6. maddesi özel nitelikli kişisel verilerden bahsetmektedir. Buna göre, kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili verileri, özel nitelikli kişisel veriler olup bunların işlenmesi yasaktır[62]. Tasarı'da özel nitelikli kişisel veriler, Yönergede belirtilen hassas verilerin karşılığı olarak kullanılmıştır. Yönergenin 8. maddesinde, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dinî veya felsefî inançları, siyasî görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklama yükümlülüğü getirmektedir. Özetle ırk ve etnik unsurlara, düşünce özgürlüğüne, sağlığa ilişkin veriler hassas olarak belirtilmiştir. Bunların ortak paydası ayrımcılık tehlikesidir[63].

Tasarının 6/2. maddesinde Yönergenin 8/2. maddesinde olduğu gibi özel nitelikli verilerin işlenmesinde hukuka uygunluk sebepleri gösterilmiştir. Bu hukuka uygunluk sebepleri, Tasarının 5/2. maddesinde ve Yönergenin 6. maddesinde öngörülen hukuka uygunluk sebepleriyle paralel niteliktedir. Buna göre, yeterli önlemler almak şartıyla, kanunlarda açıkça öngörülmesi, ilgili kişinin açık rızasının bulunması, siyasi parti, vakıf, dernek veya sendika gibi kâr amacı gütmeyen kuruluş ya da oluşumların,

62 Zaman zaman "*ırk*" ve "*etnik*" kavramlarının birbirlerinin yerine kullanıldığı görülse de bu iki kavram birbirlerinden farklıdır. Irk daha ziyade ortak bir biyolojik kökenden gelmeyi ifade eder. Etnik grup ise farklı bir tarihî kolektif şuurdan kaynaklanan kimliğin oluşturduğu bir tür sosyal gruptur. Etnik gruplar, kendi kültür, âdet, norm, inanç ve geleneklerine sahiptir. Etniklik belli bir ırk özelliğine dayanabileceği gibi kültürel veya siyasî faktörlerden de oluşabilir. Ancak ırk özellikleri ağırlık kazandıkça, etnik grup yerine, ırk grubu terimini kullanmak daha doğrudur. Bu durumda ırk grubu kavramının eş anlamlısı etnik azınlık gurubu olmaktadır. (http://www.felsefe.gen.tr/etnik_grup_ve_irk_grubu_nedir_ne_demektir.asp, E.T.: 20/04/2014)

63 BAŞALP, 43.

tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla kendi üyelerine ve mensuplarına yönelik verilerin işlenmesi, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, kişisel verilerin; kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler tarafından işlenmesi hallerinde hukuka uygunluk nedeni vardır ve bunlarla sınırlı olmak kaydıyla özel nitelikli veriler işlenebilir.

H. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hâle Getirilmesi

Tasarının 7. maddesi kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi ile ilgili hükümlere yer vermiştir. Buna göre, tasarıya ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

Avrupa İnsan Hakları Mahkemesi verdiği birçok kararda Yönergeye atıfta bulunmuş ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde yer alan "*özel ve aile hayatına saygı hakkı*"nı Yönerge ile birlikte değerlendirmiştir. Bu bağlamda Mahkeme, sadece bir kişinin özel hayatı ile ilgili bilgilerinin saklanmasının da Sözleşmenin 8. maddesi anlamında bir müdahale oluşturduğunu, bu bilginin daha sonra kullanılıp kullanılmamasının bir önemi olmadığını belirtmiştir[64]. Bu bakımdan, kişisel verilerin, işlenme sebepleri ortadan kalktığında silinmesi veya anonim hâle getirilmesi gerekir.

I. Kişisel Verilerin Aktarılması

Tasarının 8. maddesi kişisel verilerin üçüncü kişilere ve yurtdışına aktarılmasında uygulanacak usul ve esasları düzenlemektedir. Yurtdışına aktarımda ilk kural, ilgili yabancı ülkede yeterli korumanın bulunması şartıdır. Yabancı ülkelerde yeterli koruma bulunup bulunmadığına ise Tasarı ile kurulması plânlanan Kişisel Verileri Koruma Kurumu tarafından belirlenerek ilan edilecektir.

64 SALİHPAŞAOĞLU, Yaşar: "*Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme*", GÜHFD, C.XVII, S.3, y.2013, s.246.

Verinin istendiği yabancı ülkede yeterli koruma olmaması hâlinde, kişisel veriler, ancak veri sahibinin açık rızasının bulunması ile Türkiye'deki ve aktarılacağı yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmesi ve Kurumun izninin bulunması şartlarının birlikte varlığı hâlinde yurtdışına aktarılabilecektir.

