Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi

21.05.2014
v. 01

İstanbul Bilgi Üniversitesi
LAUREATE INTERNATIONAL UNIVERSITIES

tepav
türkiye ekonomi politikaları araştırma vakfı

İSTANBUL BİLGİ ÜNİVERSİTESİ BİLİŞİM VE TEKNOLOJİ HUKUKU ENSTİTÜSÜ HAKKINDA:

16 Mayıs 2010 tarihli Resmi Gazete 'de yayımlanan Yönetmelikle kurulan Bilişim ve Teknoloji Hukuku Enstitüsü, Ülkemizin bu alanda çalışan ilk ve tek akademik birimidir. Enstitü, 2004 yılında yine İstanbul Bilgi Üniversitesinde kurulan Bilişim Teknolojileri Hukuku Uygulama ve Araştırma Merkezi'nin kazanımları üstüne kurulmuştur. Bir yandan kamu, özel sektör, STK ve akademi arasında bir köprü oluşturma misyonunu taşıyan Enstitü; öte yandan 2010 yılından beri bilişim ve bilişim hukuku alanında nitelikli insan kaynağı ihtiyacını karşılamak amacıyla Bilişim Hukuku Master Programı yürütmektedir. Enstitü; kamu kurum ve kuruluşlarına bilişim hukuku ve e-devlet konularında danışmanlık yapmakta ve regülasyonların hazırlanması noktasında destek olmaktadır.

Yazarlar:

Dr. Leyla Keser, Enstitü Direktörü

Dr. Mehmet Bedii Kaya, Enstitü Öğretim Görevlisi

Batu Kınıkoğlu, LL.M, Enstitü Uzmanı

TÜRKİYE EKONOMİ POLİTİKALARI ARAŞTIRMA VAKFI (TEPAV) HAKKINDA:

TEPAV üretilecek her bilginin, geliştirilecek her fikrin Türkiye'nin aydınlık geleceğine katkı sağlayacağı inancıyla bir grup işadamı, bürokrat ve akademisyen tarafından kuruldu. Türkiye'deki fikir tartışmalarının bilgi/veri içeriğini artıracak araştırmalar yapmak üzere Aralık 2004'te faaliyete geçti. TEPAV, politika önerileri geliştirmenin yanı sıra bazı alanlarda projeler geliştirerek, gerçekleştirilmelerine katkı sağlıyor. Uygulanmakta olan kamu politikalarının izlenmesi ve değerlendirilmesi çalışmalarında da bulunan TEPAV, bu çalışmalarını destekleyecek eğitim programları ve toplantılar organize ediyor. TEPAV, çalışmalarını "objektif ve partiler-üstü" yaklaşımdan ayrılmadan, akademik etik ve kaliteden ödün vermeden sürdürüyor.

Yazarlar:

Ussal Şahbaz, Teknoloji ve Girişimcilik Programları Yöneticisi

İdil Bilgiç Alpaslan, Araştırmacı

Ali Sökmen, Araştırmacı

Bu raporun birinci bölümü Türkiye Ekonomi Politikaları Araştırma Vakfı, ikinci bölümü Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından hazırlanmıştır. Raporun ilgili bölümleri yazarlarının görüşlerini yansıtmaktadır. Raporun bu taslak haline ilişkin görüşlerinizi yazarlarla paylaşabilirsiniz (Leyla Keser: leyla.keser@gmail.com; Ussal Şahbaz: ussal@tepav.org.tr)

İÇİNDEKİLER

YÖNETİCİ ÖZETİ

Kişisel verilerin korunması; İnternet ekonomisinin gelişimiyle birlikte önemi gittikçe artan bir konu haline gelmiştir. Veri teknolojisindeki gelişim sağlık, eğitim, finans, e-ticaret, dijital pazarlama, imalat gibi sektörlerde ekonomik fırsatlar doğurmaktadır. Verinin etkin kullanımı firma verimliliğini, sektörel katma değeri, tüketici faydasını ve sosyal faydayı artırmaktadır. Hızla büyüyen dijital medya sektörü, tüketicilerin kendilerine özelleştirilmiş içerik kullanabilmelerine imkan vermektedir. Sağlık alanında veri kullanımının yaygınlaşması, kişisel sağlık hizmetlerine erişimi artırmakta ve maliyetleri düşürmektedir. Eğitim alanında veri paylaşımının artması ve teknolojinin eğitime entegre edilmesi, küresel ölçekte verimlilik artışlarını tetikleyecektir. Finans sektöründe etkin veri derleme ve paylaşım mekanizmalarının kurulması, batık kredi riskini azaltarak KOBİ'lere açılan kredileri artıracaktır. Enerji ve altyapı sektörlerinde tüketim verisinin izlenmesi enerji tasarrufu sağlarken, üretim verisinin takibi ise üretim süreçlerinde etkinliği artıracaktır. E-ticaret platformlarının yaygınlaşması tüketici faydasını artırmakta, ihracatçıların dış pazarlara erişimini kolaylaştırmaktadır. İmalat sanayinde endüstriyel veri kullanımı, etkinliğin artmasını sağlarken maliyetleri de düşürecektir. Kamu sektöründe de gerek veri kullanımının kamu süreçlerine entegre edilmesiyle, gerekse verinin özel sektöre açılması sayesinde yeni iş modelleri kurgulanmasıyla verinin ekonomik etkinliği artırması mümkündür.

Ekonomik aktörlerin veri paylaşımından doğan fayda ve maliyetleri farklı olmakla birlikte, genel bir verimlilik artışı ve toplam ekonomik fayda da artış olmaktadır. Veri kullanan büyük şirketler daha esnek olabilirken, KOBİ'ler ise müşteri odaklı iş modellerine geçiş yapmakta, karar alma mekanizmalarını etkinleştirmektedir. Veri değer zincirinin her aşamasında faaliyet gösteren yeni girişimler, süreç inovasyonuna katkı sağlamakta, tüm bu gelişmeler ise tüketici faydasını artırmaktadır.

Kişisel verilere ilişkin olarak yapılacak yasal düzenlemelerde bugün; teknolojik, hukuksal ve ekonomik yaklaşımlar birlikte bir denge gözetilerek ele alındığında bilgi ekonomisi veya ağ ekonomisi geliştirilmekte ve aynı zamanda bireyin kişisel verilerinin korunması ihtiyacı da optimum şekilde yerine getirilmiş olmaktadır. Bireyin haklarının korunması ve iş dünyası dostu yasal düzenlemeler yapılması şeklindeki hassas dengenin gözetilmesi; ancak ilgili yasal düzenlemeler yürürlüğe girmeden önce yapılacak etki analizleri ile mümkündür. Bu raporun amacı da; yasa koyucunun gözetmesi gereken hassas dengede referans alabileceği küçük çaplı bir etki analizi yapmaktır.

Raporumuzda, halihazırda Bakanlar Kurulu Gündeminde bulunan Kişisel Verilerin Korunması Hakkındaki Kanun Tasarı'sının (Tasarı) yürürlüğe girmesinin; bireylere, kişisel verilerle katma değerli hizmetler sunan şirketlere, uluslararası ekonomik ve ticari ilişkilerimize kazandıracağı faydalar hukuksal ve ekonomik açıdan analiz edilmiştir. Raporun vurguladığı temel nokta; bireyin kişisel verilerinin korunması ile bu veriler odaklı inovasyonlar geliştiren endüstrilerin ihtiyaçları arasında denge gözetecek bir yasal düzenlemeye ihtiyacımızın açık olduğudur. Bu amaçla; Raporumuzda öncelikle dünyadaki veri korumasına ilişkin uluslararası sözleşmeler, konvansiyonlar ve AB müktesebatına uyum açısından içinde bulunduğumuz durum değerlendirilmiştir. Daha sonra; iç hukukumuzda ilgili sektörlerin ihtiyaçları doğrultusunda ilgili yasalara serpiştirilmiş kişisel verilerin korunmasına ilişkin hükümlere yer verilmiş ve bu hükümlerle sağlanan sektörel korumanın, bireyin kişisel verilerin korunması ihtiyacına ne kadar ve ne ölçüde hizmet ettiği analiz edilmiştir. Hukuki analize ilişkin bir diğer başlıkta ise; Tasarı'ya kaynaklık eden, 95/46 Sayılı AB Veri Koruması Direktifi'nde yer alan hükümler ile Tasarı'da yer alan ve Direktif'ten nispeten farklılaşan hükümlere ilişkin görüş ve önerilerimize yer verilmiştir. Mahkeme uygulamasında veri koruması hukukuna ilişkin yaklaşımlar Yargıtay kararları ışığında değerlendirilmiştir. STK'ların ve bazı Bakanlıkların Tasarı'ya ilişkin görüş ve değerlendirilmeleri tüm paydaşların **"orantılı"** bir veri koruma kanunun çıkması noktasında ortak paydada buluştuklarını göstermesi anlamında Raporumuzda yerini almıştır.

GİRİŞ

Kişisel verilerin korunması, özellikle ikinci dünya savaşından günümüze kadar gittikçe artan bir önemde ulusal ve uluslararası normların, sözleşme ve konvansiyonların konusunu oluşturmaktadır. Hazırlamış olduğumuz bu Rapor; kişisel verilerin korunmasına ilişkin kronolojik hukuki veya ekonomik gelişmeler ışığında, ülkemizde Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı özelinde ekonomik ve hukuki bir değerlendirme yapmaktadır.

Kişisel verilerin korunmasına dair Anayasa'da, Türk Ceza Kanunu gibi başka kanunlarda ve sektörel düzenlemelerde hükümler bulunmasına rağmen, henüz konunun özüne yönelik bir kanuni düzenleme yürürlüğe girmemiştir.

Raporun birinci bölümü Türkiye Ekonomi Politikaları Araştırma Vakfı (TEPAV) tarafından hazırlanmıştır. Birinci bölümde, öncelikle veri teknolojilerinde yaşanan gelişmelerin sağlık, eğitim, dijital pazarlama, e-ticaret, finans, imalat sanayii gibi sektörler için getirdiği ekonomik fırsatlar incelenmektedir. Daha sonra, kişisel verilerin paylaşılmasının ve kişisel verilerin korunmasına dair hukuki düzenlemelerin farklı ekonomik aktörler ve bireyler için fayda ve maliyetleri tartışılmaktadır.

Raporun ikinci bölümü İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından hazırlanmıştır. Bu bölümde veri korumasına ilişkin uluslararası normlar, AB uyum süreci açısından durum tespiti yapılmıştır. Pozitif hukukumuzda yer alan veri korumasına ilişkin hükümler ve bu hükümlerin sağladığı hukuki koruma seviyesi irdelendikten sonra, AB düzenlemeleri ışığında Tasarı'da yer alan hükümlere ilişkin görüş ve önerilerimize yer verilmiştir.

Uzun yıllardır yasalaşmasını beklediğimiz Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı'nın; AB ve dünyadaki veri korumasına ilişkin yaklaşımlar ışığında hukuksal ve ekonomik analizini yapmaya çalışan Raporumuzun; bilgi toplumu, ağ ekonomisi, veri odaklı inovasyon ile temel hak ve özgürlükler arasındaki dengeyi gözeten bir veri koruması yasasının yürürlüğe girmesi noktasında tüm paydaşlara faydalı olmasını diliyoruz.

1. VERİYE DAYALI EKONOMİNİN GETİRDİĞİ FIRSATLAR VE KİŞİSEL VERİLERİN KORUNMASININ EKONOMİK ANALİZİ

1.1. GİRİŞ

Çalışmanın bu kısmında kişisel verinin gelişimi, kişisel verinin üretildiği değer zinciri ve verinin farklı sektörel uygulamaları incelenmekte, teknolojik gelişmelerin farklı ekonomik aktörler açısından etkileri tartışılmaktadır. Bu bölümde yapılan değerlendirmeler, ekonomik bir perspektifle gerçekleştirilmiştir. Etik değerler veya evrensel hukuk kapsamında kişisel verilerin korunmasına yönelik yaklaşımlar, yer yer yapılan değerlendirmelerle örtüşebilmekle beraber, bu bölümdeki ana hareket noktası ekonomi bilimi olmuştur. Ekonomik bir perspektiften bakınca, kişisel verilerin korunmasına ilişkin düzenlemelerin ekonomik etkinliği artırabilen veya azaltabilen yönleri bulunmaktadır. Düzenlemeler büyük şirketler, KOBİ'ler, yeni girişimler ve tüketiciler gibi farklı ekonomik aktörler için farklı seviyede fayda ve maliyetler getirebilmektedir. Kişisel verilerin korunmasına dair bir kanuni çerçeve çizilirken bu etkiler analiz edilmeli ve kanuni çerçeve toplam ekonomik etkinliği azami seviyeye çıkaracak şekilde tasarlanmalıdır. Bu hukuki çerçeveye ilişkin tartışmalar ise raporun ikinci kısmında yer almaktadır.

1990'lı yılların ikinci yarısından itibaren İnternet'in yaygınlaşması ve son dönemde mobil teknolojilerin hızlı bir şekilde gelişmesi, günümüzde verinin toplanmasını, saklanmasını, paylaşılmasını ve analizini hiç olmadığı kadar kolaylaştırmıştır. 2016 yılında İnternet kullanıcı sayısının 3 milyara ve İnternet ekonomisinin hacminin 4,2 trilyon dolara çıkması beklenmektedir. G-20 ekonomilerinde İnternet ekonomisinin önümüzdeki beş yıllık dönemde yıllık yüzde 8 artış göstereceği ve geleneksel sektörleri geçeceği öngörülmektedir. Aynı dönemde İnternet ekonomisinin G-20 ekonomileri içindeki payı da, yüzde 5,3'e çıkacaktır[1].

İnternet ekonomisinin hızlı büyümesi iki kaynaktan beslenmektedir: 1) Kullanıcı sayısındaki artış, 2) İnternete daha hızlı erişim imkanı. İnternet'e bağlı cihazların (bilgisayar, tablet, mobil cihaz) ve bağlantı ücretlerinin ucuzlaması daha çok kişinin bu cihazlara erişebilmesini ve İnternet'e erişebilmesini sağlamıştır. Önümüzdeki dönemde mobil teknoloji kullanımının, bilgisayar üzerinden İnternete erişimden daha hızlı artması ve 2016 yılında beş bağlantıdan dördünün mobil platformlar üzerinden yapılması beklenmektedir[2]. İnternet'e erişimin

[1] BCG. (2012). "The Internet Economy in the G-20".
[2] Ibid.

kolaylaşması, veriye sahip olanlarla veri sağlayıcılar arasındaki keskin ayrımın ortadan kalkmasına sebep olmuştur. Geçmiş dönemde veriye sahip olanlar, başkaları tarafından üretilmiş verileri derlemekte iken, günümüzde aynı kişi hem veri sahibi hem de veri sağlayıcı olmaktadır.

Birbirine İnternet üzerinden bağlı cihazların artması, milyarlarca sensörün dünyadaki her hareketi kaydetmesi, derlenen verinin hacmini artırmakta ve büyük bir potansiyel doğurmaktadır. 2011 yılında dünyada oluşturulan ve kopyalanan veri 1,8 zetabytedır[3]. Her gün 500 milyon resim ve her dakika 200 saatlik video internete yüklenmektedir[4]. İnternetteki içerik, temelde şu veri türlerinden oluşur: 1) Yazılı materyaller, 2) Ses dosyaları, 3) Görsel dosyalar (fotoğraflar), 4) Animasyonlar, 5) Videolar, 6) İnteraktif materyaller. Böylesine bir veri havuzu ve değişik veri kaynaklarının varlığı, "büyük veri" kavramının doğmasını sağlamıştır. Büyük veri yalnızca daha çok veriyi değil, farklı kaynaklardan derlenen verilerin bir arada işlenmesini de ifade etmektedir.

KUTU 1: Veri Türleri: Analog ve Dijital Veri

Veriler üretildikleri formata göre ikiye ayrılır. Analog veriler, sinyaller şeklindedir. Örneğin, radyo dalgaları, elektromanyetik dalgalar, analog verilerdir. Analog veriler temsil ettikleri şeyi doğrudan gösterirler. Dijital veriler ise temsil ettikleri şeyi sayılar yolu ile gösterirler. Dijital veri, veriyi 0'lar ve 1'lerden oluşan ikili formda temsil eder. Örneğin, bilgisayarın hafızasında saklanan belgeler dijital veridir. Analog veriler, kopyalandıkları zaman kalite kaybına uğrayabilirken dijital veriler sayısal yapıları nedeniyle kayba uğramaz. Karşılaştırmalı bir örnek vermek gerekirse, VHS kasetleri analog, DVD'ler dijital veriler taşır.

Analog verilerin dijitalleştirilmesi mümkündür. Örneğin mikrofilm gibi analog formatta saklanan resimleri tarayıcı kullanarak içindeki temel verileri kaybetmeden bilgisayar hafızasına aktarmak bir dijitalleştirme örneğidir. Analog veriyi dijitalleştirmenin büyük avantajları vardır. Film, kaset gibi formatlarda saklanan analog veriler zamanla bozulurken dijitalleşen veri, bozulmadan sonsuza kadar saklanabilir. Dijitalleşen verilerin kopyalanıp dağıtılması da çok daha kolay hale gelir.

[3] 1 zetabyte 10^{15} megabytedır.
[4] Executive Office of the President of the USA. (2014). "Big Data: Seizing Opportunities, Preserving Values".

Veri kaynaklarının çeşitlenmesi ve oluşturulan verinin hacminin artması, hukuki çerçevenin oluşturulabilmesi ve düzenlemelerin yapılabilmesi için verinin sınıflandırılmasını zorunlu kılmaktadır. Farklı kaynaklardan doğan veriler, verinin niteliğine göre kişisel veya kişisel olmayan veri olarak nitelendirilebilir. Kişisel veri örnekleri şunlardır:

- Kişiler tarafından oluşturulan bloglar, yorumlar, fotoğraflar, videolar,
- Kişinin İnternet aktivitesine dair bilgiler, yaptığı aramalar,
- Sosyal platformlardaki veriler, kişinin arkadaşları ve çevreleri,
- Kişinin konum bilgisi,
- Kişinin demografik bilgileri,
- Resmi niteliğe sahip ve kişiyi tanımlamak için kullanılabilecek finansal veriler, hesap bilgileri, sağlık kayıtları, emniyet kayıtları, vs.

KUTU 2: Metaveri

Metaveri, başka verileri tanımlayan verilerdir. Metaveri, başka bir veriye dair temel bilgileri içerir. Örneğin bilgisayarda saklanan bir fotoğrafın kendisi verilerden oluşmaktayken o fotoğrafın nerede, ne zaman ve hangi makine tarafından çekildiği metaveridir. Metaveri, verilerin düzenlenip erişilebilmesine olanak verir.

Kişisel verinin derlenmesi için üç temel yöntem vardır: 1) Hakkında veri derlenmek isteyen kişi/kurum bilgilerini gönüllü olarak verebilir, 2) Kişisel veriler yasal olarak takip edilip toplanabilir, 3) Kişisel verilerin işlenmesi ile yeni veri setleri oluşturulabilir. Verilerin derlenmesinden kullanılmasına dek geçen süreç, toplama, saklama, analiz ve kullanımdan oluşan dört aşamalı bir değer zinciri ile mümkün olmaktadır[5].

- ***Veri toplama:*** İnternet kullanıcılarının sayısının artması ile birlikte, veri miktarı da hızla artmaktadır. Dolayısıyla hangi verinin toplanacağı ve takip edileceği de ayrı bir önem kazanmakta ve uzmanlık gerektirmektedir. Veri doğrudan veya dolaylı yollardan toplanabilir. Doğrudan veri toplamaya bir örnek, çevrimiçi perakendecilerin müşteri hareketlerini takip etmesidir. Dolaylı veri toplama faaliyeti ise, örneğin, kişinin mobil cihazındaki GPS bağlantısı üzerinden kişinin yerinin tespit edilmesi ve buna göre o bölgedeki promosyon tekliflerinin kişiye sunulmasıdır.

[5] Kişisel Verilerin Korunması Kanunu Tasarısı'nda bu aşamalar "kişisel verinin işlenmesi" kapsamında düzenlenmektedir.

- ***Veri saklama ve birleştirme:*** Verinin derlenmesinin ardından, saklanması ve grup hareketlerinin belirlenebilmesi için birleştirilmesi gerekir. Saklanan verinin hacminin hızla artması sebebiyle, son dönemde verilerin şirket dışı sunucularda saklanmasına imkan veren teknolojilerde de gelişme gözlenmektedir.
- ***Veriyi analiz etme ve aktarım:*** Toplanan ve saklanan verinin, başka veri kaynaklarından gelen bilgilerle bir araya getirilerek detaylı kişisel dosyaların oluşturulması, bu aşamadaki esas faaliyettir. Bu tür bir analiz, firmalar için çok çeşitli fırsatları da beraberinde getirmekte ve kişiselleştirilmiş hizmetlerin kalitesinin artmasını sağlamaktadır.
- ***Veri kullanımı:*** Farklı veri setlerinin bir arada kullanılması, yeni bir çok fırsat sunmakta ve daha önceki dönemlerde mümkün olmayan analizlerin yapılmasına imkan tanımaktadır. Derlenen, saklanan ve analiz edilen veriler, gereken durumlarda ve izin verilen şartlar altında, bu verileri kullanacak diğer kullanıcılarla paylaşılabilir. Pek çok kaynaktan derlenmiş kişisel bilgilere ulaşan firmalar, çoğunlukla bu bilgileri iş yapma biçimlerini ve tüketicilerle ilişkilerini geliştirmek ve doğru tüketici gruplarını belirlemek için kullanırlar.

KUTU 3: Veri Hayat Döngüsü

Veri hayat döngüsünde veriler yaratıldığı kaynaktan toplanıp, temizlenip, formatlanarak işlenir. İşlenen veriler daha sonra istatistiksel olarak analiz edilip yorumlanır. Büyük veri, devamlı olarak yaratılan yüksek hacimli verilerin veri hayat döngüsü dâhilinde analiz edilmesidir.