J. Kişisel Verileri İşlenen Veri Sahibinin Hakları

1. Genel Olarak

Tasarının 10. maddesinde ilgili kişinin hakları yan başlığı altında kişisel verileri işlenen veri sahibinin veri sorumlusuna başvurarak kullanacağı hakları bent bent sayılmak suretiyle gösterilmiştir. Bu bentler incelendiğinde veri sahibinin haklarını genel olarak şu şekilde sıralayabiliriz.

2. Bilgi Edinme Hakkı

Tasarının 10. maddesinde sayılan haklardan veri sahibinin kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenmek, verileri işlenmişse buna ilişkin bilgi talep etmek, verilerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenmek, yurtiçinde veya yurtdışında verilerin aktarıldığı üçüncü kişileri bilmek şeklinde tanımlanan haklar veri sahibinin bilgi edinme hakkı kapsamında değerlendirilebilir. Bu haklardan da açıkça anlaşılacağı üzere veri sahibinin kendisi ile ilgili her türlü veriye dair bilgiyi edinme hakkı vardır[65].

Yönergenin 12. maddesinde de veri sahibine, aşırı gecikme veya masraf olmaksızın ve makul aralıklarla, herhangi bir sınırlama olmaksızın, kendisine dair verilerin işlenip işlenmeyeceği hususunda onay ve ilgili verilerin işlenme amaçları hususunda bilgi, işleme tâbi tutulan verilerin anlaşılır biçimde kendisine iletilmesi haklarını vermektedir. Dolayısıyla veri sahibi, bu hakkını bir kez kullanmakla hak tükenmeyecek, makul aralıklarla yani dürüstlük kuralları çerçevesinde kişi bu hakkını kullanabilecektir. Aynı şekilde kişinin hakkını kullanabilmesi için verilerinde değişiklik olmasına gerek yoktur. Yine makul aralığın ne kadar olacağı da toplanan verinin niteliğine göre belirlenmesi gereken bir durumdur. Banka hesap hareketleri konusunda daha hızlı bir cevap beklenirken medenî durumla ilgili verilerde aynı hızın

65 BAŞALP, 48.

beklenmesi uygun olmayacaktır[66].

Tasarıda, kişisel veri sahibinin hangi aralıklarla bilgi isteyebileceğine ilişkin bir ifade yer almamakla birlikte, Yönergeye uygun olarak kişisel veri sahibinin makul aralıklarla iyi niyet kuralları çerçevesinde bu hakkını kullanması gerekir. Aksi davranış hakkın kötüye kullanılması anlamına gelir ki hukuk bu kötü niyete izin vermez.

3. Verilerin Düzeltilmesini Ve Silinmesini Talep Hakkı

Kişiler kendileriyle ilgili verilerin eksik veya yanlış olması hâlinde bunların düzeltilmesini isteme hakkına sahiptir. Düzeltme hakkı hem yanlış verilerin doğru olanlarıyla değiştirilmesini hem de eksik olan verilerin tamamlanması kapsar. Aynı şekilde kişisel veri sahibi, 7. maddede öngörülen koşullar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkına da sahiptir. Bu, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde re'sen veya veri sahibinin talebi üzerine veri sorumlusu tarafından kişisel verilerin silinmesi yani veri sorumlusunun hâkimiyet alanından çıkarılması[67] demektir.

4. Bildirim, İtiraz Ve Tazminat Hakkı

Veri sahibinin veri sorumlusundan, kendisiyle ilgili verilerin düzeltilmesi, silinmesi veya yok edilmesi işlemlerini verilerin aktarıldığı diğer kişilere bildirilmesini isteme hakkı vardır. Bu bildirim, olası iyi niyet iddialarını bertaraf etmeye yönelik olduğu gibi bazen eski hâle getirme yönünde bir irade de taşır.

Tasarıya göre, veri sahibi, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz edebilir. Tasarının lafzına bakıldığında, itirazın "*özellikle otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması*" durumunda kullanılmasını ister gibi bir durum ortaya çıkmaktadır. Kanunun amacı, gerçekten kişisel verileri korumak ise işleme suretiyle ortaya çıkabilecek olumsuz sonuçlara veri sahibinin itiraz etme olanağı olmalıdır. Zira asıl olan kişisel verilerin toplanmaması ve işlenmemesidir. Ancak kanunun amacı, kişisel verileri korumaktan ziyade, kişisel verilerin sorunsuz biçimde

66 BAŞALP, 49.

67 BAŞALP, 50.

dolaşımını sağlamak ise bunun da net bir dille ifade edilmesi gerekir. Aksi hâlde, kişisel verilerin işlenmesinde üzerinde önemle durduğumuz aleniyet ilkesini bizzat kanun koyucunun kendisi göz ardı etmiş olur.