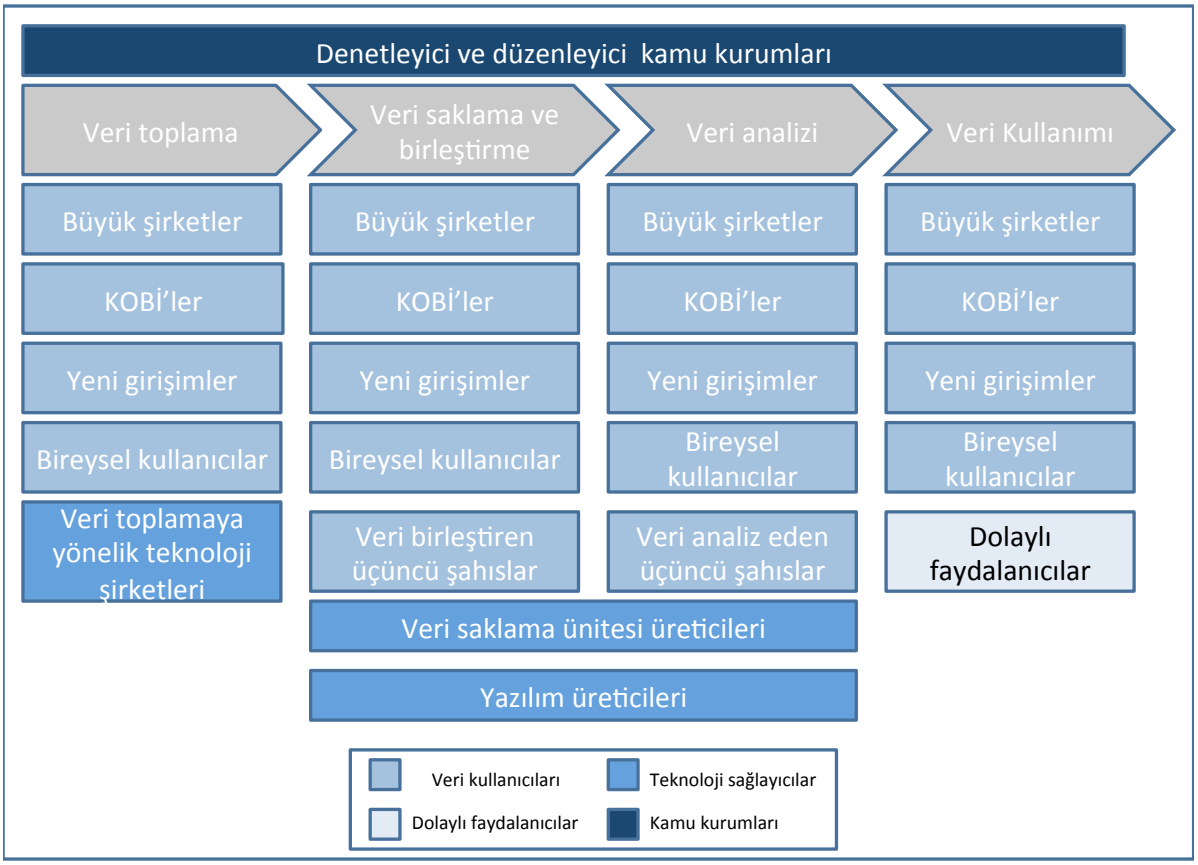
Kaynak: OECD - Exploring Data-Driven Innovation as a New Source of Growth

Gelişen teknoloji sayesinde azalan veri derleme, saklama, işleme ve kullanma maliyetleri, bilişim sektöründeki değer zincirinin büyümesini desteklemiştir. 2000'li yılların başında 1 GB veriyi harici diskte saklamanın maliyeti yaklaşık 20 dolar iken, 2013 yılında bu tutar 6 sent'e kadar inmiştir[6]. Bulut bilişimin gelişmesi ile beraber, sınırsız büyüklükte verinin aylık 5 dolar gibi düşük maliyetlerle saklanmasına imkan veren platformlar doğmuş ve veri saklama

[6] Komorowski, M. (2012). "A History of Storage Cost".

maliyetleri marjinal düzeye inmiştir[7]. Her iki yılda bir bilgisayarlardaki transistör sayısının ikiye katlanması ve düşen bilgisayar fiyatları bir arada düşünüldüğünde, veriyi işleme maliyetinin de hızla azaldığı anlaşılmaktadır[8]. Yüz yüze anketlerle ve telefonla veri toplamanın maliyeti kullanıcı başına 20-35 dolar arasında iken, İnternet üzerinden aynı verinin 1-5 dolar arasında toplanması mümkündür[9].

Şekil 1: Veri Zinciri Aşamaları ve Yer Alan Aktörler



Azalan maliyetler farklı kaynaklardan veri derlenmesini kolaylaştırdığı gibi, bu verilerin işlenmesi de tüketici tercihlerinin ve alışkanlıklarının belirlenmesini kolaylaştırmıştır. Kişisel veriler, firmaların mal ve hizmet üretimini daha etkin yapabilmeleri için kullandıkları değerli

[7] Backbaze, http://www.backblaze.com/İnternet-backup.html; Erişim tarihi: 30 Nisan 2014.
[8] Moore, G.E. (1965). "Cramming More Components Onto Integrated Circuits". *Electronics Magazine.* (Moore yasası, bilgisayarlardaki entegre devrelerde bulunan transistör sayısının iki senede bir ikiye katlandığını göstermektedir. Transistörlerin küçülmesi ve bilgisayarlarda daha fazla transistorün kullanılması, tekil çiplere daha fazla veri depolanmasına ve verinin daha hızlı işlenmesine imkan tanımaktadır. 2012 yılında IBM bir bit data yaratmak için gereken atom sayısını 1 milyondan 12'ye indirmeyi başarmışlardır. Bu, Moore yasasının öngördüğünden çok daha hızlı bir artış anlamına gelmekte ve önümüzdeki dönemde veri saklama ve işleme maliyetlerinin daha hızlı azalma ihtimaline işaret etmektedir.)
[9] Bhaskaran, V. "Online Research: A Handbook for Online Data Collection". *Survey Analytics, Issaquah, WA, USA*. 2005.

bir kaynağa dönüştürmüştür. Bu kaynağın finansal değerlemesi pek çok yöntem kullanılarak yapılabilir (Kutu 4).

KUTU 4: Kişisel verinin değerlemesi için kullanılabilecek yöntemler

- Kişisel veriye dayalı iş modeli olan firmalar için (Facebook ve diğer sosyal ağlar), firmanın piyasa değeri, gelirleri veya kullanıcı başına düşen net gelirin hesaplanması,
- Kişisel verinin yasal çerçevede satışından ve kullanımından doğan gelirlerin hesaplanması,
- Kişisel verilerin çalınması durumunda ortaya çıkacak maliyetin hesaplanması,
- Kişisel verileri satın almak isteyen firmaların ödemeye razı oldukları tutarın deneysel metotlarla ve anketlerle belirlenmesi,
- Kişinin kendi verilerini koruma altına almak için ödemeye razı olduğu sigorta bedelinin tespit edilmesi.

Kaynak: OECD. (2013). "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value". *OECD Digital Economy Papers.* 220.

Gelişen bulut bilişim hizmetleri, veri ekonomisinin bir diğer yükselen alanıdır.[10] Veri analizi için bulut bilişim altyapısı kullanmak ekonomik açıdan mantıklıdır. Büyük veri analizini kurum içerisinde yapabilmek için önemli sabit altyapı yatırımları gerekebilmektedir. Bulut bilişim altyapısı kullanılmaması durumunda veri analiz işlemleri şirketlerin kendi veri merkezlerinde yapılmaktadır. Firmalar kendi veri merkezlerine ilaveten anlık ihtiyaçlarına göre bulut bilişim altyapısının sunduğu kapasite artışından faydalanabilmekte veya veri analizi işlemlerini tamamen buluta taşıyabilmektedir. "Hizmet olarak analiz" (*analytics as a service*) adı verilen bu model büyük veri işleyen firmalar arasında sıkça tercih edilen bir uygulamadır.[11] ABD Bilişim sektöründeki üst düzey yöneticilerle yapılan bir ankete göre

[10] Ali Sökmen. (2014). "İnternette Yeni Bir Fırsat Şimdi Bulut Bilişime Kafa Yorma Zamanı!" TEPAV Politika Notu. http://www.tepav.org.tr/upload/files/1392643554-3.Internette_Yeni_Bir_Firsat_Simdi_Bulut_Bilisime_Kafa_Yorma_Zamani.pdf.

[11] Intel IT Center. (2013). "Big Data in the Cloud: Converging Technologies". Intel Solution Brief. http://www.intel.com.tr/content/dam/www/public/us/en/documents/product-briefs/big-data-cloud-technologies-brief.pdf.

büyük veri işlemenin operasyonlarında önemli yer tuttuğu şirketlerin yüzde 80'i bulut bilişimin sağladığı analiz hizmetlerine geçiş yapmayı düşünmektedir.[12]

1.2. SEKTÖR UYGULAMALARI

Bilişim teknolojilerinin gelişmesi, pazarlamadan sağlığa, eğitimden imalat sanayine dek pek çok sektörü de pozitif etkileme potansiyeli taşımaktadır. Bu alt bölümde 8 sektör için verinin etkin kullanımı ile verimlilik artışı, ilave katma değer ve kamu faydası arasındaki ilişki örnekler üzerinden incelenmektedir.

Şekil 2: Veri Kullanımın Örnek Faydaları

Sektör	Örnek Fayda
Dijital içerik ve pazarlama	Dijital pazarlama sektörünün büyümesi, sadece ABD'de yıllık 156 milyar dolar gelir ve 657 bin yeni iş sağlıyor
Sağlık	Türkiye'de kişisel sağlık hizmetlerinin devreye girmesi yıllık MR/BT sayısını %25, maliyeti 700-900 milyon dolar düşürüyor
Eğitim	Devletlerin eğitim verisini açmaları durumunda yıllık 0,9-1,2 milyar ilave küresel değer yaratılıyor
Finans	Kredi verisinin aktörler arası paylaşımı, bankaların özel sektöre açtığı kredileri %15-29 artırıyor
Enerji ve altyapı	Veri paylaşımının artması, bilinçli tüketimin önünü açıyor, üretimdeki aksaklıkları engelliyor
E-ticaret	Fiyatların çevrim içi karşılaştırıldığı sitelerin trafiğindeki %1 artış, ortalama fiyatı %1,1 düşürüyor
İmalat Sanayi	Endüstriyel internetin sağlayacağı %0,75 verimlilik artışı, 2030'a dek küresel ekonomiye 15 trilyon dolarlık katkı sağlıyor
Kamu Kesimi	Dünya genelinde açık veri kullanımının yaygınlaşması, 3 trilyon dolarlık ilave katma değer sağlıyor

1.2.1. Sağlık

Bilgi işlem teknolojilerinin sağlık alanındaki kullanımı henüz diğer sektörlerin gerisinde olmakla birlikte, bu alanda ciddi bir potansiyel bulunmaktadır. ABD sağlık sektöründe verinin

[12] GigaSpaces (2013). "Real-Time Stream Processing and Cloud-Based Big Data Increasing in Today's Enterprises". http://d3a0pn6rx5g9yg.cloudfront.net/sites/default/files/product/BigDataSurvey_Report.pdf.

etkin kullanımı, sektöre 300 milyar dolarlık kazanç sağlamaktadır[13]. Mevcut şartlarda bilgi teknolojilerinin sağlık alanındaki ana kullanımı, çoğunlukla, hasta kayıtlarının dijital ortama taşınmasından ibarettir. Dijital ortamda veri saklama hastaneler ve sağlık kurumları için standart bir uygulama olsa da, sektör henüz bilişim ve internet teknolojilerinden yeterince faydalanmamaktadır. Kırsal kesime yönelik sağlık hizmetlerinin çevrimiçi platformlara taşınması, koruyucu hizmetlerin dijital platformlardan sunulması, mobil platformlarda kullanılmaya uygun uygulamaların geliştirilmesi gibi hizmetler, toplumun daha büyük kesiminin kaliteli sağlık hizmetinden faydalanmasının önünü açarak refah artışı sağlayabilir.

Zaman içerisinde sağlık alanında derlenen veri miktarı artmıştır. Örneğin 2005 yılında ABD'de sağlık kuruluşlarının yalnızca yüzde 30'u temel elektronik verileri kayıt altına alırken, 2012'de bu oran doktorlar için yüzde 50'ye ve hastaneler için yüzde 75'e çıkmıştır. Sağlık kuruluşlarının yanı sıra, sigorta şirketlerinin, tıbbi cihaz ve ilaç üreticilerinin, tüketicilerin ve hükümetin sağlık alanına yönelik veri setleri bir arada düşünüldüğünde, veri havuzunun büyüklüğü daha iyi anlaşılabilir. Bu tür bir veri kaynağı daha iyi bir yaşam tarzının teşvik edilmesi, doğru bakım hizmetlerinin planlanması, sağlık hizmetlerinin kalitesinin yükseltilmesi ve doğru değerinin tespit edilmesi, gerekli yeniliklerin yapılması için temel bilgi kaynağıdır.

AB üyesi 12 ülkede kurulan epSOS (Smart Open Services for Avropean Patients) sistemi ile 30 binden fazla sağlık çalışanının aynı ağa bağlanarak, gerekli durumlarda hasta bilgilerini Avrupa'nın başka bölgelerindeki meslektaşları ile paylaşabilmeleri öngörülmektedir. Bu sistemin işlerlik kazanabilmesi içinse pek çok ülkenin işbirliği yapması, altyapılarını uyumlulaştırması ve ortak kuralların belirlenmesi gerekmektedir. Ancak bu sayede verilere üçüncü şahısların erişimi önlenirken, doktorların güvenliğinden emin oldukları verilerle çalışmaları mümkün kılınabilir. Sistemin işlerlik kazanmasının ardından acil servis hizmetleri Avrupa genelinde uyumlulaştırılacak, acil durumlarda hasta bilgilerine erişim kolaylaşacak ve hasta bakım hizmetlerinde topyekûn bir kalite artışı gözlenecektir[14].

Kişiselleştirilmiş sağlık hizmetleri klinik tedavinin kalitesini artırmakta ve sağlık hizmetlerinin maliyetini azaltmaktadır. Davranışsal bilimlerdeki, teknolojideki ve hizmetler sektöründeki gelişmelerin bir yansıması olarak, sağlık hizmetlerinde de genel yaklaşımlardan kişiye özel yaklaşımlara bir geçiş vardır. Bu tür bir yaklaşım hastaların erken tanıya ve

[13] McKinsey Global Institute. (2011). "Big Data: The Next Frontier for Innovation, Competition and Productivity".
[14] epSOS. http://www.epsos.eu/; Erişim Tarihi: 29 Nisan 2014.

tedaviye yönelik bilinç düzeylerini yükseltirken, bir yandan da sağlık sektöründeki maliyetlerin düşmesine katkıda bulunmaktadır[15].

Sağlık alanında başarılı bir veri uygulamasına örnek İngiltere'den gösterilebilir. Ulusal sağlık kurumu National Health Service, 2004 yılından beri hastanelerin ve cerrahların ameliyat sonuç verilerini kamuya açık olarak yayınlamaktadır. Bu sayede sorunlu alanların tespit edilmesi kolaylaşmış, yapılan iyileştirmeler sayesinde kalp ameliyatlarında ölüm oranı yüzde 22 azaltılmıştır.[16]

Özellikle büyük verinin sağlık alanındaki uygulamaları, bilimsel yenilikleri de beraberinde getirmektedir. MIT ve Harvard Üniversiteleri, büyük veriyi insan genetiğini ve genomunu araştırmak için kullanmaktadırlar. Bu sayede insanda hastalık yaratan patojenlerin ve genetik faktörlerin tespit edilmesi mümkün olmuştur. Tıp alanındaki çok sayıda problemi çözmek için ortaya atılan pek çok hipotezden hangisinin doğru olduğunun belirlenebilmesi için, daha büyük denek gruplarına ve veriye ihtiyaç vardır. Bu noktada temel sorun ise, kişilerin veri toplanmasına rıza verme süreçleridir. Veri gizliliğine yönelik kısıtlayıcı düzenlemeler, bu tür bilimsel gelişmenin de önünü tıkamaktadır.

Türkiye'de veri uygulamalarının sağlık sektörüne sağlayacağı faydalar üzerine bir etki analizi bulunmasa da, bu alanda bazı öncü adımlar atılmıştır. Örneğin Sosyal Güvenlik Kurumu, Ulusal Sağlık Bilgi Sistemi (Sağlık.NET) altında sağlık verilerini standardize edip her vatandaş için sağlık verilerini içeren elektronik karne uygulamasına başlamıştır. Bu sayede gelecekte SGK verilerini kullanarak sağlık hizmetlerinin kalitesinin ve şeffaflığının arttırılması ve tasarruf sağlanması mümkündür.

Türkiye'de hastaların sağlık kayıtlarının sahipliğini belirleyen bir hukuki düzenleme bulunmamaktadır. Bu sebeple sadece aile hekimleri hastaların bilgilerine erişebilmekte, hastanın rıza verdiği durumlarda dahi diğer doktorlar kayıtları görememektedir. Kişisel verilerin gizliliğine dair bir hukuki çerçevenin bulunmaması, hasta kayıtlarının yurtiçinde ve yurtdışında paylaşılmasını engellemektedir. Oysa elektronik sağlık kayıtlarının tutulması ve paylaşılması, sağlık hizmetlerinin kalitesini artırıp etkili sunuma imkan tanıyacaktır. Böyle bir uygulama, maliyet düşürücü kişisel hizmetlerin sunumunu da mümkün kılacaktır. Bu

[15] McKinsey Insights&Publications. (2012). "Navigating a Changing Health Care Environment: An Interview with Pfizer's Kristin Peck".

[16] Capgemini Consulting. (2013). "The Open Data Economy: Unlocking Economic Value by Opening Government and Public Data";
http://www.capgemini-consulting.com/resource-file-access/resource/pdf/opendata_pov_6feb.pdf.

uygulama, yatılı gün sayısında yüzde 5 ve MR/BT görüntüleme sayısında yüzde 25 azalma sağlayarak, yıllık 700-900 milyon TL tasarruf sağlama potansiyeli taşımaktadır[17].

1.2.2. Eğitim

Son yıllarda eğitimin dijitalleşmeye başlaması ile zaten yüksek miktarda olan veri üretimi daha da artmıştır. Çevrimiçi öğrenim ve teknoloji temelli eğitim uygulamaları ile birlikte öğrencilerin gelişimini daha iyi analiz edip programlarda öğrenmeyi kolaylaştıracak değişiklikler yapmak mümkün olmuştur. ABD'nin Eğitim Bakanlığı, çevrimiçi eğitim programlarından toplanan verilerin analizini yeni ulusal eğitim teknolojisi planının bir parçası haline getirmiştir. Çevrimiçi ve teknoloji temelli eğitimden elde edilen verilerin özellikle bu uygulamalardan daha fazla faydalanan engelli veya öğrenim bozukluğu olan çocuklara faydası olacağı beklenmektedir.[18]

Eğitim sektörü, kamu sektörünün açık veriyi benimsemesi durumunda en yüksek faydayı sağlayacak sektördür. Dünya çapında eğitimin en büyük sağlayıcısı olan devletlerin bu alandaki verileri kullanıma açması durumunda yıllık 890 ile 1,180 milyon dolar arası fazladan değer yaratılacağı tahmin edilmektedir. Bu rakama eğitimde artan kalitenin ekonominin geneline sağlayacağı faydalar dahil edilmemiştir.[19] Buna ek olarak, okulların ve öğretmenlerin performans verilerinin incelemeye açılması gibi şeffaflığı arttıracak uygulamalar sayesinde eğitim sağlayıcıları arasındaki rekabet artacak, sorunlu alanları tespit etmek kolaylaşacaktır.

Türkiye'de eğitimde veri uygulamalarının yukarıda sayılan faydalara ek olarak FATİH (Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi) projesi sayesinde özellikle büyük bir potansiyeli bulunmaktadır. FATİH projesi kapsamında her sınıfa bir akıllı tahta yerleştirilmekte ve 5.-12. sınıflarda okuyan her öğrenciye birer tablet bilgisayar dağıtılmaktadır. Bu projenin doğru içerik ve uygulama ile yapıldığı takdirde eğitimde kaliteyi önemli ölçüde arttırması beklenmektedir. Veri açısından bakıldığında, tablet bilgisayarlar aracılığıyla öğrencilerin gelişimlerinin izlenmesi, sorun yaşanan alanlara odaklanılması ve bütün tabletlerden toplanan verilerle gerçek zamanlı ve ayrıntılı analizlerin yapılması

[17] TC Kalkınma Bakanlığı. (2013). "Bilgi Toplumu Stratejisinin Yenilenmesi Projesi".
[18] Executive Office of the President. (2014). "Big Data: Seizing Opportunities, Preserving Values"
[19] McKinsey Global Institiute. (2013).

mümkün hale gelmektedir. Proje kapsamında toplanan veriler, eğitim sistemimizin geliştirilmesi, kalite ve eşitliğin arttırılması için büyük bir potansiyel taşımaktadır.[20]

1.2.3. Finans

Finans sektörü İnternet teknolojilerinin kullanıcılar tarafından en yoğun kullanıldığı sektörlerden biridir. Gerek İnternete bağlı bilgisayarlardan, gerekse mobil platformlardan çok çeşitli bankacılık ve finans hizmetlerine erişmek mümkündür. Bankaların ve finans kesiminin müşterilere dair ellerinde bulundurdukları verinin niteliği düşünüldüğünde, güvenlik ve kişisel verilere yönelik tehditlerin bu sektörde diğer sektörlere göre daha büyük risk oluşturduğu söylenebilir.

Finans sektörünün kişisel veri depolamasının hem tüketiciler, hem bankalar, hem de genel ekonomi için faydası büyüktür. Kişisel bilgi dosyaları, kişisel harcamaların izlenmesine ve alışılmadık durumlarda kişilerin aktiviteden haberdar edilmesine imkan tanımaktadır. Örneğin banka kartını daha önce hiç yurt dışında kullanmamış bir kişinin kartıyla yurtdışında harcama yapılması durumunda finans kuruluşunun kart sahibi ile iletişime geçerek harcamayı teyit etmesi, hem güvenlik kaygılarının bir göstergesidir hem de olası dolandırıcılık vakalarının önüne geçilmesi için bir önlemdir.

Bankalar sahip oldukları büyük veri havuzunu kullanarak tüketici eğilimlerini izleyebilmekte, ekonomik sıkıntı dönemlerinde ortaya çıkan dar boğazları önceden kestirebilmekte ve risk yönetimlerini buna göre yapabilmektedirler. Kamunun ise kişi veya firma bazında ve pek çok kaynaktan gelen finansal verileri derlemesi ve saklaması, kredibilitenin hesaplanmasına ve riskli tüketicilerin belirlenmesine imkan tanımaktadır. Tüketiciler herhangi bir kredi işlemi için bankalara başvurduklarında, bankaların bu merkez üzerinden tüketicileri sorgulayabilmeleri, riskli işlemleri azaltmakta ve batık kredi ihtimalini düşürerek ekonominin sağlıklı gidişatını desteklemektedir. Kredi bilgi paylaşım mekanizmasının olduğu ülkelerde, bankaların özel sektöre açtığı kredi yüzde 15-29 arasında artmaktadır[21]. 2013 yılı Haziran ayına dek Türkiye'de kredi ve kredi kartlarına ilişkin limit ve risk bilgileri, protestolu senet ve karşılıksız çekler ile negatif nitelikli ferdi kredi ve kredi kartı borçlularına ilişkin kayıtlar Merkez Bankası tarafından tutulurken, bu tarihten sonra ise sorumluluk Türkiye

[20] Eğitim Reformu Girişimi. (2013). "Fatih Projesi Eğitimde Dönüşüm için bir Fırsat Olabilir Mi?" http://erg.sabanciuniv.edu/sites/erg.sabanciuniv.edu/files/ERG_Fatih%20Projesi.pdf.
[21] Jappelli, T. ve M. Pagano. (2005). "Role and Effects of Credit Information Sharing". *Centre for Studies in Economics and Finance.* Working Paper No: 136.

Bankalar Birliği (TBB) Risk Merkezi'ne geçmiştir. TBB gerçek ve tüzel kişilere ait risk bilgisini toplayarak, üyesi olan kuruluşlar ve müşterileri ile paylaşır. Onay verilmesi durumunda, özel hukuk tüzel kişileri ile de veri paylaşılmaktadır.