Yönergenin 15. maddesinde üye devletlerin, kişilere; işte performans, kredibilite, güvenilirlik, tutum ve benzeri bazı kişisel yönleri değerlendirmek için yalnızca verilerin otomatik işlenmesine dayalı ve kişileri önemli derecede etkileyen veya onları yasal bir etkiye maruz bırakan bir karara tâbi kalmama hakkı[68] vermelerini öngörmektedir. Kişi hakkında olumsuz nitelik taşımayan profil ise dikkate alınabilecektir. Yönergenin bu maddesi ile üye devletlere, otomatik işlemlerle değerlendirilip bir takdire yer vermeksizin oluşturulan özel kişisel profillerin kullanımını iç hukuklarında sınırlama zorunluluğu getirdiği[69] ve yukarıda eleştirel bir yaklaşım sergilediğimiz bendin, bu zorunluluktan kaynaklandığı açıktır. Ancak sınırlamanın ne şekilde yapılacağı üye devletlerin takdirine bırakılmıştır. Bu bakımdan kişisel veri sahibinin itiraz hakkı, Yönergenin 15. maddesi kapsamından daha geniş tutulabilirdi.

Tasarıda, verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması durumunda zararın[70] giderilmesini talep etme, veri sahibine tanınmış bir hak olarak gösterilmiş ise de zararın varlığı hâlinde zaten Türk Borçlar Kanunu oldukça kapsamlı bir koruma sağlamaktadır. Türk Borçlar Kanununun sağladığı korumaya bir de Türk Yargı Sistemi'nin hemen her konuda onlarca yıldır ürettiği yerleşik içtihatlar eklendiğinde zararın giderilmesini talep şeklindeki bendin bir tekrardan ibaret olduğu ve bu alana bir yenilik getirmeyeceği açıktır.

---

68 Nitekim Avrupa İnsan Hakları Mahkemesi, Leander v. İsveç kararında, "*başvurucunun, kendisi hakkında bilgi toplanmasının, toplanan bu bilgilerin içeriği hakkında kendisine bilgi verilmemesinin ve bu bilgilerin yanlışlığını kanıtlama hakkının kendisinden esirgenmesinin özel hayat hakkının ihlali olduğunu ileri sürmesi*" üzerine (SALİHPAŞAOĞLU, s.247), başvurucu hakkında güvenlik soruşturması yapılması suretiyle enformasyon toplanmasının ve bunların doğruluğuna ilişkin olarak başvurucuya itiraz hakkı verilmemesinin, özel hayatın gizliliğine müdahale oluşturduğuna karar vermiştir. (Türkiye Bilişim Derneği: Kişisel Verilerin Korunması, 2. Çalışma Grubu Raporu, Nisan 2008, s.21.)

69 BAŞALP, 54.

70 Zarar maddî olabileceği gibi manevî de olabilir. Manevî zararların varlığı hâlinde, hâkim, taleple bağlı kuralının istisnası olarak, paranın yanında veya paradan ayrı olarak özür dileme, kınama, geri alma, düzeltme, cevap verme, tespit, sembolik bir miktarın davacıya ödenmesi gibi tazmin şekillerine hükmedebilir (AYDOS, Oğuz Sadık: "*Basın Yolu İle Kişilik Hakları İhlâllerinde Manevî Tazminat*", GÜHFD, C.XVI, S.2, y.2012, s.23.).

Günümüzde teknolojik alanda yaşanan hızlı gelişmeler, tüm dünya medeniyetinde ortaya çıkan sosyal paylaşım olgusu, saniyeler içinde milyonlarca kişiye ait milyarlarca kişisel verilerin depolanma, aktarılma ve işlenme kabiliyeti göz önüne alındığında, Tasarı'nın, zayıf ve adeta çıplak konumdaki kişisel verileri işlenen veri sahibine, bahşettiği hakların ne kadar sınırlı ve muğlak olduğu ortadadır. Bu bakımdan, Tasarının 10. maddesinde belirtilen hakların genel çerçeveleri burada belirtildikten sonra ayrıntılarının genel hükümlere, içtihatlara ve yönetmelik boyutunda yapılabilecek diğer mevzuat çalışmalarına bırakması uygun olabilirdi.

K. Veri Sorumlusunun Aydınlatma Yükümlülüğü

Tasarının 9. maddesinde kişisel verilerin elde edilmesi sırasında veri sorumlusunun aydınlatma yükümlülüğü özel olarak düzenlenmiştir. Buna göre, veri sorumlusu, kişisel verileri elde ettiği sırada, kendisinin ve varsa temsilcisinin kimliği, verilerin hangi amaçla işleneceği, işlenen verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukukî sebebi, yukarıda saydığımız ve Tasarının 10. maddesinde yer alan veri sahibinin diğer hakları hakkında bilgi vermekle yükümlüdür.

Kişisel verilerin, veri sahibi dışındaki kaynaklardan edinilmesi hâlinde de veri sorumlusunun veri sahibine karşı yukarıda belirtildiği şekilde aydınlatma yükümlülüğü vardır. Veri sahibi, daha önceden kişisel verilerinin işlenmesine ve üçüncü kişilere aktarılmasına rıza göstermiş dahi olsa üçüncü kişi konumundaki yeni veri sorumlusunca bilgilendirildikten sonra makul sürede, kişisel verilerinin silinmesini talep hakkına sahip olmalıdır.

Kişisel verilerin silinmesi, yok edilmesi ya da anonim hâle getirilmesi durumunda da veri sorumlusu, veri sahibini ayrıca bilgilendirmekle yükümlü tutulmuştur.

L. Veri Sorumlusunun Veri Güvenliğine İlişkin Yükümlülükleri

Tasarının 11. maddesinde veri sorumlusu, verilerin hukuka aykırı olarak işlenmesini, verilere hukuka aykırı olarak erişilmesini önlemekle, verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli tedbirleri almakla yükümlü tutulmuştur.

Veri sorumlusu, verilerin kendi adına başka bir gerçek veya tüzel

kişi tarafından işlenmesine imkân vermesi hâlinde, yukarıda belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumlu tutulmuştur.

Veri sorumlusuna, tasarıda, kendi kurum veya kuruluşunda, ilgili hükümlerin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunluluğu yüklenmiştir. Veri sorumlusunun kamu görevlisi olması ya da kamu görevlisi sayılması hâllerinde denetim görevini ihmal etmesinin ayrıca görevi ihmal suçunu oluşturacağı açıktır.

"*Veri sorumluları ile veri işleyen kişiler öğrendikleri kişisel verileri bu kanun hükümlerine aykırı olarak başkasına açıklayamazlar ve kendi şahsi çıkarları için kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.*" hükmü karşısında veri sorumlularına getirilmiş bir sır saklama yükümlülüğü söz konusudur.

Son olarak işlenen verilerin yasal olmayan yollardan başkaları tarafından elde edilmesi hâlinde, veri sorumlusuna bu durumu en kısa sürede veri sahibine ve kurulması plânlanan Kişisel Verileri Koruma Kurumuna bildirme yükümlülüğü getirilmiştir.

M. Veri Sorumlusunun Bildirim Yükümlülüğü

Tasarıda, "*Veri Sorumluları Sicili*" yan başlığı altında veri sorumlusunun, Kurum tarafından kamuya açık olarak tutulması plânlanan "*Veri Sorumluları Sicili*"ne kayıt olma zorunluluğu ve bunun usul ve esasları ile istisnalarına yer verilmiştir. Buna göre, "*kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Sicile kaydolmak zorundadır. Ancak, işlenen verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurumca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurum tarafından, Sicile kayıt zorunluluğuna istisna getirilebilir.*". Maddenin devamında ise bildirimle yapılacak kayıt başvurusunda nelerin bildirileceği belirtilmiştir.

Yönergenin 18. maddesinde üye devletlere, kısmen veya tamamen otomatik işleme faaliyeti yürüten veri sorumlusunun, bu faaliyetlerine başlamadan önce yetkili makamlara bildirimde bulunmasını sağlama yükümlülüğü getirilmiştir. Tasarıda bahsedilen Veri Sorumluları Sicili'ne kayıt zorunluluğu da bu

yükümlülüğü yerine getirme amacını taşır. İşlemin kısmen veya tamamen otomatik olması hâlinde yetkili makamlara bildirim zorunlu kılınmıştır (Yönerge m. 18). Ancak işlemin otomatik olmaması, yetkili makamlara bildirim zorunluluğunu ortadan kaldırır[71].