Finans ve bankacılık sektörüne mobil cihazlar üzerinden erişim henüz Türkiye için yeni olsa da, hızla gelişen bir alan olarak öne çıkmaktadır. Akıllı telefonların ve tabletlerin yaygınlaşması ile beraber, bankalar bu kanallar üzerinden verdikleri hizmetleri de iş modellerine yerleştirmektedir. Türkiye'de ilk mobil bankacılık uygulaması, 2007 yılında İş Bankası için geliştirilmiştir[22]. Ardından pek çok bankanın benzer uygulamalar geliştirmeleri ile 2013 yılı Aralık ayında Türkiye'de mobil bankacılık uygulamalarını en az bir kez kullanan müşterilerin sayısı 5,3 milyonu ve aktif müşteri sayısı ise 3,2 milyonu geçmiştir. Aralık 2012 ve Aralık 2013 arasında mobil platformlardan yapılan finansal olmayan işlem adedi yüzde 282 artmıştır. Aynı dönemde para transferi işlem hacmi yüzde 147 ve işlem adedi ise yüzde 124 artış göstermiştir[23]. Bu artışa paralel olarak mobil platformlara yönelik güvenlik önlemlerinin artırılması ve finansal verilerin korunması önemlidir.

Bankacılık sektörünün faydalanabileceği bir diğer veri temelli uygulama bulut bilişimdir. Fakat Türkiye'de bulut bilişimin kullanım alanları sınırsız olsa da, mevzuat bankacılık sektörünün bu hizmetten faydalanmasını engeller niteliktedir. Finans sektörüne yönelik çeşitli tebliğ ve yönetmelikler, bankacılık sektöründeki finansal verilerin erişilebilirliğini, güvenliğini ve bütünlüğünü temin etmeye yöneliktir. 2013 yılında kabul edilen, ödeme sistemlerine dair kanunda, sistem işleticisinin, ödeme kuruluşlarının ve elektronik para kuruluşlarının verileri istenildiği an erişime hazır durumda ve yurtiçinde saklamaları gerektiği ifade edilmiştir[24]. BDDK mevzuatı, Türkiye'de faaliyetlerini sürdüren tüm bankaların birincil (verilerin tutulduğunu ana kaynaklar) ve ikincil (bilgi sistemlerinin yedekleri) sistemleri yurtiçinde bulundurmalarını zorunlu tutmaktadır[25]. Mevzuattan doğan sorunlar, bankacılık sistemi gibi bulut bilişim kullanımından büyük fayda elde edecek bir sektörün önünü kapatmaktadır.

[22] http://www.bthaber.com/mobil-uygulamalar-bankalar-icin-zorunluluk-haline-geldi/; Erişim tarihi: 6 Mayıs 2014.
[23] TBB. (2014). Mobil Bankacılık İstatistikleri.
[24] Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, Kanun No: 6493, 2013.
[25] KMPG. (2013). "Bulut Bilişim ve Bankacılık Sektörü". *KPMG Gündem.*

1.2.4. Enerji ve Altyapı

Enerji sektörü, enerji kaynağının bulunmasından kullanımına dek farklı aktörleri içermektedir. Her aşamasında büyük miktarda veri üretilen bu zincirin verimliliğinin artırılması ve tüketicilere yönelik yeni hizmetlerin geliştirilebilmesi için verinin etkin kullanımı gerekmektedir. Enerji sektöründe büyük veri üreten kaynaklar, enerji kaynağını bulan ve enerjiyi kullanım için çıkaran makineler, enerji hattına giden enerjiyi üreten çeşitli santraller ve rüzgar türbinleri ile tüketicilerin tüketim miktarını gösteren akıllı sayaçlardır.

Kişisel verinin enerji sektöründe etkinliğini artırmak için en önemli kullanım alanlarından biri, enerji tasarrufu için akıllı sayaçlardan gelen verinin derlenmesidir. Eski analog sayaçların yerine geçmeye başlayan dijital, akıllı sayaçlar sayesinde hane halklarının ve kurumların enerji tüketim bilgisi anlık olarak merkezlere iletilmekte ve büyük veri birikimi sağlanmaktadır. Bu verinin doğru şekilde kullanılması ve analiz edilmesi, enerji üretim ve dağıtım şirketlerinin enerji kullanım eğilimlerini belirlemelerini, verimsiz enerji kullanımını tespit etmelerini ve gerekli düzeltmeleri yapmalarını, müşteri farklılaştırmasına giderek ve müşterilere verilen hizmeti iyileştirerek müşteri memnuniyetini artırmalarını sağlayabilir.

ABD yönetimi 2012 yılında tüketicilerin enerji harcamalarını görmelerine ve enerji tasarrufu yapmalarına imkan tanıyan *"Green Button"* girişimini devreye sokmuştur. Kamu-özel sektör ortaklığı ile hazırlanan bu program sayesinde tüketiciler harcamalarını görebilecek, ısınma ve soğuma için daha etkin yöntemler seçebilecektir. Benzer şekilde, Türkiye'de de tüketicilerin enerji harcamalarını görme hakları Enerji Verimliliği Kanunu'nun Eğitim ve Bilinçlendirme kısmında güvenceye alınmıştır. Buna göre tüketiciler bir önceki mali yıla ait tüketim miktarı ve bedelini, İnternet ortamında ve aylık bazda görebilirler[26]. Konuyla ilgili yönetmelik ise, kullanıcıların aynı tüketici grubundaki ortalama tüketim değerleri ile karşılaştırmalı şekilde tüketim değerlerini görmelerine yönelik düzenlemeleri kapsamaktadır[27]. Gerekli düzenlemeler yapılmış olmasına karşın, henüz bu konuda işleyen bir sistem bulunmamaktadır.

Veri, enerji üretimi için de önem taşımaktadır. Örneğin büyük bir rüzgar çiftliğindeki rüzgar türbinlerinin her birinden gelen verinin tek tek incelenmesi ve büyük veri seti halinde analiz edilmesi, hangi türbinin ne zaman yenilenmesi veya daha yüksek etkinlik için hangi türbinin hangi şartlar altında kullanılması gerektiğini bulmak için kullanılabilir. Bu sayede, olası

[26] 5627 Sayılı Enerji Verimliliği Kanununun Eğitim ve Bilinçlendirme Kısmı. Madde 6, Fıkra 1, Bent c, No: 2
[27] 27/10/2011 tarihli ve 28097 sayılı Resmi Gazetede yayımlanan Enerji Kaynaklarının ve Enerjinin Kullanımında Verimliliğin Artırılmasına Dair Yönetmelik, 24. Madde (Bilinçlendirme ve Tanıtım Etkinlikleri), Fıkra 2

üretim kesintilerinin önüne geçilebilir. Bu tür üretim kesintileri, bölgenin ekonomik yoğunluğuna göre ciddi ekonomik kayıplara neden olabilir. 2012 yılında yapılan bir çalışma, San Diego bölgesinde 13 saat süren elektrik kesintisinin ekonomide, en iyimser tahminle bile, en az 100 milyon dolarlık kayba sebep olduğu göstermektedir[28]. Üretim aşamasında kullanılan makinelerin ve teçhizatın daha iyi takip edilmesi ve derlenen verinin gerçek zamanlı analizi, bu tür kayıpların oluşma ihtimalini en aza indirebilir.

Türkiye'de enerji sektöründe faaliyet gösteren firmalar, abonelerinin kullandığı sayaçlar üzerinden veri toplasalar da, ülke geneline yayılmış ve enerji sektöründeki tüm verileri bir araya getirecek bir veri projesi yeni hayata geçirilmiştir. 4 Nisan 2014 tarihinde Resmi Gazete'de yayınlanan Enerji ve Tabii Kaynaklar Bakanlığı İstatistik Sistemi Veri Yönetmeliği ile enerji sektöründe faaliyet gösteren pek çok paydaşın, ellerindeki bilgileri gerçek zamanlı olarak Enerji Piyasaları İşletme A.Ş. ile paylaşmaları öngörülmektedir. Paydaşların 1 Ocak 2015'e dek gerekli alt yapıyı kurmalarının ardından, Türkiye enerji sektörüne yönelik tüketim ve arz verilerinin gerçek zamanlı takip edilebilir olması, pek çok hesaplamanın da daha etkin yapılmasının önünü açacaktır. Bu veriler, kişisel tüketim verilerini de içereceğinden, sistemin kuruluş aşamasında veri güvenliği ile ilgili gerekli önlemlerin alınması şarttır.

Büyük veri setleri, doğalgaz ve petrol üretiminin ve tüketiminin iyileştirilmesi için de önemli bir potansiyel sunmaktadır. Üretici firmalardan, hükümetlerden ve tüketicilerden derlenen verilerin etkin analizi, yatırımların optimize edilmesi, faaliyetlerin verimli kılınması ve tüketimin bilinçli olması için gereklidir. Petrol ve petrol ürünleri tüketimine dair kişisel verilerin toplulaştırılması, tüketicilere pek çok fayda sunmaktadır. Örneğin, tüketicilerin her lokasyondaki benzin satış fiyatlarını kaydedebildikleri akıllı telefon uygulamaları, diğer tüketicilerin fiyat karşılaştırması yapmasına ve rekabetin sağlıklı olmasına olanak sağlamaktadır.

Altyapı sektöründe veri analizinin sağlayacağı önemli faydalar bulunmaktadır. Büyük veri uygulamaları sayesinde altyapı hizmetlerinin takip edilip yönetilmesi kolaylaşmakta, tasarruf sağlanabilmektedir. 2012 yılında enerji dışındaki alanlarda altyapı hizmet sağlayıcılarının veri analizi yatırımları dünya çapında 700 milyon dolar seviyesindedir. Bu rakamın 2020 yılına kadar 3,8 milyar dolar seviyesine ulaşması beklenmektedir.[29] Altyapı hizmetlerinde üretim, dağıtım gibi alanlarda üretilen veriler enerji alanında olduğu gibi sensörler yoluyla toplanıp

[28] National System Research Institute for Policy Research. (2012). "Economic Impact of September 9th Power Outage". *Policy Brief.*
[29] GTM Research (2013). "The Soft Grid 2013-2020: Big Data & Utility Analytics for Smart Grid".

temizlendikten sonra algoritmalara göre analiz edilmektedir. Bu analizler sonucunda kayıp ve kaçakların nereden kaynaklandığı tespit edilebilir, talep ve arzdaki değişiklikler önceden öngörülebilir, hile ve dolandırıcılığın önüne geçilebilir. Adaptasyonu henüz başlangıç aşamasında olan altyapı sektöründeki büyük veri analizine örnek olarak Hindistan'ın Bangalore şehrinin su idaresinde kurulmakta olan büyük veri analiz sistemi gösterilebilir.

1.2.5. E-ticaret

İnternet ekonomisinin büyümesinin ana kaynaklarından biri e-ticarettir. BCG tarafından G-20 ülkelerinde yapılan çalışmaya göre, 2016 yılında çevrimiçi perakendenin tüm perakende sektörü içindeki payı gelişmiş ülkelerde yüzde 8,5 ve gelişmekte olan ülkelerde ise yüzde 3,2 olacaktır. G-20 ortalaması ise yüzde 6 olarak öngörülmektedir[30].

İnternet üzerinden ticaret sadece firmalarla tüketiciler arasında değil, tüketicilerle tüketiciler (C2C) ve firmalarla firmalar (B2B) arasında da gerçekleşmektedir. Tüketiciler ve firmalar, aradıkları ürünü lokasyondan bağımsız şekilde inceleyebilmekte, yerel pazarda bulamadıkları ürünlere erişebilmektedirler. Sadece AB'de B2B ve C2C platformları üzerinden bir yılda el değiştiren mal ve hizmet tutarı 8 trilyon doları aşmıştır[31]. Dünya genelinde 2014 yılında B2C platformları üzerinden gerçekleştirilen e-ticaret hacminin yüzde 20 artışla 1,5 trilyon dolara ulaşacağı ve bu artışın gelişmekte olan piyasalardan besleneceği öngörülmektedir. Almanya, Fransa ve İngiltere'de e-Bay'den alışveriş yapan müşteriler, gerçek dükkanlardan alışveriş yapanlara göre yüzde 17 daha düşük fiyat ödemektedirler[32]. Asya-Pasifik bölgesinin, B2C satışlarından 525 milyar dolarlık bir pay alarak ilk kez Kuzey Amerika'yı geçmesi beklenmektedir. İtalya, Almanya, Kanada, Amerika, Fransa gibi gelişmiş ülkelerde B2C pazarının 2014 yılı büyümesinin yüzde 10-15 aralığında kalması beklenirken, Çin'de bu oranın yüzde 64, Endonezya'da yüzde 45 ve Hindistan'da yüzde 32 olması beklenmektedir[33].

İnternetin perakende sektöründe yarattığı değerin bir kısmı, doğrudan alışverişten değil, tüketicilerin ürünleri satın almadan önce İnternet üzerinden yaptıkları araştırmalarından kaynaklanmaktadır. Son dönemde popüler olan İnternet üzerinden araştırıp, fiziksel

[30] BCG. (2012). "The Internet Economy in the G-20".
[31] McKinsey Global Institute. (2011). "Big Data: The Next Frontier for Innovation, Competition and Productivity".
[32] Copenhagen Economics. (2012). "Online Intermediaries".
[33] e-Marketer. (2014). "Global B2C Ecommerce Sales to Hit $1,5 Trillion This Year Driven by Growth in Emerging Markets". http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This-Year-Driven-by-Growth-Emerging-Markets/1010575; Erişim tarihi: 30 Nisan 2014.

dükkanlardan alışveriş yapma konsepti (research online and then purchase online – ROPO) yoluyla yapılan alışverişin küresel boyutta 1,3 trilyon dolara ulaştığı tahmin edilmektedir. ROPO, G-20 ülkelerinde e-ticaretten çok daha büyük bir hacme sahiptir. Örneğin Türkiye'de, 37 milyar dolarlık alışverişin ROPO ile yapıldığı görülürken, perakende e-ticaret 2 milyar dolarda kalmıştır. Bu anlamda, Türkiye diğer G-20 üyesi ülkelerin önündedir[34].

Mobil teknolojilerin gelişmesine paralel olarak, tüketicilerin mobil alışveriş yapmalarına imkan tanıyan platformlar da doğmuştur. Bu tür platformlar, tüketicilerin aradıkları ürünleri, dışarıdayken bile fiyat, kalite ve satıcı açısından karşılaştırabilmelerine imkan tanımakta, GPS verisi üzerinden elde edilen lokasyon bilgilerini kullanarak tüketiciye uygun alışveriş imkanları sunmaktadır. Internet kullanıcılarının yüzde 40'ı, fiyatları çevrimiçi olarak karşılaştırabilecekleri siteleri ziyaret etmektedirler. Bu tür sitelerin trafiğindeki yüzde 1'lik artış, ortalama fiyatın yüzde 1,1 azalmasına neden olmaktadır[35].

E-ticaret platformları, alıcıların platformlara yükledikleri bilgileri ve satın alma tercihlerini inceleyerek, kullanıcılarına özelleşmiş satın alma tercihleri sunabilmektedir. Amazon'un Aralık 2013'te patentini aldığı, "öngörülü teslimat" programı bu yönde atılmış örneklere bir adımdır. Bu uygulama alıcıların geçmişte aldıkları ürünlerin ve satın alma kararını etkileyen diğer faktörlerin incelenmesi üzerine kuruludur. Alıcıların çevrimiçi platformları hangi dönemlerde ne tür ürünleri satın almak için kullandıklarının belirlenmesi sayesinde, Amazon bölgesel depolarına bu alıcıların olası alımları ile uyumlu malları önceden gönderecektir. Bu sayede, bir alıcı ürünü satın almaya karar verdiğinde, en yakındaki depodan ürün çok daha kısa zamanda teslim edilecektir[36]. Alıcılar, bu tür uygulamalar sayesinde, aradıkları ve daha önceki alımları ile uyumlu ürünlere daha kısa zamanda erişebilmekte, zamandan tasarruf edebilmektedir.

Ancak alıcı ve satıcının fiziksel bir ortamda bir araya gelmedikleri çevrimiçi platformlardan yapılan ticarette, kişisel ve finansal bilgilerin paylaşımı için ön koşul güvenliğin sağlanmasıdır. E-ticarete dair riskler belli başlıklar altında toparlanabilir: 1) Firmalar arası işlemlerde güvenliğin nasıl sağlanacağı, 2) İşlemin yapıldığı sitelere yüklenen özel ve finansal verilerin nasıl korunacağı, 3) İşlemlerin geçerliliğinin nasıl sağlanacağı ve cezai yaptırımların nasıl uygulanacağı.

[34] BCG. (2012). "The Internet Economy in the G-20".
[35] Copenhagen Economics. (2012). "Online Intermediaries".
[36] Bensinger, G. (2014). "Amazon Wants to Ship Your Package Before You Buy It". Erişim tarihi: 9 Mayıs 2014.

Firmalar arası işlemlerde güvenliğin sağlanabilmesinin yollarından biri, kullanıcıların güvenli bir merkeze yükledikleri bilgilerle sanal kimlikler oluşturarak, işlem sırasında bu kimlikleri kullanmalarıdır. Bu sayede alıcı ve satıcı arasında doğrudan veri değişimine gerek kalmadan, veriler merkezi kontrol sistemi üzerinden doğrulanabilir ve işlemler sırasında kullanılabilir. E-ticaret sırasında ortaya çıkan ikinci risk, tüketici bilgilerinin işlemin gerçekleştirildiği platform tarafından ne kadar korunabildiği ile ilgilidir. Bu tür hizmetlerin sunulduğu platformların güvenlik altyapısına yönelik çalışmalar yapmaları, doğrulanabilir güvenlik sertifikaları ve uzaktan ödeme sistemleri kullanmaları, tüketiciler açısından güvenliği artırıcı unsurlardır. Finansal bilgilerin alıcıya ulaşmasına gerek bırakmayan PayPal gibi sistemlerin ve bu sistemlerin kullanımının yaygınlaşması, e-ticaretin yaygınlaşması ve hacminin artması için önemlidir.

Gerek işletmelerin, gerekse bireysel tüketicilerin aktif olarak kullandıkları e-ticaret platformlarının ekonomideki artan önemine paralel olarak, kişisel verilerin korunmasının önemi de artmaktadır. Bu sebeple, bir yandan kişisel bilginin güvenliliğini sağlarken, diğer yandan da e-ticaretin kullanımını sekteye uğratmayacak bir hukuki çerçevenin oluşturulması gerekmektedir.

1.2.6. İmalat Sanayi

Gelişen veri depolama ve analiz olanakları, sensör maliyetlerinin düşmesi, ve internet erişiminin artması sayesinde sanayide verinin potansiyelini değerlendirmek için yeni fırsatlar ortaya çıkmıştır. "Endüstriyel İnternet" olarak da adlandırılan bu yeni fenomenin ortaya koyduğu en önemli yenilik akıllı makinelerdir. Sensörler aracılığıyla üretim sürecinin her aşamasını yakından takip eden, internet üzerinden birbirine bağlı akıllı makinelerden gelen veriler, gelişmiş veri analizi uygulamalarıyla anlık olarak işlenebilmektedir. Bu verilerin işlenmesi sayesinde performans, otomasyon ve verimlilik artmaktadır.

Büyük firmalar faaliyet süreçleri boyunca ortaya çıkan büyük veri setlerini, insan kaynakları ve müşteri ilişkileri yönetimi dışında pek çok başka amaç için de kullanmaktadır. Örnek olarak bir jet uçağının motorlarına yerleştirilen sensörler yakıt tüketiminden aşınmaya kadar değişik verileri anlık olarak takip edebilir, bu sayede bakım ve onarımın optimize edilip motor verimliliğinin artmasını sağlayabilir.[37] GE, uçak ve trenlerinden gelen veriler üzerinde

[37] Peter C. Evans & Marco Annunziata. (2012). "Industrial Internet: Pushing the Boundaries of Minds and Machines"

çalışarak büyük maliyet tasarrufu sağlayacak ve makinelerin birbirleri ile iletişim kurmalarına imkan tanıyacak bir endüstriyel İnternet projesi üzerinde çalışmaktadır. GE, bu sistemin havayollarının toplam yakıt maliyetinde yıllık yüzde 1 iyileşmenin 15 yılda 30 milyar dolar kümülatif tasarruf sağlayacağını öngörmektedir. Alitalia Havayolları'nın denediği sistem, uçakların iniş ve kalkışındaki kanat hareketlerini optimize ederek havayolunun 2 yılda 46 milyon dolar tasarruf etmesini sağlamıştır[38].

İmalat sanayi, büyük verinin işlenmesinden olumlu etkilenecektedir. Veriye dayalı uygulamalar sayesinde ürün geliştirme ve montaj maliyetlerinde yüzde 50 düşüş, sermaye ihtiyacında da yüzde 7'lik bir düşüş sağlamak mümkündür.[39] Endüstriyel İnternetin ABD ekonomisine sağlayacağı verimlilik ve üretkenlik artışı yıllık yüzde 1 seviyesinde olduğu takdirde 20 yıl sonra kişi başı gelir seviyesinde yüzde 40'lık fazladan bir artışa sebep olacaktır. Eğer Endüstriyel İnternet dünyanın geri kalanında ortalama yüzde 0,75'lik üretkenlik artışı sağlayabilirse 2030 yılının Dünya ekonomisine fazladan 15 trilyon dolarlık bir katkı sağlayacaktır. Bu, baz senaryonun yüzde 17 üstünde bir gelir seviyesi anlamına gelmektedir.[40]

Makinelerin birbiri ile iletişimine dayanan *"machine to machine (M2M)"*, endüstriyel İnternet kullanımının en iyi örneklerinden biridir. Makinelere ve araçlara takılan sim kartlar sayesinde cihazların birbirleri ile iletişim kurmaları sağlanırken, bu sayede ciddi tasarruf fırsatları da doğmaktadır. Türkiye'deki potansiyelin kullanılabilmesi için Maliye Bakanlığı 2012 yılında M2M hatları için özel iletişim vergisini kaldırmış ve 6 aylık sürede M2M kullanan cihaz sayısı yüzde 81 artmıştır. 2013 yılı itibarıyla Türkiye'de 2,1 milyon makine uzaktan yönetilmektedir. Buna karşılık Türkiye'nin uzaktan yönetilebilir makine potansiyeli ise 150 milyondur[41]. Bu cihazlardan alınan telsiz ruhsat ücretinin de kaldırılması durumunda, kısa sürede M2M abone sayısının 5,4 milyona çıkması beklenmektedir[42].