N. İstisnalar

Tasarıda yer alan hükümlerin bazı hâllerde uygulanmayacağı belirtilmiştir. Buna göre,

a) Kişisel verilerin, gerçek kişiler tarafından tamamen kişisel veya aynı konutta beraber yaşayanlarla ilgili faaliyetlerine ilişkin olarak işlenmesi halinde,

b) Kişisel verilerin anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi halinde,

c) Kişisel verilerin, bu Kanunda belirtilen genel ilkelere, veri güvenliğine ilişkin tedbirlere ve mesleki davranış kurallarına uygun olarak basın özgürlüğü çerçevesinde işlenmesi halinde,

d) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunun istihbari faaliyetlere ilişkin hükümleri çerçevesinde kişisel verilerin işlenmesi halinde,

e) Kişisel verilerin, milli güvenlik ve milli savunma amacıyla işlenmesi halinde,

Bu kanun hükümleri uygulanmayacaktır.

O. Genel Değerlendirme

Tasarı genel olarak incelendiğinde, Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Şahısların Korunmasına ilişkin 108 sayılı sözleşmesi ve Yönerge paralelinde hazırlandığı ve çoğu kez Yönergenin Türkçe tercümesi olduğu görülecektir. Avrupa Birliği ile Türkiye arasındaki gerek adlî gerek idarî teşkilatlanma arasındaki farklılıklar dolayısıyla kanun hazırlanırken, yabancı hukuka ilişkin kavram ve hükümlerin

71 BAŞALP, 57.

deyim yerinde ise daha çok "*içselleştirilmesi*" gerektiği açıktır. Bu bağlamda, hem kavramların, hem hak ve yükümlülüklerin daha açık ve anlaşılır şekilde tasarıya yansıtılması önemlidir.

Tasarının yasalaşması ile birlikte genel olarak bu alandaki bir boşluğun doldurulacağı açıktır. Ancak Tasarı'nın "*Suçlar*" başlığı altında yer alan maddesindeki "*kişisel verileri silmeyen veya anonim hâle getirmeyen veri sorumlusu*"nun cezalandırılacağına ilişkin hüküm haricinde diğer hükümlerde hep TCK'ya atıfta bulunulmuştur ve bu anlamda tekrara düşülmüştür. Zaten kişisel verilerin korunması ile ilgili TCK'da hükümler mevcuttur. Kişisel verileri silmeyen veya anonim hâle getirmeyen veri sorumlusunun cezalandırılacağına ilişkin hükmün ek fıkra hâlinde TCK'ya eklenmesi ile kanaatimizce tekrardan kurtulmak mümkün olabilir.

Tasarı'da yer alan kabahatlere ilişkin hükümlerin de 5326 sayılı Kabahatler Kanunu içerisinde yer almasında bir sakınca yoktur. Böylece hangi kanunda nelerin aranacağı net bir şekilde ortaya konulmuş olabilir.

Şu aşamada böyle bir kanunun yürürlüğe girmesinde tereddütlerin, endişelerin olması kaçınılmazdır. Zira kanunla yeni bir takım, terimler, hak ve yükümlülükler ile yeni kurumlar hukuk sistemimize dâhil edilmektedir ve tasarının okunduğu hâli ile anlaşılması da güçtür. Gerek kişisel verileri işleyen gerek kişisel verileri işlenen gerekse toplumun diğer bireylerine tasarı anlatılmalı, görüşleri, talepleri, endişeleri alınmalı ve takibinde mevzuat çalışmaları yapılmalıdır. Ancak görülen odur ki, ilk komisyonun kurulduğu 1995 yılından bu yana bu yönde bir çalışma yapılmamış ve Sözleşme ile Yönerge hükümleri üzerinden tasarı çalışmalarına devam edilmiştir. Bu sebeple tasarının bazı yönleri belirsizliğini korumaktadır. Örneğin, üyelik sistemi ile web sitesine kullanıcı kaydı yapan bir web sitesi yöneticisinin kişisel verileri toplamak yönündeki eylemi kişisel midir? Ya da Tasarı'nın "*İstisnalar*" başlığı altında yer verilen "*tamamen kişisel olarak işleme*" nedir, hangi hallerde kişinin eylemi kişisel olarak işleme, hangi hâllerde başka türlü işleme olarak kabul edilecektir?