1.2.7. Kamu Kesimi

Vergi, meteoroloji, trafik, sağlık gibi alanlardaki faaliyetlerinden dolayı kamu sektörü, genellikle bir ülkenin en büyük veri üreticisi, ve dolayısı ile veri uygulamalarından en çok

[38] http://www.fastcompany.com/most-innovative-companies/2014/ge; Erişim tarihi: 1 Mayıs 2014.
[39] McKinsey&Company. (2011). "Big data: The Next Frontier for Innovation, Competition and Productivity"
[40] Peter C. Evans & Marco Annunziata. (2012).
[41] BT Haber, Telekom. (Mart 2013).
[42] http://www.radikal.com.tr/ekonomi/akilli_makinalarla_15_milyar_tasarruf-1188935; Erişim tarihi: 9 Mayıs 2014

fayda yaratabilecek kurumdur. Bu fayda, iki şekilde olabilir. Birincisi, veri analizi uygulamaları yoluyla sağlanacak tasarruf ve kalite iyileşmesidir. Örneğin, kamunun ürettiği büyük veri potansiyelinden tam olarak yararlanılması durunda AB ülkelerindeki kamu sektörü için 250 milyar Avro ek değer ve yüzde 0,5 ek üretkenlik artışı sağlanacaktır. Büyük verinin Amerikan perakende sektöründe kar marjını yüzde 60 arttırabileceği ve yüzde 0,5 – 1 arası üretkenlik artışı sağlayabileceği düşünülmektedir.[43] Bir diğer fayda ise, kamunun elindeki verileri işlenebilir formatlarda açık veri (Open Data) olarak kullanıma sunmasıdır.

Kamunun elinde tuttuğu verileri kamuoyu ile paylaşması, hem firmalar hem de tüketiciler için olumlu etki sağlama potansiyeline sahiptir. Verinin açık hale getirilmesi, verinin fiyatının sıfıra eşitlenmesi ve herkesin kullanımına açılmasıdır. Dünya genelinde açık veri uygulamasının yaygın olarak hayata geçmesi 3 trilyon dolarlık ilave katma değer sağlayabilir.

Bu konudaki en güncel örneklerden biri, Danimarka'da adres sisteminin açık veri haline getirilerek paylaşılmasıdır. Kamu Veri Merkezi'nden adres verisi alan 1200 üyenin faaliyetleri incelenerek yapılan etki analizleri, 2005-2009 döneminde açık adres verisinin toplam 62 milyon avro fayda sağladığını göstermiştir. Buna karşılık hükümet için verileri açık hale getirmenin maliyeti ise sadece 2 milyon avro olmuştur[44]. Kamu verilerinde açık veri prensibini benimseyen ilk Afrika ülkesi olan Kenya, kamu ihalelerindeki fiyat ve teklif verilerini paylaşması sayesinde yıllık 1 milyar dolar tasarruf sağlamıştır.[45]

Hükümetlerin veriyi açarak üstlendikleri maliyet, zaman içerisinde azalan niteliğe sahiptir. İlk etapta verinin paylaşılması için verinin derlenmesine ve anlaşılır şekilde düzenlenmesine yönelik faaliyetler, göreli yüksek maliyete sebep olsa da; zaman içerisinde sistemin sürdürülebilirliğine yönelik katlanılacak maliyetin daha düşük olması beklenir. Nitekim 2010 yılında adres verisini açık tutmanın Danimarka hükümeti için maliyeti 0,2 milyon Avro iken, toplumsal fayda ise 14 milyon Avro olmuştur. Bu faydanın yüzde 30'u kamu kesiminde yaratılırken, yüzde 70'i ise özel kesime yöneliktir.

Yukarıdaki verilen örnekte açık veri kullanımının Danimarka ekonomisi için yarattığı fayda ve maliyet hesaplanırken, sadece doğrudan ölçülebilen veriler göz önüne alınmıştır. Oysa bu veriyi alan ve doğrudan kullanan ekonomik aktörlerin yanı sıra, dağıtım zincirindeki verimlilik artışının zincirdeki diğer aktörleri de etkileyeceği aşikardır. Örneğin, adres

[43] McKinsey&Company. (2011). "Big data: The Next Frontier for Innovation, Competition and Productivity"
[44] Danish Enterprise and Construction Authority. (2010). "The Value of Danish Address Data".
[45] McKinsey Global Institiute. (2013). "Open data: Unlocking innovation and performance with liquid information"

verisinin güncel ve kesin olması sonucu sürüş rotalarının kısalması enerji kullanımını ve çevre kirliliğini azaltarak, toplumsal faydayı artırmaktadır. Bu tür dışsallıklar göz önünde bulundurulduğunda, kamu kesiminin elindeki verileri kullanıcılar ile paylaşmasının, hesaplanandan daha büyük etkiye sahip olacağı söylenebilir.

Kamu sektöründeki verilerin paylaşıma açılmasının faydalananlar kamu ve özel sektör olarak ikiye ayrılabilir. Kamunun sağladığı faydalardan ilki verilerin kullanıma açılması sonucu oluşan iktisadi faaliyetler yoluyla veya verileri işleyen firmalardan alınan vergiler yoluyla sağlanan gelir artışıdır. Örnek olarak, Avrupa Birliği ülkelerinde kamu sektöründe üretilen verilerin açık ve erişilebilir hale getirilmesinin toplam ekonomik faydasının 140 ile 180 milyar Avro arasında olduğu hesaplanmıştır.[46] Mevcut durumda kamuya açık verilerin AB ekonomisine 2010 yılı itibariyle 32 milyar Avro katkı sağlamaktadır. Bu rakam yıllık yüzde 7 gibi yüksek bir hızla büyümekle beraber potansiyelin oldukça altındadır.[47]

Kamunun bir diğer faydası ise şeffaflığın artması ve dolayısıyla hem vatandaşlara sunulan hizmetin kalitesinin yükselmesi, hem de israfın daha kolay tespit edilip engellenmesidir. Örnek olarak Kaliforniya eyaletinde kullanılan ve kurulumu 21 bin dolara mal olan Kamu Şeffaflık Portalı, ziyaretçilerin tespit ettikleri israf kaynaklarının giderilmesi sayesinde 20 milyon dolardan fazla tasarruf sağlamıştır.[48]

Kamu sektöründe toplanan verilerin kullanıma açılmasının bir diğer önemli faydalanıcısı ise özel sektördür. Kamu verilerinin işlenmesine dayalı iş yöntemleri önemli gelir kaynağı oluşturabilmektedir. Örneğin İspanya'da sadece açık veri kullanımına dayalı olarak iş yapan firmalar 2011 yılında toplam 330 ile 550 milyon Avro arasında ciro yapmış, 4 bin kişilik istihdam sağlamıştır.[49] Kamu verilerinin kullanıma açılması bu alanda kurulacak yeni girişimlerin oluşumu açısından faydalı olacaktır. Avrupa Birliği ülkelerinde meteorolojik, coğrafi ve idari kamu verilerinin kullanıma açılması sayesinde özellikle Avusturya ve İspanya'da bu konuda uzmanlaşan firmalar ortaya çıkmıştır. Kamuya açılan verilerdeki artış ile bu sektörde çalışan firmaların ciroları arasında pozitif bir korelasyon bulunmaktadır.[50]

---

[46] Vickery, Graham. (2011). "Review of Recent Studies on PSI Re-use and Related Market Developments" *Information Economics*. http://www.paikkatietoikkuna.fi/c/document_library/get_file?uuid=b1ad5545-266e-4e1b-8970-b855dbcbf997&groupId=108478.

[47] Capgemini Consulting. (2013). "The Open Data Economy: Unlocking Economic Value by Opening Government and Public Data". http://www.capgemini-consulting.com/resource-file-access/resource/pdf/opendata_pov_6feb.pdf.

[48] Frontier Group. (2009). "California Budget Transparency 2.0"

[49] Open Data Portal. (2012). "Characterization Study of the Infomediary Sector" Annual Report.

[50] MICUS. (2009). "Assessment of the Re-use of Public Sector Information".

Şirketler de, hizmetlerini iyileştirmek için başka girişimler tarafından derlenen büyük veri setlerini kullanmaktadırlar. Örneğin, hava durumu bilgisi, kamu kurumları tarafından özel sektörle paylaşılan bir bilgidir. Bu veriyi derleyen ve analiz eden firmalar, yeni iş modellerinin doğmasını sağlayabilir. Dünyanın 3 milyon farklı noktasındaki tüketicinin dijital ve mobil davranışlarını, bu lokasyonlardaki hava durumu ile beraber takip eden Weather Company, bunun bir örneğidir. Firmanın oluşturduğu büyük veri setleri, kozmetik ve sağlık sektöründeki pek çok başka firma için pazarlama stratejisini belirlemek üzere kullanılan ve tüketici faydasını da artıran değerli bir kaynaktır[51].

Türkiye'de Başbakanlık 2011-2015 Stratejik Planı kapsamında şeffaf, hesap verebilir, verimli ve etkili çalışan bir kamu yönetiminin gerçekleştirilmesine öncülük etmek hedefi bulunmaktadır.[52] Açık verinin bu bağlamda önemli bir rolü olacaktır. Türkiye'de açık veriden tam anlamıyla istifade edilebilmesi için gereken yatırımın altyapı hariç 1,6 ile 3,8 milyon TL arası olacağı tahmin edilmektedir. Bu masrafa karşılık kamu verisinin yeniden kullanılmasının ekonomiye toplam 1 ile 7 milyar TL arasında fayda sağlayacağı düşünülmektedir.[53] Açık veriyi hayata geçirmede en önemli kurum olan Türkiye İstatistik Kurumu'nun verileri standardize etmek ve paylaşmak alanında çalışmaları bulunmakla beraber, henüz yurtdışındaki örneklere benzer uygulamalar bulunmamaktadır.

1.3. FAYDA VE MALİYETLER

Bu bölümde kişisel verilerin paylaşımı ve korunmasının büyük ölçekli şirketler, KOBİ'ler, yeni girişim şirketleri ve tüketiciler üzerindeki iktisadi fayda ve maliyetleri tartışılmaktadır. Yapılan fayda ve maliyet analizleriyle, kişisel verilerin korunmasına ilişkin hukuki çerçevenin oluşturulmasına ilişkin bir iktisadi altyapı ortaya konulmaktadır.

Ekonomi teorisinde, ekonomik aktörlerin bir karar sürecine ilişkin bilgi miktarı arttıkça ekonomik etkinliği en üst seviyeye çıkaracak kararlar alacakları öngörülür. Rekabetçi piyasa varsayımı altında, tam bilgi ekonomik etkinliğin ön koşuludur. Örnek olarak, sadece toplu biçimde e-posta adreslerine spam e-posta atan bir pazarlamacı, birçok tüketiciye ilgilenmediği mesajlar gönderirken; önceden paylaşılan kişisel veriye dayanarak her tüketicinin ilgisine

[51] http://www.fastcompany.com/most-innovative-companies/2014/industry/big-data; Erişim tarihi: 1 Mayıs 2014.
[52] T.C. Başbakanlık. (2010). "T.C. Başbakanlık (2011-2015) Stratejik Planı" http://www.basbakanlik.gov.tr/handlers/filehandler.ashx?fileid=5947.
[53] McKinsey. (2013). "Bilgi Toplumu Stratejisinin Yenilenmesi Projesi İhtiyaç Tespiti ve Öneriler Raporu"

göre ilanlar gösteren bir dijital pazarlamacı hem tüketici hem de kendisi açısından faydalı bir bilgilendirme yapabilir[54]. Dolayısıyla, paylaşılan veri miktarı arttıkça ekonomik etkinlik artacaktır.[55] Veri paylaşımına konan engeller iktisadi kaynakların etkin dağılımını engellemektedir[56].

Öte yandan, veriyi paylaşan kişilerle, verinin paylaşıldığı şirketler arasında ekonomik güç açısından bir asimetri bulunabilir. Ayrıca, kişisel verinin bir kez paylaşıldıktan sonra, kişinin kontrolünden çıkarak teorik olarak sonsuz kez paylaşılabilir hale gelmesi, kişilerin veri paylaşmaktan çekinmeyecekleri bir hukuki koruma sisteminin kurulmasını veri paylaşımının sürdürülmesi için gerekli hale getirmektedir. Dengeli ve fayda-maliyet analizlerini gözeten bir hukuki çerçeveden yapılmış kanunlar, kişisel veri paylaşımını da optimal bir seviyeye çıkarabilir. Ayrıca, kanunun uluslararası normlarla uyumlu olduğu durumlarda, yerli şirketlerin yabancı şubeleriyle, yabancı şirketlerin de yerli şubeleriyle veri paylaşımı kolaylaşır.

[54] Varian, H. (1996). "Economic Aspects of Personal Privacy".
[55] Posner, R. (1978). "The Right of Privacy". *Georgia Law Review*. 12(3).
[56] Stigler, G. (1980). "An Introduction to Privacy in Economics and Politics". *Journal of Legal Studies.* 9(4).

Şekil 3: Ekonomik Aktörlerin Veri Paylaşımından Doğan Fayda ve Maliyetleri

Ekonomik Aktör	Fayda	Maliyet
Büyük şirketler	Esneklik ve maliyetlerin düşmesini sağlıyor; verimlilik artışına yol açıyor	Bulut bilişimi kullanmanın sabit organizasyonel maliyeti
KOBİ'ler	Müşteri odaklı iş modelleri yaygınlaşıyor, iş süreçlerinin her bir halkasında verimlilik artıyor, daha etkin karar alınabiliyor	Yasal düzenlemelere uyum maliyeti
Yeni girişimler	Veri derleme, saklama, analiz konularında çalışan yeni girişimler inovatif iş modelleri geliştiriyor	Yasal düzenlemelere uyum maliyeti
Tüketici	Arama ve satın alma işlemlerinde zaman kazanıyor, kişiselleştirilmiş ürün ve hizmetler alıyor	Kişisel verinin yeterince paylaşılmadığı durumlarda tüketiciler gereksiz e-postalara, tanıtımlara ve yüksek maliyetlere maruz kalıyor

1.3.1. Büyük Ölçekli Şirketler

Gerek fiziksel mekanlarda faaliyetlerini yürüten ve faaliyetlerinin bir kısmını İnternet ortamına taşıyan, gerekse de sadece çevrimiçi platformlarda faaliyetlerini sürdüren büyük ölçekli şirketler için bilişim teknolojisinin sunduğu pek çok avantaj vardır. Yapılan akademik çalışmalar, firma büyüklüğü ile İnternet teknolojilerinin benimsenmesi arasında pozitif yönlü bir ilişki olduğunu göstermektedir. Büyük ölçekli şirketler İnternet teknolojilerini kullanma konusunda, KOBİ'lere göre daha başarılıdır[57]. Buna karşın, büyük ölçekli firmaların teknoloji kullanımını ilerleyen süreçlerde iş modellerine yerleştirebilmeleri ve e-iş anlayışını benimsemeleri ise firma içi yapısal dinamiklerin değiştirilmesi ile mümkündür[58].

[57] Del Aguila-Obra, Ana ve Antonio Padilla-Melendez. (2006). "Organizational Factors Affecting Internet Technology Adoption". *Internet Research.*
[58] Zhu, Kevin v.d. (2006). "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on e-Business". *Management Science.* 52(10).

Büyük ölçekli şirketlerin iş hacimleri büyük olduğu için, müşterilerle iletişimde bilişim teknolojisinin kullanılması maliyetleri ciddi ölçüde azaltmaktadır (örneğin müşterilerle posta yerine internet üzerinden iletişim kurarak posta maliyetlerinin azaltılması). Daha büyük bir müşteri havuzuna sahip olan büyük firmaların özellikle müşteri ilişkileri yönetimi alanında veriyi etkin kullanmaları, tüketici eğilimlerini toplulaştırılmış şekilde takip etmelerine, belli tüketim tercihlerine sahip gruplara veya kişilere dönemsel teklifler yapabilmelerine, stoklarını daha iyi yönetebilmelerine ve dağıtım zincirini daha iyi organize etmelerine imkan sağlar. Bu süreçlerde gözlenen verimlilik artışları ise, firmaların maliyetlerini azaltıp karlılıklarını artırmalarına, rekabet gücü kazanmalarına yardım eder.

Operasyonlarla ilgili faaliyetlerin bulut bilişim hizmeti sunan platformlara taşınması (firmanın insan kaynakları, muhasebe, finans ile ilgili kayıtlarının uzak sunuculara yüklenmesi), büyük şirketler için, KOBİ'lere nazaran daha yüksek operasyonel maliyet doğurmaktadır. Örneğin, büyük şirketlerin faaliyetlerini uzaktan erişime açmaları ve prosedürlerin bulut bilişim üzerinden yürütülmesine uygun alt yapıyı kurarak sistemleri entegre etmeleri, KOBİ'lere nazaran daha maliyetlidir. Fakat bu tür bir yaklaşım, çalışanların uzaktan çalışmalarına imkan tanıdığından, zaman ve verimlilik kaybını azaltmaktadır. Coca-Cola, Nike, Avon gibi büyük şirketler bulut bilişim teknolojisini iş yapma biçimlerine entegre etmiş büyük firma örnekleridir[59]. Harcama kalemlerinin niteliğine göre değişen sabit maliyetlere karşılık, büyük şirketlerin orta ve uzun vadede bilişim teknolojisini etkin kullanımının daha yüksek fayda getireceğini söylemek mümkündür.

Binlerce çalışana sahip büyük firmalarda insan kaynakları yönetimi, mikro yönetim ile çözülemeyecek kadar karmaşık bir süreçtir. Büyük firmaların sistemlerinde derledikleri veriler kimi zaman öngörüde bulunmak için yeterli olmamaktadır. Bu amaçla geliştirilen büyük veri uygulamaları çalışanların becerileri, tecrübeleri ve kişilikleri gibi temel bilgileri, petrol fiyatları, işsizlik oranları, sosyal medya kullanımı gibi farklı kaynaklardan derlenen veriler ile birleştirmektedir. Bu sayede hangi tip çalışanın işi bırakma ihtimalinin hangi dönemde arttığı önceden tahmin edilmekte ve firmanın gerekli durumlarda önlem almasının önü açılmaktadır[60].

[59] "Three Benefits of Cloud Computing for Only Big Businesses".
http://www.eustaceconsulting.com/blog/general/three-benefits-of-cloud-computing-for-only-big-businesses/;Erişim tarihi: 1 Mayıs 2014.

[60] http://www.fastcompany.com/most-innovative-companies/2014/industry/big-data; Erişim tarihi: 1 Mayıs 2014.

Büyük şirketlerin internet teknolojilerini benimsemeleri ve iş yapma biçimlerini yeni teknolojiler ışığında güncellemeleri, doğrudan firmayı etkileyen maddi kazançların yanı sıra *network* etkisi üzerinden pozitif dışsallıklar da yaratmaktadır. Bir ülkede teknoloji adaptasyonu konusunda öncü olmaya yetecek finansal kaynaklara sahip büyük şirketlerin İnternet tabanlı teknolojileri kullanmaya başlaması ve daha küçük tedarikçileri de bu teknolojileri kullanmaya teşvik etmesi, küçük firmaların da avantajınadır[61]. Örneğin büyük bir beyaz eşya üreticisi firma, tedarikçileri ve bayileri ile olan ilişkilerini bilgisayar üzerinden devam ettirmeye karar verdiğinde, bu firma ile çalışmaya devam etmek isteyen tedarikçiler ve bayiler de gerekli bilişim alt yapısını oluştururlar. Bu sayede, büyük firmalar aldıkları kararlarla piyasadaki teknolojik dönüşümü de tetikler.

İnternet ve bilişim teknolojileri ile bulut bilişimin kullanımı, büyük şirketlerin de benzer esnekliğe sahip olmasına imkan tanımaktadır[62]. Örneğin, farklı ülkelerde ofisleri olan bir şirket, bu ofislerdeki yöneticiler ile toplantı yapmak istediğinde, hepsini şirket merkezine getirmek yerine, dijital platformları kullanarak çevrimiçi toplantı yapabilmekte ve maliyet avantajı yakalamaktadır.

Verilerin kalitesinin, erişilebilirliğinin ve kullanılabilirliğinin artması, büyük firmalarda çalışanların verimliliğini, yatırımlara geri dönüşü ve şirketlerin kaynak kullanımının verimini de arttırmaktadır (Kutu 5). Fortune 1000'de yer alan firmalarla yapılan bir çalışmaya göre, verinin kullanılabilirliğinin %10 artırılması, yıllık 2,1 trilyon dolarlık gelir artışı sağlamaktadır[63]. Verilerin erişilebilirliğinin yüzde 10 artması ise şirketlere 65 milyon dolar net gelir sağlamaktadır.[64]

Büyük firmaların sistemlerinde tuttukları en önemli veri gruplarından biri de finansal verileridir. Bu veri özel niteliğe haizdir ve suç odaklı üçüncü şahısların hedefinde bulunabilir. Büyük veri kullanımı, dolandırıcılık ve suç unsuru içeren faaliyetlerin tespitini kolaylaştırmaktadır. Verinin klasik yöntemlerle incelenmesi ve manüel metotların kullanılması, suçun tespitini zorlaştırıp süreci uzatırken, finansal hasarın artmasına da sebep olabilir. Bu gibi durumlarda, büyük verinin analiz edilmesi ve firmaya yönelen tehditlerin

[61] Zhu, Kevin v.d. (2003). "Electronic Business Adoption by European Firms: A Cross Country Assessment of the Facilitators and Inhibitors". European Journal of Information Systems. 12.
[62] Widjaya, I. (2011). "Cloud Computing Allows Big Business to be as Nimble as Small Business". *Cloud Business Review.*
[63] Mani, D. vd. (2010). "An Empirical Analysis of the Impact of Information Capabilities Design on Business Process Outsourcing Performance". MIS Quarterly. 34(1).
[64] Barua, A., Mani, D. ve Mukherjee, R. (2011) "Measuring the Business Impacts of Effective Data". University of Texas

tespit edilmesi önemlidir. 2016 yılına dek büyük küresel şirketlerin dörtte birinin, bu amaçla büyük veri kullanımına yöneleceği ve ilk yatırım maliyetlerinin altı ayda geri kazanılacağı öngörülmektedir[65].

Büyük şirketler pek çok farklı ülkede operasyonlar yürütmekte, şirket satın alma yoluyla yeni pazarlara giriş yapmaktadır. Çok sayıda büyük Türk şirketi de, yurtdışındaki firmaları satın alarak benzer genişleme süreçlerinden geçmektedir. Şirketlerin veriyi süreçlerine entegre edebilmeleri ve rekabet gücü kazanmaları için, 1) verinin Türkiye'ye getirilebilmesine imkan tanıyacak, kişisel verilere uluslararası standartlarda koruma sağlayan bir mevzuat, 2) verinin başka ülkelere götürülmesini, özellikle bulut bilişim kullanımını engelleyecek kısıtlamalarının olmaması gerekir. Kurumsal verinin Türkiye'de tutulmasına dair kanuni çerçeve olmayışı, farklı ülkelerde şirket satın alan Türk firmalarını zorlamaktadır. Bu tür bir yaklaşım, insan kaynağı ve operasyonel verinin Türkiye'ye transfer edilmesi için firmaların her ülkedeki kamu otoritesinden izin almasına, uzun bürokratik süreçlerle meşgul olmasına ve yüksek maliyetleri üstlenmesine neden olmaktadır. Kişisel verilerin korunmasına dair kanunun çıkarılmasıyla, Türkiye'nin AB nezdinde veri koruması sağlayan bir ülke (safe habor) olarak kabul görmesi bu maliyetlerin asgariye indirilmesini sağlayacaktır.