Kişisel verilerin korunması sadece "*Kişisel Verilerin Korunması Kanunu*"na indirgenmemelidir. Kişisel verilerin korunmasına ilişkin DDK raporunda, *"Kimlik Paylaşımı Sistemi Yönetmeliği'nin 11. maddesinin 3. fıkrasında; "Kimlik Paylaşımı Sistemi çerçevesinde kimlik bilgisine erişebilen kamu kurum ve kuruluşlarınca ve 5411*

sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankalarca kişilerden ayrıca nüfus cüzdanı örneği veya kimlik bilgilerine ilişkin başkaca bir belge istenemez." düzenlemesine ve Ocak 2013 itibariyle Kimlik Paylaşım Sistemine online erişebilen kamu kurumu ve özel kuruluş sayısının 2.478 olmasına rağmen, pek çok işlemde kişilerin kimlik fotokopisinin alınması uygulamasına devam edildiği" rapor edilmiştir[72]. Raporda da açıkça görüleceği üzere, kanun çıkarmak yetmemekte, çıkarılan mevzuat hükümlerinin yönetmelik, tebliğ, genelge ve benzeri ek uygulamalarla ilgililere ulaştırılması, eylemsizlik prensibine sıkı sıkıya bağlı kamu kurum ve görevlilerini harekete geçirecek bir takım tedbirlere başvurulması gerekmektedir.

Tasarıda, kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esasların belirlenmesi yönetmeliğe bırakılmışken kanunun bir bölümün kurulması plânlanan Kişisel Verileri Koruma Kurumuna ayrılması da kanunun odak noktasını kaydırmaktadır. Kişisel verilerin korunmasına ilişkin müstakil bir kanuna sahip ülkelerin çok büyük bir kesiminde, bu alanda önleyici, düzenleyici tedbirleri almak üzere bağımsız bir kurumun bulunduğunu, ayrıca Avrupa Birliği'nin 2013 yılı Türkiye İlerleme Raporunda "*tamamen bağımsız bir veri koruma otoritesinin kurulması gerektiği*"nin belirtildiğini göz önüne almakla birlikte, Kanunda bir madde ile Kişisel Verileri Koruma Kurumunun kurulacağı belirtildikten sonra kurulması, kadrosu, hizmet birimleri, görev ve yetkileri gibi hususlar ayrı bir kanun, tüzük ya da yönetmelik gibi unsurlara bırakılabilirdi. Ancak bu yöndeki bir düzenlemenin kanun koyucunun tamamen takdiri olduğu hususu tartışmasızdır.

Tasarıda kurulması planlanan Kişisel Verileri Koruma Kurumu Başkanlığı'nın Adalet Bakanlığı'na bağlı olacağı belirtilmektedir. Tasarıda geçen "*bağlı*" yapı ile Sözleme ve Yönergede belirtilen ve Yönergeyi iç hukuklarına aktaran birçok ülkedeki "*bağımsız idarî otorite*"ler göz önüne alındığında Kişisel Verileri Koruma Kurumu Başkanlığı'nın bağımsız bir idarî otorite olarak kurulması gerektiği açıktır.

VIII. SONUÇ

Avrupa'da 1960'lı yıllarda tartışılmaya başlanıp 1980'li yıllarda yasal çerçeveye kavuşturulan kişisel verilerin korunması konusunda ülkemizde bu isimle bir kanun çıkarılmamış olması başlı

72 DDK raporu, 785.

başına bir eksiklik sayılamaz. Zaten Kişisel Verilerin Korunması Kanununun çıkarılmaya çalışılmak istenmesinin altında yatan asıl sebep Avrupa Birliği uyum sürecidir. Yoksa tabi ki kişisel veriler Anayasamız, Ceza Kanunumuz, Medenî Kanunumuz ve Borçlar Kanunumuz başta olmak üzere mevzuatla koruma altındadır. Tasarının tıkandığı husus da buradan kaynaklanmaktadır. Avrupa Birliği uyum sürecinde gerekli olan bir kanunun çıkarılması algısı, terimleri de tanımları da soyut hâle getirmektedir. Bu sebeple, Tasarı'nın "*Avrupa Birliği ile uyum*" ana fikrinden ziyade, Türk hukuk uygulamalarında bu alanda yaşanan aksaklık ve ortaya çıkan eksiklikleri gidermeye yönelik olarak düzenlenmesi, bu alanda yapılacak ikincil düzenlemelere temel teşkil edecek şekilde "*çerçeve kanun*" olarak hazırlanması, yukarıda bahsi geçen Anayasa, kanunlar ve yönetmeliklerde eksiklikler varsa ek maddelerle ya da güçlendirilmesi gereken yerler varsa madde değişiklikleri ile revize edilmesi daha kulağa hoş gelmektedir.