1.3.2. KOBİ'ler

Veri işlemeye yönelik yatırım maliyetleri hızla düşmektedir. 1997 yılında bir firmanın İnternet ortamında varlık gösterebilmesi için gereken ön yatırım maliyeti 5 milyon dolar iken, bulut bilişim, sunucu sayısındaki artış ve teknolojinin yaygınlaşması sayesinde günümüzde bu tutar çok daha düşüktür[66]. Veri işleme maliyetlerinin düşmesi, mevcut ve olası müşteriler hakkında bilgi edinme, hedefe yönelik pazarlama faaliyeti yürütme ve müşterilerin kişisel tercihlerine uygun üretim yapma ya da hizmet verme kabiliyetlerinin şirket ölçeklerinden bağımsız olarak artmasını sağlamaktadır.[67]

Şirketlerin tüm kararlarında verinin önemi artmaktadır. Verinin firmalar tarafından kullanılması, karar alma süreçlerine daha fazla bilginin entegre edilmesini, çıktının ve verimliliğin artmasını sağlamaktadır. Veriye dayalı karar alma mekanizmalarını kullanan

[65] http://www.gartner.com/newsroom/id/2663015; Erişim tarihi: 1 Mayıs 2014.
[66] Mettler, A. ve Anthony D. Williams. (2012). "Wired for Growth and Innovation". *Lisbon Council Policy Brief.*
[67] OECD. (2010). "The Economics of Personal Data and the Economics of Privacy". OECD Background Paper.

firmalarda, çıktı ve verimlilik yüzde 5-6 daha yüksektir[68]. Veriyi etkin kullanan firmaların sağladığı avantajlar içerisinde en önemli olanlar, müşterilerle ilişkilerin geliştirilmesi ve iş modelinin müşteri için değer yaratma üzerine kurgulanmasıdır. Büyük müşteri portföyüne sahip firmalar, büyük veri setlerini yeni teknolojileri kullanarak analiz edip, müşteriler için daha iyi fiyatlama stratejileri izleyebilmektedirler. Bu süreçte dijital teknolojilerin kullanımı, firmaların verimliliğini yüzde 5, karlılığını ise yüzde 6 artırmaktadır[69]. Bilişim teknolojilerinin sağladığı katma değerin yüzde 75'i, web-tabanlı teknolojileri kullanan geleneksel firmalar tarafından sağlanmaktadır. Bu firmalar müşteri ilişkileri ve değer yaratımı için veriden faydalanmakta ve bu sayede müşteri erişimini artırmaktadır[70].

Kişisel verilerin paylaşımının kısıtlanmasına yönelik düzenlemeler, KOBİ'lerin üstlenmeleri gereken maliyetleri artıracaktır. Örnek olarak, yeni önerilen ve mevcut duruma göre daha sıkı hükümler içeren AB Regülasyonu, AB'de faaliyet gösteren ortalama bir KOBİ'nin, hangi sektörde faaliyet gösterdiğine bağlı olarak, yeni düzenleme sebebiyle 3000 ile 7200 Avro arasında fazladan maliyete katlanması gerektiğini göstermektedir. Bu tutar, ortalama bir KOBİ'nin bilgi işlem harcamalarının yüzde 16-40'ına denk gelmektedir[71]. Yeni uygulama sadece AB'de faaliyet gösteren firmaları değil, AB'deki yerleşiklerin kişisel verilerini kullanan tüm firmaları etkileyecektir. Dolayısıyla, gerçek etkinin çok daha büyük olacağı tahmin edilmektedir.

[68] Brynjolfsson, E. vd. (2011). "Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?" *Working Paper.*
[69] McAfee, A. ve E. Brynjolfsson. (2012). "Big Data: The Management Revolution". HBR.
[70] McKinsey Global Institute. (2011). "Big Data: The Next Frontier for Innovation, Competition and Productivity".
[71] Christensen, L. vd. (2013). "The Impact of Data Protection Regulation in the EU".

KUTU 5: Verinin Özellikleri

Kalite: Verinin hata oranını, genişliğini, zamanında toplanabilmesini ve anında işlenebilirliğini ifade eder.

Kullanılabilirlik: Verinin sadeliğini, manipüle edilebilirliğini ve tutarlılığını ifade eder.

Akıllılık: Verilerden çıkarılabilecek tavsiyelerin değerini ifade eder.

Erişilebilirlik: Verilere dışarıdan ve uzaktan erişime imkân olmasını ifade eder.

Satış Mobilitesi: Verilerin müşterilerle ilişkilerdeki kullanımını ifade eder.

Kaynak: University of Texas, 2011

1.3.3. Yeni Girişimler

Veri işleme maliyetlerinin düşüşü ve bulut bilişim sayesinde, veriye dayanan yeni girişimler (startup) için piyasaya giriş engelleri de düşmektedir. Bu sayede, veri kullanımını iş modelinin merkezine yerleştiren pek çok yeni girişim İnternet ekonomisinin merkezine oturmuştur. Bu girişimlerin büyük bir kısmı, çevrimiçi aracı olarak hizmet vermekte ve üçüncü şahısların etkileşimine imkan tanıyan çevrimiçi platformları yönetmektedir. Çevrimiçi aracıların arama motoru (Google, Yahoo), sosyal ağlar (Facebook, LinkedIn), e-ticaret platformları (eBay, Amazon) ve bulut bilişim gibi farklı türleri bulunmaktadır. Geçmiş 10 yıllık dönemde sınırlı iletişimden, açık bilgi paylaşımına geçişin yaşanması ile birlikte, çevrimiçi aracıların ekonomik rolü pekişmiş ve sundukları hizmetlerin verimlilik artışları sağladığı gözlenmiştir. Bu tür aracılık faaliyetleri 2009 yılında AB GSYİH'na 350 milyar avro katkı sağlamıştır. Katkının 150 milyar avrosu diğer sektörlerdeki firmaların, 35 milyar avrosu ise çevrimiçi aracıların sunduğu bedelsiz hizmetlerden yararlanan tüketicilerin faydasıdır[72]. Bu aracılar, sadece hizmet sağlayıcı konumunda oldukları için, yeni bir yasal çerçeve çizilirken, platformlarını kullanan üçüncü şahıslar arasındaki anlaşmazlık durumlarında herhangi bir yükümlülük taşımalarının önüne geçilmelidir.

Gerek yeni bir girişim, gerekse de çevrimiçi aracıların en bilinenler örneklerinden biri Facebook'tur. Kurulduğu tarih olan 2004'ten bu yana devamlı büyüyen Facebook, Mart 2014'te aylık 1,28 milyar kullanıcı sayısına ulaşmıştır. Bu büyük kullanıcı havuzu, özellikle

[72] Copehnagen Economics. (2012). "Online Intermediaries".

reklam verenler için önemli bir kaynaktır ve reklam gelirleri şirketin 2011 yılı gelirlerinin yüzde 85'ini oluşturmaktadır. Facebook, elindeki veriden daha çok faydalanabilmek ve veriye dayalı hizmetlerini geliştirebilmek için veri merkezleri kurmaktadır.

Netflix, Spotify gibi dijital içerik sağlayıcıları ile yapılan işbirlikleri, kullanıcıların özelleştirilmiş içerik görmelerine ve beğendikleri içeriği ağlarındaki diğer kullanıcılarla paylaşmalarına izin vermektedir[73]. Netflix 2013'de 7 milyondan fazlası ABD dışındaki 40 ülkede olmak üzere, 29,2 milyon aboneye ulaşmıştır[74]. Yapılan araştırmalar, Netflix'in ABD'deki herhangi bir kablolu yayından daha çok izlendiğine ve yayıncılık endüstrisini değiştirdiğine işaret etmektedir[75].

Müzik piyasasındaki benzer bir dönüşüm de Spotify ile yaşanmıştır. Büyük veriden faydalanarak kullanıcılara yeni bir müzik dinleme deneyimi yaşatan uygulamanın 2013 yılı itibarıyla, 6 milyonu paralı olmak üzere toplam 24 milyon aktif kullanıcısı vardır. Kullanıcı profilleri, kişilerin dinledikleri müzik türleri ve parçalar, kullanıcılara en beğenecekleri müziğin önerilmesi için kullanılmaktadır[76]. Kullanıcıların müzik parçalarını veya albümleri satın almalarına gerek bırakmayan uygulama, herkes için müziğe erişimi kolaylaştırmıştır[77].

2014 yılı başında Facebook tarafından 19 milyar dolara satın alınan Whatsapp, dijital teknolojinin sunduğu imkanlardan faydalanarak, kullanıcılarına dünyanın herhangi bir yerindeki diğer kullanıcı ile bedava mesajlaşma fırsatı tanıyan bir uygulamadır. Kullanıcıların sadece diledikleri kişilerle mesajlaştıkları ve kişisel verilerini üçüncü şahıslarla paylaşmak zorunda kalmadıkları bir iş modeli geliştirmeyi hedefleyen ve en iyi ihtimalle birkaç yüz milyon dolar cirosu bulunan[78] Whatsapp'ın, Türkiye'deki tüm şirketlerden daha yüksek bir değerlemeye ulaşması dikkat çekicidir.

Nest, evlere yönelik termostat ve duman alarmları üreten, tüketici verisini kullanarak bir fark yaratan ve 2014 Ocak ayında Google tarafından 3 milyar dolara satın alınan bir teknoloji girişimidir. Nest'in ürettiği termostatlar yerleştirildikleri mekanı bir hafta gözlemledikten

[73] http://bmimatters.com/2012/04/10/understanding-facebook-business-model/; Erişim tarihi: 9 Mayıs 2014.
[74] http://www.contactmusic.com/article/netflix-introduces-multiple-viewer-profiles_3792936; Erişim tarihi: 14 Mayıs 2014.
[75] http://www.forbes.com/sites/dorothypomerantz/2012/07/03/netflix-has-more-viewers-than-any-cable-network/; Erişim tarihi: 12 Mayıs 2014.
[76] http://www.bigdata-startups.com/BigData-startup/big-data-enabled-spotify-change-music-industry/; Erişim tarihi: 12 Mayıs 2014.
[77] http://www.hypebot.com/hypebot/2012/10/how-spotify-changed-music.html; Erişim tarihi: 12 Mayıs 2014.
[78] Whatsapp, kullanıcılarında ilk sene herhangi bir ücret talep etmemekte, sonraki yıl ise 99 cent ücretle uygulamanın kullanılmasını sağlamaktadır. 400 milyon kullanıcısı olan uygulamanın, her kullanıcı "birinci yıl" eşiğini geçmiş olsa bile elde edebileceği toplam ciro en çok 400 milyon dolardır.

sonra kendi kendilerini programlarlar ve değişen hava koşullarına uygun ayarları yaparlar. Kişisel veriye dayalı bir algoritma ile çalışan bu sistem, tüketici başına ortalama 173 dolarlık enerji tasarrufu sağlamaktadır.

İnternet teknolojilerinin yeni girişimlerde etkin şekilde kullanılması, özellikle süreç inovasyonunu desteklemektedir. Var olan teknolojilerin farklı sektörlerde ve yeni kullanım alanlarına uyarlanarak devreye sokulması, ekonomik verimliliği artırmakta ve yenilikçiliğin iş modellerine eklemlenmesini desteklemektedir. Dolayısıyla kişisel verilerin korunduğu ancak yeni girişimlerin iş modellerini de destekleyen bir hukuki zeminin oluşturulması, ekonominin sağlığı açısından da önemlidir.

Büyük şirketlerin çoğu, şirket içinde inovasyon yapmak için gereken esnekliği yitirmektedir. Yenilik çoğu zaman dışarıdaki daha küçük şirketlerden gelmektedir. Veri alanında da benzer bir fırsat bulunmaktadır. Yeni girişimler veri alanında büyük şirketlere de verimlilik artışı sağlayabilir. Büyük şirketlere ve kamuya ait verilerin yeni girişimlere paylaşılması, inovasyonu tetikleyerek toptan verimlilik artışları sağlayabilir.

1.3.4. Tüketiciler

Tüketicilerin İnternet ekonomisinden faydalanmaları büyük ölçüde kişisel verilerini paylaşmalarına bağlıdır. Bu fayda, birinci olarak, e-posta, sosyal ağlar, mobil mesajlar gibi ücretsiz hizmetler alma şeklinde ortaya çıkabilir. İkinci olarak, Amazon.com'un büyük veri teknolojisine dayanan önerileri gibi, ücretli satılan ürün ve hizmetlere dair kişiselleştirilmiş öneriler almak şeklinde ortaya çıkabilir. Üçüncü olarak, Bölüm 2.1'de anlatıldığı gibi, dijital pazarlama yoluyla piyasadaki ürün ve hizmetler hakkında kişiselleştirilmiş şekilde bilgilendirilme yoluyla ortaya çıkabilir.

Amerikalı tüketiciler üzerinde yapılan araştırmalar, İnternet ekonomisinde ortaya çıkan bu fayda sonucu tüketicilerin günde ortalama 3,75 dakika tasarruf ettiğini göstermektedir. Bu zaman kazancının parasal değeri ise kullanıcı başına 500 dolarlık tüketici faydasına denk gelmektedir[79]. G-20 ekonomilerinde ise, tüketicilerin İnternet kullanımlarından doğan tüketici faydasının ortalama 1,400 dolar civarında olduğu görülmektedir[80].

[79] Varian, H. (2013). http://www.economist.com/blogs/freeexchange/2013/03/technology-1#sthash.ZVvZxtCQ.dpbs; Erişim tarihi: 28 Nisan 2014.
[80] BCG. (2012). "The Internet Economy in the G-20".

Mevcut veriden tam olarak istifade edilmesinin tüketiciler için faydası olacaktır. İktisadi açıdan bakıldığında tüketicilerin, İnternetten sağladıkları faydanın pozitif olduğu görülmektedir. Tüketicinin çeşitli hizmetlerden sağladığı bu faydaya "tüketici fazlası" adı verilir. Küresel boyuttaki GPS verilerinin tam olarak değerlendirilmesi durumunda şirketler için ek 100 milyar dolar ciro, kullanıcılar için ise 700 milyar dolar değerinde tüketici fazlası ortaya çıkacaktır.[81] Medyanın dijital ortama taşınması, tüketici faydasını artıran bir unsurdur. Dijital medya, geleneksel medyaya göre tüketiciler için yüzde 10 daha fazla fayda sağlamaktadır[82]. Avrupa'da dijital medya ile geleneksel medyadan elde edilen tüketici değerinin birbirine yakın olduğu görülmektedir[83]. Bilgisayarların yanı sıra mobil cihazların kullanımının artması, dijital medyanın tüketiciler üzerindeki etkisini ve tüketici faydasını gelecekte de artırmaya devam edecektir.

Artan veri derleme, işleme ve bilgi dosyası oluşturma süreçleri neticesinde, kullanıcılar kişisel verilerin gizliliği konusunda daha duyarlı hale gelmişlerdir. Bir kullanıcının kişisel verilerini başka bir kullanıcı veya firma ile paylaşması, bu kullanıcının karşıdakine açık çek vermesi anlamına gelmektedir. Her ne kadar kullanıcı, veriyi paylaştığı aktörün açıkladığı veri derleme nedenini bilse de, olası diğer amaçları veya veri ile daha sonra yapılacakları her zaman bilmemektedir. Bu tür bir belirsizliğin ve kişilerin dijital ortamda veri paylaşmalarından doğacak olumsuzlukların azaltılması için, verinin ilk paylaşıldığı ekonomik aktörün verinin gizliliği ve korunması konularında belli sorumlulukları olması gerekir. Yasal yükümlülüklerin olmadığı bir durumda, verinin paylaşıldığı aktörün veri gizliliğine yönelik tedbir alması için herhangi bir ekonomik neden oluşmamakta ve veriyi paylaşan kullanıcı, belirsizlikle karşı karşıya kalmaktadır. Dolayısıyla, kişilerin veri gizliliği konusundaki endişelerinin temelinde, sonraki süreçlerin belirsizliği yatmaktadır[84].Verinin paylaşımı konusunda fayda-maliyet analizi yapılması, doğru ve dengeli bir yasal çerçeve çizilmesi için önemlidir. Tüketicilerin bu faydayı elde etmesi, etkin bir koruma rejimine bağlıdır. Tüketicilerin kendilerini güvende hissedecekleri bir çerçevenin olmadığı durumda, kullanıcılar kişisel verilerini paylaşmaktan imtina ederler.

Kişisel verilerin korunması ile ilgili süregiden tartışmalarda, *"opt-in" ve "opt-out"* kalıpları sıklıkla duyulmaktadır. *"Opt-in"*, kullanıcıların kendileriyle ilgili bilginin toplanmasına ve

[81] Ibid.
[82] BCG. (2013). "Follow the Surplus: How U.S. Consumers Value Online Media". Dijital medya 970 dola tüketici faydaı (consumer surplus) sağlarken, geleneksel medya için bu tutar 900 dolardır.
[83] BCG. (2013). "Follow the Surplus: European Consumers Embrace Online Media".
[84] OECD. (2010). "The Economics of Personal Data and the Economics of Privacy". OECD Background Paper.

paylaşılmasına etkin bir şekilde izin vermesidir. Bu uygulamanın geçerli olduğu AB üyesi ülkelerde, bir İnternet sitesi, servis sağlayıcısı veya sosyal platform, herhangi bir internet kullanıcısı hakkında bilgi toplamadan ve bu kişinin dijital aktivitelerini takip etmeden önce mutlaka kullanıcının iznini açık şekilde almalıdır. *"Opt-out"* ise daha çok ABD'de uygulanmaktadır. Bu uygulamada, bir siteye giren her kullanıcının kişisel bilgilerini paylaşmayı kabul ettiği varsayılmakta ve kişisel bilgilerini paylaşmak istemeyen kullanıcıların, ilerleyen süreçte bunu açık ve net bir şekilde ifade etmeleri gerekmektedir[85].

Günümüzde kullanılan web tarayıcılarında varsayılan ayar, *"opt-out"* seçeneğidir. Kullanıcılara tarayıcının kurulumu sırasında *"opt-in"* veya *"opt-out"* seçeneklerinden birini seçme şansı verilmesi, kullanıcıların tercihleri doğrultusunda bir deneyim yaşamalarına izin verecektir[86]. Opt-in ve opt-out seçeneklerinden herhangi birisi, diğerine göre kişisel güvenliği koruma bağlamında üstün değildir. Buna karşılık, "opt-in" seçeneği bilginin serbest akışını engellemekte ve ekonominin tamamı için daha yüksek maliyet doğurmaktadır.

KUTU 6: Dijital Ortamda Farklı İzin Prosedürleri

Opt-in: Kullanıcılar, herhangi bir İnternet sitesine e-posta adreslerini kullanarak üye olduklarında, ancak açık şekilde izin verirlerse bu İnternet sitesinden e-posta alabilirler.

Opt-out: Kullanıcılar, herhangi bir İnternet sitesine e-posta adreslerini kullanarak üye olduklarında, bu İnternet sitesinden e-posta alabilirler ve e-posta almak istemediklerinde bunu şirkete açıkça ifade ederler.

"Opt-in" seçeneğinin bir ülkedeki çevrimiçi faaliyetlerin temeline yerleştirilmesi, pek çok sorunu da beraberinde getirebilir. Yeni pazarlara açılmak ve farklı müşteri grupları için daha iyi pazarlama faaliyetleri tasarlamak isteyen bir şirket, *"opt-out"* seçeneği altında genel müşteri profilleri oluşturabilir ancak *"opt-in"* seçeneği altında her müşteriden tek tek izin alması gerekir. Bu ise, şirket için fazladan maliyet demektir[87]. Örneğin, reklam sektöründe

[85] Johnson, E.J. v.d. (2002). "Defaults, Framing and Privacy: Why Opting In-Opting Out?" *Marketing Letters.*
[86] Isley, S.C. (2013). "Opt-In, Opt-Out; Why Not Forced Choice?" *Rand Blog.*
[87] Cate, F. ve M. Staten. (2001). "Protecting Privacy in the New Millenium: The Fallacy of "Opt-In"."

faaliyet gösteren bir şirketin müşterileri ile iletişime geçmek için tek tek izin alması, etkinliği yüzde 18 azaltmaktadır[88].

Herhangi bir kullanıcının *"opt-in"* seçeneğini tercih etmesi, uzun sözleşmeleri okumak zorunda kalması anlamına gelmektedir. Çoğu kullanıcı çevrimiçi aktivitede bulunmadan önce sözleşmeleri okumamakta ve doğrudan rıza göstermektedir. Yapılan çalışmalar, ABD'deki her İnternet kullanıcısının, dijital ortamda önlerine çıkan sözleşmeleri onaylamadan önce okuması durumunda, yıllık 781 milyar dolarlık ulusal fırsat maliyeti doğacağını ortaya koymaktadır[89]. Ekonomik kaybı en aza indirecek ve kullanıcılara baştan seçim yapma şansı tanıyacak sistemler, kişisel verilerin korunması adına önemli gereklilikler olarak öne çıkmaktadır.

1.4. DEĞERLENDİRME

Kişisel verinin toplanması ile ilgili küresel ölçekte yapılan ve halihazırda tartışılan pek çok düzenleme vardır. Dünya Ekonomik Forumu çok taraflı bir yaklaşımı benimsemiş ve küresel olarak kabul edilebilecek normların belirlenmesine yönelik toplantılar düzenlemiştir (Kutu 7). OECD ve üyesi ülkeler, birbirine geçmiş ağların bulunduğu günümüz dünyasına uygun düzenlemeleri yapmak için harekete geçmişlerdir. Pek çok sivil toplum kuruluşu da, kişisel verilerin gizliliği ve dijital dünya konularına farklı açılardan yaklaşan çalışmalar yürütmektedir. AB yeni bir yönetmelik ile kişisel verilerin korunmasına yönelik daha sıkı tedbirleri hayata geçirmek üzeredir[90].

Veriye dayanan ekonomik fırsatların yakalanması, kişisel verilerin işlenmesini dengeli biçimde düzenleyecek bir hukuki çerçevenin varlığına bağlıdır. Bu çerçeve, verinin faydalı kullanımı ve olası pozitif dışsallıklar ile kişisel bilginin gizliliğini dengelemeli, kişisel verilerin işlenmesinde rıza, kişisel verilerin anonimleştirilmesi gibi hususları bir denge içinde düzenlemelidir[91].

Kişisel veri ekosisteminin karmaşıklığı ve hızla değişmesi, daha esnek bir yasal çerçeveyi de gerekli kılmaktadır. Örnek olarak, Avrupa Birliği'nde geçerli olan yasal çerçevenin temeli

[88] Staten, M. ve F. Cate (2003). "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA". *Duke Law Journal.* 52:745
[89] McDonald, A. ve L. Cranor. (2008). "The Cost of Reading Privacy Policies". *Journal of Law and Policy for Information Society.*
[90] World Economic Forum. (2013). "Unlocking the Value of Personal Data: From Collection to Usage".
[91] Tene, O. ve J. Polonetsky. (2012). "Privacy in the Age of Big Data: A Time for Big Decisions". Stanford Law Review.

verinin belli merkezlerde kilit altında tutulduğu 1970'li yıllara dayanmaktadır. Oysa verinin başka kullanımlarının olabileceği, veri toplama maliyetlerini azaltan yeniliklerin işlenen veri miktarını hızla artıracağı, kişisel verilerin her an derlenmesinin ve izlenmesinin kullanıcıları tedirgin edebileceği, buna karşılık kullanıcının veri derlenen her saniye için izin vermesinin dikkat dağıtıcı ve rahatsızlık verici olabileceği düşünüldüğünde, bu çerçevenin bazı sınırlarının yeniden tartışılmasında fayda bulunmaktadır.

Kişisel verilerin korunmasına ilişkin mevzuatın, derlenen verinin kullanılması ile ortaya çıkacak değeri olası risklerle karşılaştıran bir temele dayanması, makul ve esnek bir yapıda olması gerekmektedir. Kişisel verinin ve gizliliğin korunmasının gerçek maddi değerlerini belirlemek zordur. Bu sebeple, kişisel verilerin nasıl korunacağına dair bir çerçeve çizilirken bilgiyi paylaşmak ve saklamak arasında, hem bilgiyi veren kişi hem de toplumsal açıdan faydayı en üst düzeye çıkaracak bir dengeyi gözetmek gereklidir. Böyle bir hukuki çerçeve, hem tüketicileri hem de firmaları gözetmeli, ekonominin tümünün etkinliğini artırmayı hedeflemelidir.

AB tarafından hayata geçirilmesi önerilen "Genel Veri Koruma Düzenlemesi", ABD'de yerleşik ve veri kullanımı açısından Avrupalı muadillerine göre daha özgür bir ortama sahip olan firmalar tarafından kısıtlayıcı bulunmaktadır. Veri transferinin kısıtlanmasının, AB hizmet ihracatında yüzde 6,7 ve milli gelirde yüzde 0,8 ile yüzde 1,3 arasında bir daralmaya yol açacağı öngörülmektedir. Çalışmalar, bu kısıtlamaların AB'deki girişimleri zorlayacağını ve ABD kaynaklı yatırım sermayesinin AB'de İnternet girişimlerini desteklemekten uzak durabileceğini göstermektedir. Özellikle yeni tasarının anlaşılmaz olması ve sektörde çalışanlar tarafından dahi tam olarak anlaşılamaması, yatırımcıların yeni girişimlerden uzak durmalarına neden olacak bir faktör olarak öne çıkmaktadır[92]. Dijital girişimciliğin artması ve bu alanda daha çok yatırımın yapılması, hukuki çerçevenin ne derece açık ve kısıtlayıcılıktan uzak olduğu ile alakalıdır. Yasal mevzuatın hazırlanması sırasında, yatırımları artırıcı bir yaklaşımın benimsenmesi, bu alandan doğan ve ekonominin diğer sektörlerine de yayılan yenilikçi fikirlerin gelişimi için önemlidir.

Bir yandan kişisel verilerin korunmasını sağlayan, diğer yandan da toplam ekonomik faydayı artıran bir hukuki çerçevenin tartışılabilmesi için özellikle üzerinde durulması gereken üç husus mevcuttur: Kişilerin çevrimiçi platformlarda verilerini nasıl paylaşacaklarına dair

[92] Erixon, F. Vd. (2013). "EU Policies on Online Entrepreneurship: Conversations with U.S. Venture Capitalists". ECIPE.

tartışmanın temelinde, kullanıcı rızası yatmaktadır. Kullanıcıların rıza vermedikleri veya uygun görmedikleri durumlarda, çevrimiçi platformlar tarafından kendileri ile ilgili bilgi derlenmesinin önüne nasıl geçileceğini belirlemek için, "opt-in" ve "opt-out" seçeneklerinin ekonomik, hukuki ve sosyal açıdan değerlendirilmesi gerekir. Diğer yandan büyük verinin hayatın her alanına girmesi, verinin kimliğinden ayrılmasını (anonimleştirmeyi) güçleştirmektedir. Dolayısıyla, verilerin ne şekilde saklanacağı ve miadı dolan verilerin silinmesi ile ilgili hususlar anonimleştirmenin önüne geçmektedir.

En sık tartışılan konulardan biri, her tür teknoloji firmasının veri derlemeden önce tek tek kullanıcılardan izin almasının (*opt-in*) mı, yoksa her kullanıcının kendisine dair veri toplanmaması için firmayı açık şekilde bilgilendirmesinin (*opt-out*) mi daha etkin bir çözüm olduğudur. Günümüz koşullarında bilgi ekonominin bel kemiğidir. Tüketicilerden firmalara, yeni girişimlerden hükümetlere dek pek çok ekonomik aktör, daha iyi kararlar vermek ve ekonomik faydayı artırmak için veri kullanmaktadır. Bu çağda yenilik, verimlilik, etkinlik ve büyüme veriye dayalı gerçekleşmektedir. Veri analizinden elde edilen faydanın kişisel verilerin gizliliğine dair risklerden daha büyük olduğu durumlarda, *opt-in* seçeneği toplam ekonomik faydayı azaltabilir. Mutlak rızaya dayanan bir yaklaşım, verinin büyük ekonomik değeri karşısında gereğinden fazla katı kalabilir.

Büyük veri teknolojisindeki gelişmelerle, kişisel olan ve olmayan veri arasındaki ayrım son dönemde silikleşmeye başlamıştır. Önceki dönemlerde bir kişinin İnternet'te yaptığı aramalar, doğrudan kişinin kimliği ile ilişkilendirilemezken; yakın dönemli gelişmeler ise bu tip bağlantılara izin vermektedir. Milyonlarca sensörden her an ve herkes hakkında toplanan veri, bilginin derlenmesine getirilmek istenen kısıtların etkisini azaltmaktadır. Veri kaynağı ister analog, ister dijital olsun, derlenen veriler daha önce düşünülmeyen şekillerde bir araya getirilmekte ve ilk toplama amacının ötesinde amaçlar için kullanılabilmektedir. Ortaya çıkan bu potansiyel, kurumları daha çok veri toplamaya teşvik etmektedir. Derlenen veriyi kimlikten ayrıştırıp saklamaya yönelik teknolojiler gelişse de, görünürde anonim olan veri setlerine yeniden kimlik kazandırmaya yönelik teknolojiler daha hızlı gelişmektedir[93]. Dolayısıyla, hangi verinin kişisel veri olarak kabul edilip korunacağını belirlemek gittikçe zorlaşmaktadır.

[93] Executive Office of the President of the USA. (2014). "Big Data: Seizing Opportunities, Preserving Values".

Ülkemizde kişisel verilerin korunmasına ilişkin kanuni çerçevenin bulunmaması şirketlerimizin uluslararası faaliyetlerini de zorlaştırmaktadır. Mevcut koşullar altında, yurtdışındaki firmaları satın alan ve yurtdışında operasyon yürüten Türk şirketleri, Türkiye'de veri gizliliğine dair hukuki bir çerçeve olmadığı için, çalışanlara ve müşterilere dair kişisel verileri Türkiye'ye transfer ederken güçlük çekmektedir. Birçok durumda, bu işlemler için her ülkeden tek tek izin alınması gerekmektedir. Bu, hem zaman hem de para açısından yüksek bir maliyet anlamına gelmektedir. Her ne kadar ticaretinde en büyük ortağı AB olan Türkiye'nin AB'deki tasarının getirdiği koşullardan etkilenmemesi için, AB tasarısı ile uyumlu bir çerçeve çizmesi gerekse de, sermaye akımlarının serbest olduğu günümüz ekonomisinde yatırımcıları ülkeye ve İnternet yatırımlarına destek vermeye çekmenin ön koşulu anlaşılır, şeffaf ve iş yapmayı kolaylaştırıcı bir hukuki çerçeveye sahip olmaktır.

Yukarıda yapılan tartışmalar ışığında, kullanıcıları her tür riskten korumaya çalışan kısıtlayıcı bir mevzuat yerine, riskleri belirleyen ve belirlenmiş sınırlar içerisinde kullanıcıların İnternet kullanımından aldıkları faydayı artıran bir mevzuat çerçevesi kurulması esastır. Mevzuat çerçevesi geliştirilirken, bir yandan veri süjelerinin korunmasını sağlayıp, bir yandan da veriye sahip olanların toplulaştırılmış ve anonimleşmiş veri ile çalışmalarına fırsat veren mahremiyeti artırıcı teknolojiler (Kutu 8) de dikkate alınmalıdır. Başka bir ifadeyle, mahremiyeti artırıcı teknolojilerin, mevzuatta bugün yapılacak tanımları geçersiz hale getirmesinin önüne geçmek için mevzuat esnek bir yaklaşımla hazırlanmalıdır. Mevzuat, hızla değişen yapıya ayak uydurabilmelidir.

Veri işlenmesine ilişkin teknolojilerin hızlı gelişimi, temelinde verinin yer aldığı İnternet'in hayatımızın merkezine yerleşmesi, kişisel verilerin korunmasına ilişkin hukuki çerçevenin hem önemini artırmakta, hem de ekonominin tüm aktörlerini dikkate alan dengeli bir yaklaşımla oluşturulmasını zorunlu kılmaktadır. Ülkemizde de kişisel verilerin korunmasına dair kanunun, gelişen teknolojilerin sağladığı ekonomik fırsatları kısıtlamayacak ve inovasyonun önünü açacak sade bir çerçeve kanun niteliğinde bir an önce kanunlaştırılmasında fayda bulunmaktadır.

KUTU 7: Dünya Ekonomik Forumu'nun Kişisel Verilerin Korunmasına İlişkin Diyalog Süreci Sonuçları

Dünya Ekonomik Forumu'nun (WEF), gelişen teknolojiler ışığında kişisel verilerin korunmasına ilişkin olarak özel sektör, kamu ve akademi dünyasının liderleriyle yürüttüğü diyalog sürecinin sonucunda, veri ekosisteminin düzenlenmesine ilişkin olarak aşağıdaki üç unsur öne çıkmıştır[94]

Şeffaflıktan karşılıklı anlayışa geçiş: Şeffaflığın artırılması ve kullanıcıların neye izin verdiklerini görmeleri için, pek çok uygulama ve İnternet sitesinde uzun yasal anlaşmalar yayınlanmaktadır. Ancak kullanıcıların büyük kısmı, karşılarına gelen bu anlaşmaları okumamakta ve anlaşmaları incelemeyi zaman kaybı olarak görmektedir. İnternetin kişisel hayatlarla böylesine entegre olduğu bir dönemde, İnternette atılan her adımın izne tabi olması ve her adım için yasal anlaşmaların kullanıcıların önüne çıkarılması, çözüm olmaktan uzaktır.

Pasif izinden aktif kullanıcıya geçiş: Geçmiş dönemde İnternet kullanıcıları, müşteri ilişkileri yönetimi için takip edilen birer sübje iken, kendilerinden toplanan verinin ne şekilde kullanılacağına izin verdikleri çevrimiçi sözleşmeler ile karşılaşmaktaydılar. Günümüzde ise verinin çok farklı şekillerde toplanıp işlenmesi, kullanıcıların her adımda izin prosedürleri ile karşılaşmalarını imkansız kılmıştır. Dolayısıyla, kullanıcıların "evet/hayır" temelli sözleşmeler yerine, izin sürecinde daha etkin bir seçim ve kontrol mekanizması ile muhatap kılınmaları gerekmektedir.

Siyah beyazdan griye geçiş: Verinin derlenmesi ve farklı aktörler tarafından kullanılmasından doğan kavramsal karmaşık sistemin doğurduğu iki temel zorluk vardır. Birincisi, her faaliyet için sınır belirlemeye yönelik keskin ayrımlardan kaçınılması gerekmektedir. Bu tür bir yaklaşım, kimi uygulama için hayır, kimisi için de aynı bağlamda evet cevabı verecek bir kullanıcının tüm uygulamalar için evet ya da hayır cevabı vermesini gerektirir ve kullanıcıya seçim şansı bırakmaz. İkincisi, yasal çerçevenin kişilerin aktivitelerini değil, toplanan verinin kullanımını düzenlemesi gerekir.

[94] World Economic Forum (2013). Unlocking the Value of Personal Data.

2. HUKUKİ ANALİZ

Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı'nın endüstri ve bireyin haklarını da gözetecek bir yapı içerisinde yasalaşmasının paydaşlara ve ekonomimize kazandıracaklarının analiz edildiği ilk bölümden sonra; Raporumuzun bu bölümünde ise; Tasarı'da yer alan başlıca hükümlerin hukuksal olarak analiz edilmesi ve değerlendirmelerimize yer vereceğiz. Bu başlıkta; veri korumasına ilişkin AB'deki normatif düzenlemeler, AB ilerleme raporları kapsamında durum, pozitif hukukumuzdaki düzenlemeler ve Yargıtay kararları ile Tasarı'daki bilgi toplumu, veri odaklı inovasyon ve ağ ekonomisi açısından önemli gördüğümüz hükümlere ilişkin önerilerimiz yer almaktadır.

2.1. TÜRKİYE'DE VERİ KORUMASI HUKUKİ DÜZENLEMESİNİN AB UYUM SÜRECİ AÇISINDAN DEĞERLENDİRİLMESİ

2.1.1. AB'de Kişisel Veri Korumasının Tarihi

Kişisel veri koruması, AB'de uzun yıllardır önemli ve temel bir konu durumunda yer almaktadır. Kişinin özel yaşamının korunması, bir uluslararası anlaşmada ilk kez 1948 yılında İnsan Hakları Evrensel Beyannamesinde düzenlenmiştir. Beyannamenin 12. maddesi, *"hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır"* hükmü getirmektedir. Bundan sadece 2 yıl sonra, 1950 yılında, Avrupa Konseyi, Avrupa İnsan Hakları Sözleşmesini hazırlamış, sözleşme 4 Kasım 1950'de Roma'da imzalanmış ve 3 Eylül 1953'te yürürlüğe girmiştir. Türkiye de 1954 yılında sözleşmeyi onaylamıştır. Sözleşmenin 8. maddesi, aşağıdaki hükmü getirmektedir;

> *"1.Herkes, özel yaşamına ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.*
>
> *2. Bu hakkın kullanılmasına bir kamu makamı tarafından, ulusal güvenliğin, kamu emniyetinin ya da ülkenin ekonomik refahının yararı, suçun ya da düzensizliğin önlenmesi, sağlığın ya da ahlakın korunması için, yahut başkalarının haklarının ve özgürlüklerinin korunması için, hukuka uygun olarak yapılan ve bir demokratik toplumda gerekli bulunanlar hariç, hiçbir müdahale olmayacaktır."*

Türkiye hem İnsan Hakları Evrensel Beyannamesi hem de Avrupa İnsan Hakları Sözleşmesini imzalamış bir ülke olarak bu sözleşmeler ile bağlı konumdadır.

Avrupa İnsan Hakları Sözleşmesinin 8. maddesine dayanarak, Avrupa Konseyi 1960'lardan itibaren, bilgi teknolojileri alanındaki gelişmeler sonucunda, kişisel verilerin korunması alanında çeşitli metinler kabul etmiştir. Bunlardan en önemlilerinden biri, 1981 yılında hazırlanan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmedir. Türkiye sözleşmeyi imzalamasına karşın hala onay sürecini işletmemiştir.Bu duruma Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun, *"Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları"* raporunda da yer verilmiştir.[95] Günümüzde bütün AB üyesi ülkeler sözleşmeyi imzalamış ve onaylamış durumdadır.

Avrupa Konseyinin dışında, Avrupa Birliğinde, 95/46/EC sayılı ve 24 Ekim 1995 tarihli Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Direktif kabul edilmiş ve üye ülkeler tarafından iç hukuklarına geçirilmiştir. Direktifin amacı, üye ülkeler arasında veri koruması alanında bir birlik yaratılmasıdır. Ancak veri korumasını oldukça sıkı bir şekilde korumayı amaçlayan AB, üye ülkelerin, Direktiften önce sahip oldukları veri koruma rejimi Direktiften daha yüksek bir koruma sağlıyorsa, bu korumayı devem ettirme hakkını da ülkelere sağlamıştır.[96] Veri Koruması Direktifinin uygulama alanı, Avrupa Ekonomik Topluluğu Sözleşmesi uyarınca, AB üyesi ülkelerin yanı sıra, Avrupa Ekonomik Topluluğu üyesi olan İzlanda, Lihtenştayn ve Norveç'i de içerisine almaktadır.[97]

2012 yılında, Avrupa Komisyonu, veri koruması alanında büyük bir reform önerisi açıklamıştır.[98] Reform ile AB çağında yeni bir Genel Veri Koruması Regülasyonu hazırlanması öngörülmektedir. Regülasyon ile mevcut 95/46/EC sayılı Direktif ortadan kaldırılacaktır. Her ne kadar Veri Koruması Direktifi ülkelere sınırlı alanlarda değişiklik

---

[95] T.C. Cumhurbaşkanlığı Devlet Denetleme Kurumu, *"Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları", s.780.*

[96] 95/46/EC sayılı Direktif, Beyan 10 şu şekildedir: *"Kişisel verilerin işlenmesi hakkındaki ulusal kanunların amacı, başta kişisel mahremiyet hakkı olmak üzere, hem Topluluk kanununun genel esaslarında, hem de İnsan Hakları ve Temel Özgürlüklerini Koruma hakkındaki Avrupa Sözleşmesinin 8. maddesinde tanınan temel hakları ve özgürlükleri korumaktır; bu nedenle, bu kanunların yakınlaştırılması, sağladıkları korumanın azalmasına yol açmamalı aksine, Topluluk içinde yüksek seviyeli bir korumanın sağlanması için çabalamalıdır."*

[97] Agreement on the European Economic Area, Official Journal L 1 of 3.1.1994

[98] Daha fazla bilgi için, bkz:
http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (İngilizce).

yaparak iç hukuka uygulama hakkı tanısa da, Direktifler ülkeler tarafından iç hukuklarına geçirilirken ortaya farklı uygulamalar çıkabilmektedir. Bu farklılığın da ortadan kaldırılabilmesi için, yeni düzenlemenin bir Direktif değil bir Regülasyon olması öngörülmüştür. Bu şekilde, Regülasyon, ülkelerin iç hukuklarında doğrudan etki doğuracak, her bir ülkenin konuyu iç hukuka aktarmak için kanun çıkarmasına gerek olmayacak ve bu şekilde ülkeler arasındaki veri koruması kanunlarında farklılık ortaya çıkmayacaktır.

AB'de oldukça sıkı bir şekilde korunan kişisel verinin, yeni Regülasyon ile teknoloji ve iletişim sektörünü olumsuz yönde etkileyecek şekilde korumanın artırılmasından çekilen çeşitli kuruluşlar, yeni Regülasyon için bazı öneriler getirmiştir.[99] Bunlar arasında şunlar sayılabilir;

- Takma adlı (pseudonymous) verinin açık bir şekilde tanımlanması,
- Kişisel verinin korunmasında profilleştirme uygulamaları yerine kişiselleştirme uygulamalarına yoğunlaşılması,
- Kişisel verinin işlenmesi için kişilerden rıza alınması durumunun gelişen teknolojiler göz önüne alınarak düzenlenmesi,
- Bulut hizmet sağlayıcıları için açık ve net tanımlar ve yükümlülükler ortaya konması,
- Aracı kurumların sorumluluklarının sınırlı şekilde düzenlenmesi,
- Teknolojiden bağımsız bir düzenleme öngörülerek belirli sektörler, teknolojiler ve hizmetler için fazladan veri koruma sorumlulukları getirilmemesi,
- Uluslararası veri transferi süreçlerinin basitleştirilmesi,
- Unutulma hakkı ve profilleştirme ile ilgili hükümlerin günümüz şartları ile uyumlu bir şekilde düzenlenmesi,
- Regülasyonun kişisel verilerin korunması ve sektörde yenilikçiliğin önünü açmada uygun bir denge yakalaması.

[99] Industry Coalition for Data Protection, "Paper on Proposals for a 'New EU Legal Framework on Data Protection'; American Chamber of Commerce to the European Union, "AmCham EU position on the General Data Protection Regulation"; Center for Democracy & Technology, "CDT Analysis of the Proposed Data Protection Regulation".

2.1.2. AB İlerleme Raporları Çerçevesinde Değerlendirme

AB 2013 yılı ilerleme raporunda, Türkiye'de veri koruması ile ilgili bir çerçeve kanun bulunmaması eleştirilmiş ve bunun çeşitli alanlarda AB ile Türkiye arasındaki işbirliğini engellediğine değinilmiştir. Örnek olarak, bilgi toplumu hizmetleri ile ilgili olarak, Türkiye'de Siber Güvenlik Kurulunun kurulduğuna ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hazırlandığına değinilmiş, ancak e-ticaret ve kişisel veri koruması alanındaki kanunların çıkarılmaması ve Türkiye'nin *"Şartlı Erişime Dayalı Hizmetlerin Yasal Olarak Korunmasına ilişkin Avrupa Sözleşmesi"*ne taraf olmaması eleştirilmiştir.[100] Bunun dışında, polis işbirliği ve örgütlü suçlarla mücadele konusunda, Türkiye'de kişisel verilerin korunmasına ilişkin mevzuatın olmamasının Europol ile operasyonel işbirliği anlaşması imzalanamamasına yol açtığı belirtilmektedir.[101] Raporda aynı konuya terörle mücadele konusunda da değinilmiş, *"kişisel verilerin korunmasına ilişkin bir kanunun bulunmaması ve Türkiye ile AB ve AB'ye üye ülkeler terörizmin tanımını ve yaptırımlarını belirleyen normlar arasında farklılık olduğu dikkate alındığında, bu konuda AB'ye üye ülkeler ve AB kurumları ile olan polis ve adli işbirliği sınırlı"* olduğu belirtilmiştir. [102]

Avrupa Komisyonu, kişisel verilerin korunması konusunu, Türkiye'nin AB süreci için önemli bir konu olarak görmektedir. İlerleme raporunda da belirtildiği gibi, *"kişisel verilerin korunmasına ilişkin olarak, belirgin bir ilerleme sağlanmamıştır. Türkiye'nin kişisel verilerin korunmasına ilişkin genel bir kanunu kabul etmesi ve bu bağlamda tamamen bağımsız bir veri koruma otoritesinin kurulması gerekmektedir."*[103]

[100] Avrupa Komisyonu, Türkiye 2013 Yılı İlerleme Raporu, s.32; http://www.abgs.gov.tr/files/strateji/2013_ilerleme_raporu_tr.pdf.
[101] Avrupa Komisyonu, Türkiye 2013 Yılı İlerleme Raporu, ss.67, 68; http://www.abgs.gov.tr/files/strateji/2013_ilerleme_raporu_tr.pdf
[102] Avrupa Komisyonu, Türkiye 2013 Yılı İlerleme Raporu, s.68; http://www.abgs.gov.tr/files/strateji/2013_ilerleme_raporu_tr.pdf.
[103] Avrupa Komisyonu, Türkiye 2013 Yılı İlerleme Raporu, s.64; http://www.abgs.gov.tr/files/strateji/2013_ilerleme_raporu_tr.pdf.