Öz olarak kişisel verilerin, genel olarak hak ve özgürlüklerin korunmasının iki boyutu vardır: Mevzuat boyutu ve ilgili kişi boyutu. İlki yukarıda belirtilmiştir. Ancak hak ve özgürlüklerin korunmasında, ikincisi ilkine nazaran daha önemlidir. Çünkü çoğu zaman, bireyin kendisini koruması durumunda, zarar tehlikesi ya en başından ortadan kalkmaktadır ya da mevzuatın sağlayacağı korumadan daha önce bertaraf edilmektedir.

Kişisel verilerin paylaşılmasının hemen öncesinde bazı hususlara biraz dikkat edilmesi, kişinin kurumlardan ya da hukuk düzeninden koruma talep etmesini gerektirmeyecek bir ortam sağlayabilir.

İnternetin kurallarına ilişkin farklı listelemeler yapılsa da, bizce İnternet'in birinci kuralı, İnternet ortamında sunulan hiçbir mal veya hizmetin karşılıksız olmadığıdır. Ücretsiz olması muhtemeldir ancak bedava değildir. Zira İnternet ortamında sunulan her şeyin az ya da çok bir karşılığı vardır. Bu karşılık, para ve benzeri nakdi bir değer olabileceği gibi kişi, mal ya da hizmetlerin reklamı da olabilir. Hiç biri değilse bile sunulan mal veya hizmet, mal veya hizmeti sunan kişi ya da kurumun tanınırlığını, şöhretini artırmayı amaçlıyor olabilir ki bu da bir nevi reklam ve mal veya hizmetten beklenen karşılıktır. İnternet kullanıcılarının bu fikri hep zihinlerinin bir köşesinde tutmaları, onları gelebilecek potansiyel tehlike ve tehditlere karşı daha dikkatli davranmalarına sevk edecektir. Bu bakımdan özellikle ücretsiz olduğu bildirilen mal

ve hizmetler İnternet üzerinden temin edilirken, kullanıcılardan istenilen her türlü bilginin titizlikle irdelenip, muhtemel riskler en aza indirgendikten sonra gerekiyorsa verilmesinde fayda vardır.

İnternet kullanıcıları, İnternet ortamından temin ettikleri her türlü program, ses dosyası, görüntü dosyası, imaj dosyası ve saire belgenin güvenirliğini test etmeden, bu belgelerin güvenirliği yönünde araştırma yapmadan ya da güvenilir olduğuna kesin kanaat getirmeden bilgisayar, cep telefonu gibi cihazlarına indirmemeli ve kullanmamalıdırlar. Bir servisinin ya da hizmetin güvenilir olup olmadığını öğrenmenin en iyi yolu yine İnternet'tir. Zira çok popüler bir arama motoruna program, mal veya hizmetin güvenilir olup olmadığı yönünde girilecek bir sorgu ifadesinde, ekrana gelecek onlarca sosyal paylaşım sitelerinde, tartışma forumlarında çok sayıda insanın kullanıcı deneyimleri yer almaktadır. Bu ise, sunulan program, mal veya hizmetin güvenilir olup olmadığı hususunda kullanıcıya fikir verir.

Özellikle üye kaydı yapan web sitelerini ve bu sitelerle bağlantılı diğer yazılımları kullanmak için kişisel veriler açıklanırken varsa kullanıcı sözleşmeleri, gizlilik politikaları dikkatlice okunmalı, böyle bir kullanıcı sözleşmesi ve gizlilik politikası yoksa kişisel verilerin açıklanacağı muhtemel kişilerden e-posta ve benzeri bir yolla bilgi talep edilmelidir. Zira kişinin, kendi verisi üzerindeki hâkimiyeti açıklanana kadardır. Bu veriler açıklandıktan sonra yetki ve inisiyatif tamamen üçüncü kişilerdedir. Kanunun amacı da öz itibariyle, bu yetki ve inisiyatifin veri sahibine zarar vermeksizin, usul ve yasalara uygun olarak kullanılmasını sağlamaya yöneliktir.