2.2. TÜRKİYE'DE VERİ KORUMASI HUKUKİ DÜZENLEMESİNİN POZİTİF HUKUKUMUZ AÇISINDAN DEĞERLENDİRİLMESİ

Türk Hukukunda hâlihazırda, kişisel verilere ve bu verilerin korumasına ilişkin çerçeve bir kanun bulunmamaktadır. Kişisel verilere ilişkin düzenlemelerin belirli bir çatı altında toplanmamasından doğan eksiklik ise, kişisel verilere ilişkin hususları barındıran ilgili kanunlar çerçevesinde düzenlenerek giderilmeye çalışılmıştır. Aşağıda pozitif hukukumuzda yer alan bu düzenlemeler yer almaktadır:

2.2.1. Kişisel Verilerin Korunmasına İlişkin Türk Hukukundaki Mevcut Düzenlemeler

a) Türkiye Cumhuriyeti Anayasası

Anayasa'nın 20. maddesinin 3. fıkrası şu şekildedir;

> *"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."* Madde ile kişilere kendileriyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme dâhil olmak üzere kişisel verilerin korunması anayasal hak olarak tanınmaktadır. Madde ayrıca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğini belirtmektedir. Ancak bunun yanında kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği de belirtilmiştir. Bahsedilen anayasal hüküm her ne kadar bu konudaki esas ve usullerin kanunla düzenleneceğini vurgulasa da, ülkemizde kişisel verilerin korunması konusuna özgülenmiş çerçeve bir düzenleme henüz bulunmamaktadır.

b) Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanunu'nun ("TCK") 135 ve devamı maddelerine göre, kişisel verilerin hukuka aykırı olarak; elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır.

TCK'nin "kişisel verilerin kaydedilmesi" başlıklı 135. maddesi kişisel verilerin ve hassas kişisel verilerin hukuka aykırı kaydedilmesini suç saymıştır. Maddeye göre;

> *"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*
>
> *(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."*

Bu maddenin devamı olan 136. madde de, kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve yayılmasını aşağıdaki şekilde suç saymıştır;

> *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."*

TCK, aynı zamanda, kişisel verilerin bu şekilde hukuka aykırı olarak kaydedilmesi, verilmesi, yayılması, ele geçirilmesi fiillerinin kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ve belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hallerini nitelikli hal olarak saymış ve bu durumlarda verilecek cezanın yarı oranında artırılacağını düzenlemiştir.

TCK, aynı zamanda silinmesi gereken kişisel verilerin silinmemesini de suç saymış ve 138. madde *ile "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir"* hükmü getirmiştir.

Tasarının kanunlaşmasıyla, ülkemizde gerek kamu gerek özel sektörde kişisel verilerin korunması ile ilgili farkındalığın artacağı şüphesizdir. Gerçekten de, Tasarı henüz kanunlaşmamasına rağmen, Tasarı ile ilgili tartışmaların kamuoyuna yansıması sonucu, kişisel verilerin korunmasına ilişkin farkındalıkta bir artış gözlemlenmektedir. Adalet Bakanlığının sağladığı bilgilere göre, TCK'nın kişisel verilerin hukuka aykırı kaydedilmesini düzenleyen 135. maddesi ve kişisel verilerin hukuka aykırı olarak verilmesi veya ele

geçirilmesini düzenleyen 136. maddesi kapsamında açılan dava sayılarında son yıllarda bir artış gözlemlenmektedir. Adalet Bakanlığının sağladığı bilgilere göre, 2011-2013 yılları arasında TCK'nın 135. ve 136. maddeleri ile ilgili olarak açılan dava sayısı şu şekildedir;[104]

Kanun Maddesi	2011 Yılı Açılan Dava Sayısı	2012 Yılı Açılan Dava Sayısı	2013 Yılı Açılan Dava Sayısı
135	198	259	236
136	737	1009	1048

Tasarının kanunlaşması ile, yalnızca Tasarıdaki hükümler hayatımıza girmeyecek, TCK'daki hükümler daha anlaşılır bir şekilde tanımlanmış olacak ve çerçeve bir kanun bulunmaması dolayısıyla pasif durumda olan kimi kanun maddeleri de anlam ifade etmeye başlayacaktır.

Ülkemizde kişisel verilerin korunması ile ilgili bir çerçeve kanunu bulunmaması dolayısıyla, TCK'da düzenlenen bu fillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesi, hangi verilerin kişisel veri olduğunun belirlenmesi ya da yukarıda sayılan fiillerin tanımları ve kapsamları gibi konularda uygulamada tereddütler ortaya çıkmaktadır. Bu tereddütler, Raporun ilerleyen kısımlarında da görülebileceği gibi, çeşitli mahkeme kararlarında da görülebilmektedir. Veri koruması hukukunun ve bu konudaki farkındalığın eksikliği Türk Ceza Kanununun 135. maddesinin 1. ve 2. fıkralarında açıkça görülmektedir. Zira 135. Maddeye göre normal kişisel veriler ile özel niteliği olan (hassas) verilerin hukuka aykırı olarak işlenmesi halinde verilecek faile ceza arasında bir fark mevcut değildir. TCK'nın bu maddelerinin tam olarak yürürlüğe konabilmesi ve konu ile ilgili mahkeme kararlarındaki tereddütlerin ortadan kaldırılabilmesi için kişisel verinin ve hukuka uygun / hukuka aykırı kişisel veri işlemenin ne olduğunun, kişisel verilerin korunmasına özgü bir kanun ile belirlenmesi gerekmektedir.

c) Adli Sicil Kanunu

5352 sayılı Adli Sicil Kanunu, adli sicil bilgilerinin Adalet Bakanlığı Adlî Sicil ve İstatistik Genel Müdürlüğündeki Merkezî Adlî Sicilde tutulacağını düzenlemektedir. Kanunun 11. maddesi adli sicil ve arşiv bilgilerinin gizli olduğunu, bu bilgilerin görevlilerce açıklanamayacağını ve Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamayacağını düzenlemektedir.

[104] Adalet Bakanlığı Bilgi Edinme Bürosuna yapılmış olan 29.04.2014 tarihli başvuru sonucu iletilen bilgiler

d) Bilgi Edinme Hakkı Kanunu

4982 sayılı Bilgi Edinme Hakkı Kanunu, kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir. Ancak Kanun, bilgi edinme hakkının sınırsız olmadığını düzenlemiş ve bilgi edinme hakkı kapsamında değerlendirilemeyecek bilgi türleri saymıştır. Bu bilgi türlerinden biri de özel hayatın gizliliğine ilişkin bilgilerdir. Bu doğrultuda, Kanunun 21. maddesi aşağıdaki hükmü getirmektedir;

> *"Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır.*
>
> *Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir."*

e) Türk Medeni Kanunu

4721 sayılı Türk Medeni Kanunu, kişi hak ve özgürlüklerini koruyan maddeler içermektedir. Kanunun 23, 24 ve 25. Maddeleri sırasıyla;

- *Kimsenin özgürlüklerinden vazgeçemeyeceği veya onları hukuka ya da ahlâka aykırı olarak sınırlayamayacağı,*
- *Hukuka aykırı olarak kişilik hakkına saldırılan kimsenin, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebileceği,*
- *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 saldırı hukuka aykırı olduğu,*

hükümlerini getirmekte ve kişilik haklarına saldırıda bulunulan kişinin sahip olduğu dava haklarını düzenlemektedir.

2.2.2. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 4 Mayıs 2007 tarihinde kabul edilmiş ve 6 Şubat 2014 ile 26 Şubat 2014 tarihilerinde önemli değişikliklere uğramış şekilde yürürlüğünü sürdürmektedir. Henüz yeni değişikliğe uğrayan ve kamuoyunda oldukça

tartışmalı bir konu olmayı sürdüren 5651 sayılı Kanun üzerinde detaylıca durmakta önem bulunmaktadır.

5651 sayılı Kanun esaslı olarak üç ana konuyu düzenlemektedir:

(1) İçerik, yer, erişim ve toplu kullanım sağlayıcılar gibi temel İnternet aktörlerinin hukuki, cezai ve idari sorumlulukları;
(2) Sınırlı sayı prensibine göre belirlenmiş sekiz farklı suç için, erişimin engellenmesi yöntemiyle mücadele edilmesi;
(3) İnternet ortamında kişilik haklarının ve özel hayatın gizliliğinin ihlalleri durumlarında İnternet içeriğine nasıl müdahale edileceğinin usulü.

5651 sayılı Kanunun düzenlediği her üç konunun kişisel verilerin saklanması ve korunması hukuku ile yakın bağıntısı bulunmaktadır. Bu bölüm altında bu konuyla ilgili 5651 sayılı Kanun hükümleri etraflıca incelenecektir.

a) Veri Saklanmasına İlişkin Hükümler

5651 sayılı Kanun altında İnternet trafiği ile ilgili verilerin saklanmasına ilişkin çeşitli hükümler bulunmaktadır. Bu hükümler farklı İnternet aktörler için farklı nitelik ve kapsamda belirlenmiştir. Ayrıca, 5651 sayılı Kanun trafik bilgisi olarak tanımladığı nitelikli veri türü için ayrı yükümlülükler ve koruma mekanizmaları öngörmüştür. Müteakip bölümde her bir İnternet aktörü için bu düzenlemeler etraflıca incelenecektir:

aa) İçerik Sağlayıcılar Açısından Hukuki Risk Analizi

5651 sayılı Kanunun 2. maddesinin 1. fıkrasının (f) bendinde "*İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*" olarak tanımlanan içerik sağlayıcıların temel yükümlülükleri 4. Madde altında etraflıca düzenlenmiştir. 4. maddenin bu çalışma bakımından önemli olan kısmı 6 Şubat 2014 tarihinde 3. Fıkrasıdır. Hüküm şöyledir:

> *"(3) (Ek: 6/2/2014-6518/87 md.) İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır."*

Bu hüküm her ne kadar doğrudan kişisel verilerin saklanması veya korunması ile ilgili veya trafik bilgisi gibi nitelikli bir veri ile ilgili doğrudan bir düzenleme içermemesine rağmen, fıkranın kaleme alınış şekli bu konuyla ilgili hukuki riskler içermektedir.

Öncelikle söz konusu düzenleme içerik sağlayıcılara kapsamı ve sınırı belli olmayan ve öngörülemeyen muğlak bir yükümlülük altına sokmaktadır. Fıkrada kastedilen *"Başkanlık"*, BTK altındaki TİB'dir ve bu fıkra TİB'e sadece 5651 sayılı Kanun değil, diğer tüm Kanunlarla verilen veya verilebilecek her türlü görevin ifası kapsamında belli davranışlarda bulunması veya belli davranışlardan kaçınması yönünde bir yükümlülük altına sokmaktadır.

Üst yasal çerçevenin belirsizliğinin yanı sıra, yapılacak davranışlar ve kaçınılacak davranışlar bakımından da bir belirsizlik söz konusudur. Bu fıkraya göre, TİB tarafından talep edilen bilgiler, talep edilen şekilde TİB'e teslim edilecek ve TİB tarafından bildirilen tedbirler alınacaktır. Öncelikle hangi bilgilerin talep konusu olabileceği belirsizdir. Ayrıca, hangi usulde bu bilgilerin teslim edileceği belli değildir. Aynı doğrultuda, hangi tedbirlerin alınacağı ve hangi davranışlar veya usuller yerine getirildiği takdirde bu fıkra hükümlerinin yerine getirilmiş sağlayacağı belirsizdir.

Söz konusu bilgilerin trafik verisi olduğu durumunda ise, 5651 sayılı Kanunun 3. maddesine 26 Şubat 2014 tarihinde eklenen 4. fıkra ile birlikte okunması gerekmektedir. "Bilgilendirme Yükümlülüğü" başlıklı 3. Maddenin 4. fıkrası şu şekildedir:

> *"(4) (Ek: 26/2/2014-6527/16 md.) Trafik bilgisi ancak bir suç soruşturması ve/veya kovuşturması kapsamında mahkemelerce talep edilmesi hâlinde Başkanlık tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınarak verilir."*

Trafik bilgisi ise 2. maddenin 1. fıkrasının (j) bendinde şu şekilde tanımlanmıştır:

> *"j) (Değişik: 26/2/2014-6527/15 md.) Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,"*[105]

3. maddenin 4. fıkrasına göre trafik bilgisi için özel bir koruma mekanizması öngörülmüş ve trafik verilerinin ancak bir soruşturma veya kovuşturma olması durumunda ve de mahkeme tarafından bu yönde bir talep olması durumunda TİB tarafından içerik sağlayıcı, yer sağlayıcı ve/veya erişim sağlayıcıdan alınacağı öngörülmüştür İnternet ortamında içerik oluşturan, değiştiren veya sunan kişiler olarak tanımlanan içerik sağlayıcılar en geniş ifadeyle İnternet kullanıcılarını ifade etmektedir. Bu düzenlemenin yaklaşımı esasında yerinde değildir. Zira, içerik sağlayıcıların trafik bilgisi tutması teknik olarak ne pratiktir ne de mümkündür.

[105] Bu tanımlama da 26 Şubat 2014 tarihinde değişikliğe uğramıştır. Değişiklik öncesi trafik bilgisi şu şekilde tanımlanmaktaydı: "*j) Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri*".

İçerik sağlayıcının kapsama alınmasına ilişkin tartışma bir kenara bırakılacak olursa; 4. maddenin 3. fıkrası kapsamının yukarıdaki açıklamalar ışığında (1) trafik bilgisi, (2) trafik bilgisi dışında kalan diğer bilgiler, şeklinde iki farklı kategoride incelenebilir.

Trafik bilgisi için 3. maddenin 4. fıkrası özel bir güvence sağlamakta ve ancak hakim kararıyla TİB tarafından bu bilginin talep edileceğini öngörmektedir. Ancak trafik bilgisi dışında kalan diğer bilgiler için böyle bir güvence bulunmamaktadır. 4. Maddenin 3. Fıkrasın bu haliyle kişisel verileri açısından ciddi bir hukuk risk içermektedir. Hangi tür verilerin kapsama girmesinin belirsizliğinin dışında, TİB gibi idari bir makamın her türlü kanun altında düzenlenebilecek görevlerinin ifası kapsamında emir ve talimatını yerine getirme yükümlülüğü altına koyulmasının makul bir gerekçesi yoktur. Bu bağlamda, 4. Maddenin 3. Fıkrası önemli hukuki sorunlara yol açabilecek riskleri barındıran bir düzenlemedir.

bb) Yer Sağlayıcılar Açısından Hukuki Risk Analizi

5651 sayılı Kanunun 2. maddesinin 1. fıkrasının (m) bendinde "*Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler*" olarak tanımlanan içerik sağlayıcıların temel yükümlülükleri 5. Madde altında etraflıca düzenlenmiştir. 5. maddenin bu çalışma bakımından önemli olan kısmı 6 Şubat 2014 tarihinde eklenen 3. fıkrasıdır. Fıkra şu şekildedir:

> *"(3) (Ek: 6/2/2014-6518/88 md.) Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür."*

5651 sayılı Kanun'a eklenen bu düzenleme önemli bir yasal boşluğu doldurmuştur. Bu hüküm eklenmeden önce yer sağlayıcıların trafik bilgisi saklama yükümlülükleri uygulama yönetmeliği altında düzenlenmekteydi. Özel hayatın gizliliği başta olmak üzere birçok temel hak ve hürriyete ilişkin önemli etkileri olan trafik bilgisi saklama yükümlülüğünün idari bir düzenleme altında düzenleniyor olması uzun bir süredir eleştirilmekteydi. Bu eleştiriler göz önüne alınarak trafik bilgisi saklamaya ilişkin hüküm yasal bir zemine kavuşturulmuş ve temel hak ve hürriyetlere ilişkin kısıtlamaların kanunla yapılmasını öngören Anayasanın 13. maddesiyle de uyum sağlanmıştır. Trafik bilgisi tutmanın kişisel verilerin korunması açısından etkileri bir sonraki bölüm altında etraflıca incelenmektedir.

Yer sağlayıcılar ile ilgili bu çalışma açısından önemli diğer bir hüküm ise 5. maddeye 6 Şubat 2014 tarihinde eklenen 5. fıkradır. Fıkra şu şekildedir:

"(5) (Ek: 6/2/2014-6518/88 md.) Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür."

Bir önceki bölümde etraflıca incelendiği üzere benzer yükümlülük içerik sağlayıcılar için getirilmiştir. Bu bağlamda, 4. maddenin 3. fıkrası için getirilen eleştiriler 5. maddenin 5. ıkrası için de geçerlidir. Söz konusu düzenleme yer sağlayıcılara kapsamı ve sınırı belli olmayan ve öngörülemeyen muğlak bir yükümlülük altına sokmaktadır. Bu bağlamda, 5. maddenin 5. fıkrası kişisel verilerin korunması açısından önemli hukuki sorunlara yol açabilecek riskleri barındıran bir düzenlemedir.

cc) Erişim Sağlayıcılar Açısından Hukuki Risk Analizi

5651 sayılı Kanunun 2. maddesinin 1. fıkrasının (e) bendinde "*Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler*" olarak tanımlanan içerik sağlayıcıların temel yükümlülükleri 6. madde altında etraflıca düzenlenmiştir. 6. Maddenin bu çalışma bakımından önemli olan 1. fıkrasının (b) bendidir. Bend şu şekildedir:

"(1) Erişim sağlayıcı; (...) (b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla, (...) yükümlüdür."

Türk Hukukunda kişisel verilerin korunmasına yönelik özel bir düzenleme olmayışı önemli bir eksikliktir ve hem yer sağlayıcılar hem de erişim sağlayıcılar için öngörülen trafik bilgisi saklama yükümlülüğü açısından ciddi bir hukuki risk oluşturmaktadır. Anayasa'nın 20. maddesine 2010 yılında eklenen 3. fıkrasına göre "*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.*"

5237 sayılı Türk Ceza Kanunu'nda 21 Şubat 2014 tarihinde yapılan değişikliklerle kişisel verilerin korunması ile ilgili suçların cezası iki katına artırılmış olsa da, Anayasanın 20. maddesinin 3. fıkrasında yer alan güvenceyi hayata geçirecek özel bir kişisel verilerin korunması düzenlememesi olmaması ciddi bir hukuki risk oluşturmaktadır. 24.07.2013 tarihinde yürürlüğe koyulan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik de bu anlamda gerekli korumayı sağlamaktan

uzaktır. Her ne kadar trafik bilgilerinin saklanmasına ilişkin hüküm Avrupa Birliği Kişisel Verilerin Korunması Direktifi'nden esinlenmişse de, Avrupa Adalet Divanı'nın 8 Nisan 2014 tarihinde AB Veri Saklama Direktifi ile ilgili vermiş olduğu iptal kararının bu bağlamda ayrıca dikkate alınması gerekmektedir.[106]

Trafik bilgisi bir İnternet kullanıcısının özel hayatı ile ilgili birçok detayı, kişisel tercihleri, politik eğilimlerini, sağlık bilgilerini, ticari sırlarını ifşa edebilecek nitelikte kritik bilgiler içeren bir veri türüdür. Her ne kadar amaç bir suç işlendiği durumda failin tespitine yönelik ise de, özellikle sürenin uzunluğu, bir kişinin hayatı ile ilgili neredeyse her detayın kolayca tespit edilmesine olanak tanımaktadır. 5651 sayılı Kanun gereğince bir yıldan az ve iki yıldan fazla olmamak üzere saklanması gereken bu verinin amacına aykırı ve hukuka aykırı şekilde kullanılmasını önleyecek özel bir düzenlemenin olmayışı, ciddi hukuki risk oluşturmaktadır.

Erişim sağlayıcılar ile ilgili bu çalışma açısından önemli diğer bir hüküm ise 6. maddeye 6 Şubat 2014 tarihinde eklenen 1. fıkranın (d) bendidir. Bend şu şekildedir:

> *"d) (Ek: 6/2/2014-6518/89 md.) Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla,"*

Bir önceki bölümde etraflıca incelendiği üzere benzer yükümlülük hem içerik hem de yer sağlayıcılar için getirilmiştir. Bu bağlamda, hem içerik hem yer sağlayıcılar için getirilen eleştiriler 6. maddenin 1. fıkrasının (d) bendi için de geçerlidir. Söz konusu düzenleme erişim sağlayıcılara kapsamı ve sınırı belli olmayan ve öngörülemeyen muğlak bir yükümlülük altına sokmaktadır. Bu bağlamda, 6. maddenin 1. fıkrasının (d) bendi kişisel verilerin korunması açısından önemli hukuki sorunlara yol açabilecek riskleri barındıran bir düzenlemedir.

b) Erişimin Engellenmesi Uygulamasının Değerlendirilmesi

5651 sayılı Kanun, 8. madde altında sınırlı sayı prensibine göre belirlenen belli suçlar için ve 9 ile 9/A maddeleri altında düzenlenen kişilik haklarının ihlali ve özel hayatın gizliliğinin ihlali durumlarında İnternet içeriğine erişimin engellenmesi olanağı tanımaktadır. İnternet içeriğine erişimin engellenmesi için 2007 yılından bugüne DNS engelleme tekniği kullanılmaktadır. Şubat ayında yapılan değişiklikle URL engelleme tekniği benimsenmiş olsa da, bu tür engellemeyi yapabilecek teknik altyapı henüz kurulmamıştır. DNS engelleme

[106] Detayları için bkz. Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, 8 April 2014.

tekniği ile yakın zamanda işler hale gelmesi beklenen URL engelleme tekniklerinin kişisel veriler açısında doğrudan ve dolaylı çeşitli etkileri bulunmaktadır.

DNS engelleme tekniğinin kişisel veriler üzerindeki etkisi dolaylıdır. DNS engelleme tekniği kolayca aşılabilecek bir engelleme tekniğidir. Ancak yaygın olarak kullanıldığı bilinen bu tekniklerin asıl oluşturduğu sorun bilgi güvenliği açıklarıdır. Engellemeleri aşmak için yapılan DNS değişiklikleri, VPN, tunnelling veya benzeri proxy kullanılması Türk İnternet kullanıcılarının verilerinin riskli alanlarda paylaşıma açmakta ve bilgi güvenliği riski açmaktadır. Bu bağlamda, etkin olmadığı ispatlanmış bir engelleme tekniğinin kullanılmasının bu açıdan tekrar gözden geçirilmesi gerekmektedir.

URL engelleme tekniğinin kişisel veriler üzerindeki etkisi doğrudandır. Özellikle DNS engellemenin bilgiye erişim ve iletişim hürriyetlerini ölçüsüz engellemesine yönelik eleştiriler; Avrupa İnsan Hakları Mahkemesi'nin 18 Aralık 2012 tarihli Ahmet Yıldırım/Türkiye kararında bu konuda Türkiye'yi mahkum etmesi bu alanda reform yapılmasına yönelik reform dinamikleri olmuştur. Bu bağlamda, 5651 sayılı Kanun'da Şubat ayında yapılan değişikliklerle URL engelleme tekniği açıkça kanunla tanımlanmış ve zorunlu olmadıkça bir web sitesinin tamamına erişimin engellenemeyeceğine ilişkin bir düzenlemeye gidilmiştir. Anayasa Mahkemesi 2 Nisan 2014 tarihinde Twitter sitesine erişimin engellenmesine yönelik olarak yapılan bireysel başvuru üzerine vermiş olduğu kararda da, URL engelleme tekniği dışında bir engelleme tekniği kullanılmasının yolunu kapatmıştır.