Yine yukarıda bahsedilen türden web siteleri ve diğer programlar aracılığı ile kişisel veriler açıklanırken bunların ne amaç için istendiğinin ve/veya kullanılacağının veri sahibi tarafından öngörülmesi en azından öngörülmeye çalışılması gerekmektedir. Zira bir okulun mezunlarını bir araya getirmeye çalışan ya da kullanıcılara bedava müzik indirme olanağı sunduğunu iddia eden bir İnternet sitesi, veri sahibinin banka ve kredi kartı bilgilerini, cinsel eğilimlerini, siyasî görüşünü öğrenme çabası içerisine girmişse veri sahibinin, kişisel verilerini açıklamadan önce mutlaka bir kez daha durup düşünmesi gerekir.

***

KAYNAKÇA

ATAK, Songül: "*Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler*", TBB Dergisi, S.87, y.2010, s. 90-120.

AYDOS, Oğuz Sadık: "*Basın Yolu İle Kişilik Hakları İhlâllerinde Manevî Tazminat*", GÜHFD, C.XVI, S.2, y.2012, s.1-36.

BAŞALP, Nilgün: Kişisel Verilerin Korunması ve Saklanması, Ankara 2004.

BEYLİ, Ceylin: "*Bilgi Toplumunda Kişisel Veriler - Kişisel Verilerin Korunması Kanun Tasarısı Üzerine Eleştiriler*", Bilişim Hukuku, der. Mete Tevetoğlu, İstanbul 2006.

CUNHA, Mario Viola de Azevedo: Market Integration Through Data Protection: An Analysis of the Insurance and Financial Industries in the EU, Dordrecht 2013.

ÇEKER, Mustafa: "*İnternet Ortamında Yapılan Usulsüzlüklerden Bankaların Hukukî Sorumluluğu*", Prof. Dr. Bilge ÖZTAN'a Armağan, Ankara 2008.

DANA, Raphaël**/TAVELLA,** Ramiro: Data Protection and Privacy: Jurisdictional Comparisons, "France", Londra 2012, s.149-169.

EC-Council: Ethical Hacking and Countermeasures: Web Applications and Data Servers, New York 2010.

EDİS, Seyfullah: Medenî Hukuka Giriş ve Başlangıç Hükümleri, B. 6, Ankara 1997.

EREN, Fikret: Borçlar Hukuku Genel Hükümler, B. 16, Ankara 2014.

ERGÜN, İsmail: Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara 2008.

FISCHER-HUBNER, Simone: IT-Security and Privacy-Design and Use of Privacy-Enhancing Security Mechanisms, Heidelberg 2001.

HENMI, Anne**/LUCAS,** Mark**/SINGH,** Abhisbek**/CANTRELL,** Chris: Firewall Policies and VPN Configurations, Canada 2006.

KUSCHEWSKY, Monika: Data Protection and Privacy: Jurisdictional

Comparisons, "Germany", Londra 2012, s.169-193.

OĞUZ, Habip: İnternet Ortamında Kişilik Haklarının İhlâli ve Korunması, B.2, Ankara 2012.

RODRIGUES, Roberto**/WILSON,** J, Petra**/SCHANZ,** Stephen **J.:** The Regulation of Privacy and Data Protection in The Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to personal-Identifiable Health Databases, Washington 2001.

SALİHPAŞAOĞLU, Yaşar: "*Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme*", GÜHFD, C.XVII, S.3, y.2013.

SAVAŞ, F. Burcu: "*İş Hukukunda 'Siber Gözetim'*", Çalışma ve Toplum Dergisi, S.22, y.2009.

SMITH, Graham J. H.: Internet Law and Regulation, B.4, Londra 2007.

TAYLOR, Mark: Genetic Data and the Law: A Critical Perspective on Privacy Protection, Cambridge 2012.

TIPTON, Harold F.**/KRAUSE,** Micki: Information Security Management Handbook, B.6, Northwest 2007.

TOPALOĞLU, Mustafa: Bilişim Hukuku, Adana 2005.

U.S. Congress, Office of Technology Assessment: Federal Government Information Technology: Electronic Record Systems and Individual Privacy, Washington 1986.

UYGUR, Turgut: Açıklamalı - İçtihatlı Borçlar Kanunu – Sorumluluk ve Tazminat Hukuku, B.2, C.2, Ankara 2003.

YAZICIOĞLU, R. Yılmaz: Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukukî Boyutları İle, İstanbul 1997.

ZEVKLİLER, Aydın**/ACABEY,** M. Beşir**/GÖKYAYLA,** M. Emre: Zevkliler Medenî Hukuk, B. 6, Ankara 2000.