Öte yandan, URL engelleme tekniğini uygulamak için DNS engelleme tekniğinin aksine ek yazılım ve donanım yatırımı gerektirmektedir. Bu bağlamda, URL engelleme tekniğinin etkinliği ve işlerliği bu alanda yapılacak yatırımın büyüklüğü ile orantılıdır. URL engelleme tekniği altyapıda önemli bir dönüşüm gerektirmektedir. URL engelleme tekniği ile İnternet ortamında belli konumdaki içeriğe erişimin engellenmesi mümkün olmakta; bir web sitesinin tüm içeriği ile erişime kapatılmasının önüne geçmektedir. Ancak, bu şekilde bir engelleme yapılması için İnternet omurgasında konuşlandırılacak ve özel yazılımlarla programlanmış donanımların belli bir filtre uygulaması ve trafik analizi yapması gerekmektedir. Bu trafik analizi sırasında tüm İnternet kullanıcısı trafiğinin incelenmesi, filtrelenmesi ve kaydedilmesi mümkündür. Teknik olarak "*paket analizi*" veya incelemenin kapsamına göre "*derin paket analizi*" olarak adlandırılan bu süreç, kişisel verilerin korunması açısından önemli riskleri bulunmaktadır.

Bir önceki bölüm altında incelendiği üzere Türk hukukunda kişisel verilerin korunması ile ilgili özel bir düzenleme yer almamaktadır. Anayasal hükümlerin uygulanması için çıkarılması planlanan yasal düzenleme hala tasarı aşamasındadır. Aynı doğrultuda, bir önceki bölümde açıklandığı üzere, trafik bilgilerinin en az 1 yıl ve en fazla 2 yıl süre ile saklanması gerekmektedir. Bu süre bir kişinin özel hayatı ile ilgili birçok detayı, kişisel tercihleri, politik eğilimlerini, sağlık bilgilerini, ticari sırlarını ifşa edebilecek nitelikte kritik bilgilerin toplanması, derlenmesi ve analiz edilmesi için yeterli uzunlukta bir süredir. Tüm bu hususlar göz önüne alındığında, her ne kadar URL engelleme tekniği ölçülü bir engelleme tekniği ise, kişisel verilerin korunması ile ilgili etkin bir mekanizma olmadan uygulanması ciddi hukuki riskler taşımaktadır.

Sonuç olarak, 5651 sayılı Kanun altında kişisel verilerin korunmasını doğrudan veya dolaylı olarak ilgilendiren çeşitli hükümler yer almaktadır. Kanun, içerik, yer ve erişim sağlayıcılar için genel bir trafik bilgisi toplama ve gerektiğinde TİB ile paylaşma ile ilgili düzenlemeler yapmıştır. Ayrıca, erişimin engellenmesi usulünde kişisel verilerin korunması ile bağlantılı hususular yer almaktadır. Tüm bu hükümlere ve teknik uygulamalara karşın, kişisel verilerin korunmasına ilişkin kapsamlı ve tatmin edici bir düzenlemenin yer almayışı ve Türk hukukunda bu amaçla özel bir düzenleme olmaması ciddi hukuki riskler oluşturmaktadır.

2.2.3. Sektörel Kanun ve İkincil Düzenlemeler

Kişisel verilerin gizliliği ve korunması alanında sektörel kanun ve düzenlemelerde çeşitli hükümlere rastlamak mümkündür:

a) İş Kanunu

4857 sayılı İş Kanununun 75. maddesi aşağıdaki hükmü getirmektedir;

> "*İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.*
>
> *İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."*

Buna göre, işveren, işçi ile ilgili verileri iş sözleşmesi ve iş ilişkisinin izin verdiği ölçüde kullanmakla yükümlüdür.

b) Bankacılık Kanunu

5411 sayılı Bankacılık Kanunu, banka çalışanlarının, müşterilere ait gizli bilgileri, kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamayacağını düzenlemektedir. Kanun, bu hükme uymayanların bir yıldan üç yıla kadar hapis ve bin günden ikibin güne kadar adlî para cezası ile cezalandırılacağı hükmünü getirmiştir.

c) Banka ve Kredi Kartları Kanunu

5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 23. maddesi aşağıdaki hükmü getirmektedir;

> *"Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. […] Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür."*

Aynı Kanunun 39. maddesi, bu hükme aykırı hareket eden kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişilerin, bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılacağını düzenlemektedir.

d) Tıbbi Deontoloji Tüzüğü

Tüzüğün 4. maddesi ile *"Tabip ve diş tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez. Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz"* hükmü getirmekte ve hastanın gizli bilgilerinin korunması gerekliliğini düzenlemektedir. Benzer şekilde, Hasta Hakları Yönetmeliğinin 23. maddesi;

> *"Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.*
>
> *Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz.*

Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.

Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz."

hükmü getirerek hasta bilgilerinin korunmasını amaçlamaktadır.

e) Elektronik Haberleşme Kanunu

Elektronik haberleşme sektörü bakımından temel düzenleme olan 5809 sayılı Elektronik Haberleşme Kanunu'nun elektronik haberleşme hizmetine ilişkin temel ilkeleri sıralayan 4. Maddesi kişisel verilerin korunmasına değinmiş ve *"bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi"* ilkesine yer vermiştir. Bu konuda düzenleme yapma yetkisi Bilgi Teknolojileri ve İletişim Kurumu'na ("BTK") verilmiştir. Ancak Anayasa Mahkemesi, Danıştay İdari Dava Daireleri Kurulu tarafından yapılan başvuru sonucu, BTK'ya kişisel verilerin işlenmesi konusunda yetki veren maddeyi iptal etmiştir. Kişisel verilerin korunması, Anayasaya göre kanun ile yapılması gereken bir düzenleme olduğu için, Anayasa Mahkemesi, ilgili maddeyi Anayasaya aykırı bulmuştur.

f) Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik

Yönetmelik, 24.07.2012 Tarih ve 28363 Sayılı Resmi Gazete 'de yayımlanmıştır. Yönetmelik'in yürürlük tarihi, yayımından itibaren 6 ay sonra olarak belirlenmiştir; Yönetmelik 24.01.2013'te yürürlüğe girmiştir. Yönetmelik elektronik haberleşme sektöründe kişisel verilerin işlenmesi bakımından, AB'nin özellikle 2002/58 Sayılı Direktifi kapsamında önemli düzenlemeler getirmektedir. Yönetmelik, AB'nin ilgili düzenlemeleri ile paralel şekilde, veri işlemeye ilişkin temel ilkeleri belirlemiş ve bunlara ek olarak işletmecilere şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğinin sağlanmasına ilişkin birtakım tedbirleri öngörmüştür.

g) Elektronik İmza Kanunu

5070 Sayılı Kanunun elektronik sertifika hizmet sağlayıcısı ile ilgili,

- Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

- Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

- Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz

şeklinde yükümlülükler getirmektedir.

Yukarıda bahsedilen düzenlemelerin yanı sıra, Türk Borçlar Kanunu, Türk Ticaret Kanunu, Nüfus Hizmetleri Kanunu, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik gibi düzenlemeler içerisinde de kişisel verilerin korunmasına ilişkin belirli hükümler yer almaktadır.

2.2.4. Kişisel Verilerin Korunması Konusunda Yargıtay Kararları

Çerçeve bir kişisel verilerin korunması kanunu bulunmaması ve bunun dolayısıyla kişilerde kişisel verilerinin korunmasına dair bir kültür oluşmaması ve TCK'daki ilgili maddelerin tam olarak işletilmemesi nedeniyle, Yargıtay'da, TCK'nın kişisel verilerin korunması ile ilgili maddeleri kapsamında çok fazla dava görülmemiştir. Ancak Yargıtay'da konuyla ilgili görülmüş olan önemli davalara değinmek gerekmektedir:

a) Yargıtay 12. Ceza Dairesi'nin 2011/15721 E. ve 2012/11074 K. Numaralı Kararı

Yargıtay bu kararında; bir gazete muhabirinin, mağdurla takma isim kullanarak yazmış olduğu kitap sonrası mağdurun gerçek kimliğini tespit etmek amacıyla araştırma yaparak mağdurun gerçek kimliğine ulaşması ve bir gazetenin internet sitesinde "*'Kocasını 300 erkekle nasıl aldattığını kitabında ballandıra ballandıra anlatan kadının izini süren Güneş, insanın kanını donduran bir gerçeğe ulaştı*" başlığıyla vermesinin *haber verme sınırlarını aştığı ve kişisel verileri ele geçirmek ve yaymak suçunu oluşturduğu* kararını vermiştir.

b) Yargıtay 12. Ceza Dairesinin 2011/20111 E. ve 2012/12850 K. Numaralı Kararı

Bu kararda Yargıtay, belediyedeki işlerini halletmek için belediyeye giden sanığın, belediye başkanının belediyede bulunmaması nedeniyle ilçeye dönmesi ve belediye başkanına ait makam aracının mesai saatleri içinde bir kahvehanenin önünde park halinde olduğunu ve beyanına göre başkanın da kahvede oyun oynadığını görmesi üzerine, kahvehanenin önünde park etmiş halde bulunan belediye aracının fotoğraflarını çekmek isterken belediyede çalıştığını ve başkanla gezdiğini beyan eden katılanın gelerek sanığı engellemeye çalışarak sanığın kolundan çekmesi üzerine, sanığın da kendisini engelleyen ve muhtemel bir şikayet hakkını kullanmasına engel olan bu şahsın kim olduğunu öğrenmek amacıyla katılanın fotoğrafını çekmesi şeklinde gelişen olayda, mahkemenin bir suç oluşmadığına ilişkin kararını onamıştır.

c) Yargıtay 12. Ceza Dairesinin 2012/13049 E. ve 2012/14798 K. Numaralı Kararı

TCK'da kişisel verinin ne olduğu açıklanmış olmasa da, Yargıtay, kararlarında hangi eylemlerin kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi ve ifşa edilmesi eylemlerini oluşturacağını tartışmıştır. 2012/13049 E. ve 2012/14798 K. numaralı kararında, Yargıtay, " *5237 sayılı TCK'nın 136/1. maddesinde düzenlenen 'Verileri hukuka aykırı olarak verme veya ele geçirme' suçunun oluşabilmesi için, belirli veya belirlenebilir bir kişinin nüfus bilgisi, adresi, parmak izi, DNA bilgisi, cinsel eğilimi, sağlık bilgileri, etnik kökeni, siyasi görüşü, felsefi ve dini inancı gibi kişiye ilişkin her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi gerektiği*"ne değinmiştir. Yargıtay, bu kararında, henüz temyiz aşamasında olan bir mahkeme kararının niteliği gereği kişisel veri olarak kabulünün mümkün olmadığı sonucuna varmıştır.

d) Yargıtay 12. Ceza Dairesinin 2012/16872 E. ve 2012/18221 K Numaralı Kararı

TCK'da *"özel hayatın gizliliğini ihlal"* ve *"kişisel verilerin kaydedilmesi"* suçlarının iki ayrı suç olarak düzenlenmesi ve kişisel verilerin korunması ile ilgili özgül bir kanun bulunmaması dolayısıyla kapsamın tam olarak belirlenememesi durumu, Yargıtay'ın 2012/16872 E. ve 2012/18221 K. numaralı kararında belirgindir. Yargıtay bu kararında TCK madde 135'de düzenlenen *"kişisel verilerin kaydedilmesi" suçunun oluşabilmesi için, "belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesinin gerekmekte"* olduğunu belirtmiştir. Bunun ardından kişisel verinin ne olduğunu tartışmış ve "*'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" sonucuna varmıştır. Ancak bunun ardından Yargıtay ilginç bir karara varmış ve *"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 […] 5237 sayılı TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği*"ni söylemiştir. Yani Yargıtay, kişinin özel hayatına ilişkin görüntü ya da sesinin kişisel veri olduğunu, ancak kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa edilmesinin kişisel verilerin kaydedilmesinden ayrı bir suç olarak düzenlendiği, bu nedenle kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği hükmüne varmıştır. Yani Yargıtay kişinin özel hayatına ilişkin görüntü ya da sesinin *hem kişisel veri olduğunu hem de kişisel veri kapsamında değerlendirilemeyeceğini* söylemektedir. Buradaki karışıklığın nedenlerinden biri, kişisel verinin tanımının bir çerçeve kanunda tam olarak yapılamaması ve birbirleri ile çok benzer konuları düzenleyen maddelerin bu durumda karışıklığa yol açması olarak düşünülebilir.

2.3. TASARI İÇİN DEĞİŞİKLİK ÖNERİLERİ

Kişisel Verilerin Korunması Hakkında Kanun Tasarısı, AB Veri Koruması Direktifi başta olmak üzere, veri korumasına ilişkin diğer normlarla büyük ölçüde uyum içindedir. Bizim bu bölümde yaptığımız değişiklik önerilerinin başlıca amacı ise; Tasarı'yı AB regülasyonu ile getirilen önemli hükümlerle uyumlu hale getirmek, bireyin anayasal hakkı olan veri koruması hakkının efektif olarak kullanılmasını sağlamak, veri odaklı yenilikçiliğin teşvik edilmesini sağlamak ve verilerden katma değerli hizmetler geliştiren kuruluşlar ile bireyin hakları arasında denge gözeterek ağ ekonomisinin gelişiminin önünü açmak, orantılılık ilkesini temel bir değer olarak yasadaki hükümlerin yorumunda kullanmak, kurulacak veri koruması kurulunun tam bağımsızlığını temin etmek, sadece basın özgürlüğü değil, ifade hürriyeti gibi diğer temel hak ve özgürlüklerin de veri işlemede dikkate alındığı uygulamalar yaratmak, *"co-regulation"ı "codes of conduct"*lar üzerinden teşvik etmek, veri sicilleri ve kayıt sistemlerine yoğunlaşmak yerine veri sorumlusunun yükümlülüklerini artırmak ve onun üzerinden işleyecek bir veri koruması yönetişimi yaratmak, aracı hizmet sağlayıcıların sorumluluklarına ilişkin iç hukukumuzdaki çerçeveye uygun bir yaklaşım benimsenmesini teşvik etmektir. Taslakla ilgili belirli maddelere ilişkin görüş ve önerilerimiz aşağıda yer almaktadır:

2.3.1. Amaç

Tasarı'da Kanunun amacı şu şekilde tanımlanmaktadır:

> Madde 1*: "Bu Kanunun amacı, kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir".*

Amaç hükmünde AB Veri Koruması Direktifi ile uyumluluk adına, Kanunun, kişisel verilerin işlenmesinde, verilerin serbest dolaşıma imkân bırakarak özel hayatın gizliliğini korumayı amaç edindiğini belirtmek yerinde olacaktır. Ayrıca Raporumuzda sıkça vurguladığımız üzere; veri korumasına ilişkin yasal düzenlemelerin amacı; bir yanda bireyin temel hak ve özgürlüklerini korumak iken, diğer yanda kuruluşların bu verileri işleme ihtiyacını dengelemek olmalıdır. Mevcut hükümde ise bu dengenin gözetilmediği ve Tasarı'nın sadece bireyin temel hak ve özgürlüklerini korumaya odaklandığı görülmektedir. Bu nedenle Amaç hükmünde; bu iki süjenin kişisel verilere ilişkin hakları arasındaki denge gözetilmesinde fayda görülmektedir.

2.3.2. Kişisel veri

Tasarı kişisel veri kavramını şu şekilde tanımlamaktadır:

> Madde 3/ç: *Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,* ifade etmektedir.

Direktiften farklı olarak, Taslakta, kişisel verinin tanımında orantılılık ilkesine yer verilmemiştir. Direktif Resital md. 26'da kişisel verinin belirlenmesinde orantılılık ilkesinin gözetileceği belirtilmektedir. Ülkemizdeki Taslak Kanunda da kişisel veri tanımında aynı prensibin benimsenmesi önerilmektedir. Bu sebeple, aşağıdaki gibi bir prensibin Taslağın ilgili bölümünde benimsenmesi gerektiği düşünülmektedir;

"Veri koruması prensipleri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi açısından uygulanmalıdır. Bir kişinin kimliğinin belirlenebilir olup olmadığının tespitinde, ilgili kişinin kimliğini belirlemek için başkaları tarafından yapılması olası ve makul yöntemler hesaba katılmalıdır. Veri sahibinin tanınmasının mümkün olmadığı şekilde yapılan anonim işlemelerde ise koruma prensipleri uygulanmamalıdır."

2.3.3. Veri Sorumlusu

Tasarı Madde 3/ğ hükmüne göre veri sorumlusu kavramı şunu ifade etmektedir:

> *"Veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi"*

Tasarı'da veri sorumlusu'na ilişkin bu tanım yerine, AB Veri Koruması Direktifi md. 2/d'deki *" gerçek ya da tüzel kişi, kamu kurumu ya da kuruluşu veya kişisel veri işleme amaçlarını birlikte ya da tek başına belirleyen diğer kişiler"* anlamında kullanılması önerilmektedir. Çünkü; aşağıda değineceğimiz üzere ayrıntılı bir *"veri kayıt sistemi kurulması ve yönetilmesi"* yaklaşımı AB'de artık güncel bir yaklaşım olmadığı için, veri sorumlusunun tanımı da bu yaklaşımdan arındırmak gerekmektedir. Ayrıca AB'de veri sorumlusu olabilecek süjelerin kapsamı daha genişken, Tasarı'da daha dar tutulmuştur.

2.3.4. İlgili Kişinin Rızası

İlgili kişinin rızası Tasarı Madde 5/f.1 hükmünde şu şekilde tanımlanmaktadır:

> *"Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez".*

Rıza, veri işlemek için hukuki dayanaklardan yalnızca biri olup tek hukuki dayanak değildir. Ancak *"rıza"* kavramının kullanıcılara ve topluma fayda sağlayacak, veri işleme temelli yenilikçilik göz önüne alınarak değerlendirilmesi gerekmektedir. İlgili kişinin sadece "evet" veya "hayır" diyen pasif süjeler olması yerine, kendi verileri ile ilgili şeffaf süreçlere aktif katılımlarının sağlandığı uygulamalar yaratılmalıdır. Yine *"rıza"*, veri sahibinin bilgilendirilmiş olmasını sağlayan, rızanın özgürce verildiğini gösteren, ilgili kişinin iradesini yansıtan ve kişisel veri işleme işleminin kapsamını hesaba katan her türlü uygun metot ile alınabilir. Rıza aynı amaç ya da uygun amaçlar için gerçekleştirilen her türlü işleme faaliyetini kapsamalıdır. İlgili kişinin rızası elektronik ortamda gelen bir talep üzerine alınmışsa; bu talebin açık, öz ve bireye sunulacak olan hizmetin kullanımını gereksiz yere kısıtlamayacak şekilde olmalıdır.

2.3.5. Kişisel Verilerin İşlenmesi-Genel İlkeler

Kişisel verilerin hangi ilkeler ışığında işleneceği Tasarı'da şu şekilde düzenlenmiştir:

Madde 4 - (1) *Kişisel veriler, ancak, bu Kanunda ve diğer kanunlarda öngörülen esas ve usullere uygun olarak işlenebilir.*

> *(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur;*
> *a) Hukuka ve dürüstlük kurallarına uygun olmak.*
> *b) Doğru olmak.*
> *c) Belirli, açık ve meşru amaçlar için işlenmek.*
> *ç) Toplandıkları veya yeniden işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak.*
> *d) Güncel olmak.*
> *e) İşlendikleri amaç için gerekli olan süre kadar muhafaza edilmek.*

Tasarı'da md. 22/b hükmünde yer *alan "Kişisel verilerin anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi"* şeklindeki istisnanın, hukuka uygun bir neden olarak benimsenmesi ve md. 4/c hükmüne eklenmesi önerilmektedir[107].

[107] Madde hükmü şu şekilde formüle edilebilir: *"belirli açık ve meşru amaçlar için toplanmış ve söz konusu amaçlar dışında bir amaçla işlenmemiş olmalıdır. Ayrıca, verilerin, tarihi, istatistiksel ya da bilimsel amaçlarla işlenmesi, uygun olmayan amaç olarak kabul edilmez."*

Gerek bireysel gerek toplumsal fayda ve bilgi toplumu hedefi açısından bakıldığında; veriden hukuki himaye çerçevesi içinde maksimum ölçüde istifade etmek ve kişilerin özel hayatının gizliliğine saygı duyarak bir değer yaratmanın mümkün olmasını sağlamak gerekmektedir.

2.3.6. Anonim Hale Getirme, Anonimleştirme Teknikleri ve Takma Adlı Veri (Pseudonymous Data)

a) Anonim Hale Getirme

Tasarı Madde 3/a) hükmüne göre; anonim hale getirme şunu ifade etmektedir:

> *"Kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini",*

Tasarı md. 3/a'da yer alan anonim hale getirme tanımın; kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiyle, ***aşırı maliyet ya da çaba olmadan*****,** ilişkilendirilemeyecek hale getirilmesini ifade eder" şeklinde formüle edilmesini öneriyoruz. Bir yöntemin aşırı maliyet veya çaba gerektirip gerektirmediği de yine orantılılık ilkesi çerçevesinde değerlendirilmek gerekecektir.

b) Anonimleştirme Teknikleri

Tasarı'nın anonimleştirme tekniklerine işaret eden md. 7/f.2 hükmü; kişisel verilerin anonim hale getirilmesine ilişkin usul ve esasların yönetmelikte gösterileceğini belirtmektedir:

> *Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikte gösterilir.*

Anonim veri, kişisel veri niteliğinde olmadığı için AB içinde ne birincil ne de ikincil bağlayıcı düzenlemelerde anonimleştirme tekniklerine atıf yapan herhangi bir düzenleme mevcut değildir. Bilakis yönetmelikle anonimleştirme tekniklerinin belirlenmesi, bilgi güvenliği veya siber güvenlik açısından da sorun yaratabilecektir. Gelişen teknolojiye bağlı olarak değişen bu konuda ikincil düzenlemelerde bu konuya yer vermemek veya teknoloji nötr bir bakış açısıyla süreçler öngörmek yerinde olacaktır. Bu anlamda AB Veri Koruması Direktifi Resital Madde 27'de düzenlenen işleme kuralları verilerin anonim olarak işlenmesi ve veri sahibinin

kimliğinin tespit edilemeyecek şekilde saklanması konularında rehberlik etmesi açısından faydalı bir araç olarak kullanılabilir.

c) Takma Adlı Veri (Pseudonymous Data)

Tasarı'da yer almayan ancak AB Regülasyon Tasarısında yer alan kavramlardan biri de takma adlı veri (pseudonymous data) kavramıdır. Kavram özetle şunu ifade etmektedir: ″takma adlı veri" ek bilgiler kullanılmadan belirli bir veri sahibi ile ilişkilendirilemeyen ve söz konusu ek bilgilerin ayrı olarak, ilişkilendirilmeyi önleyici önlemler altında saklandığı kişisel veriler anlamına gelmektedir. Eğer veri sorumlusu tarafından işlenen veri, sorumlunun bir kişiyi doğrudan belirlemesine izin vermiyorsa ya da takma adlı veri oluşturuyorsa, veri sorumlusu yalnızca bu kanuna uyumluluk sağlamak için ilgili kişiyi belirlemek amacıyla söz konusu ek bilgileri alamaz ya da işleyemez. Tek başına kullanıldığında, herhangi bir ek bilgi olmadan, bir bireyi tanımlayamayan ancak en fazla bireyleri tanımlamadan birbirinden ayırabilen veriler gibi veri tipleri de koruma gerektirmektedirler. Çünkü bu veriler ile tekrar tanımlayabilme mümkün hale gelmektedir. Ancak veri sorumlularının alacağı yeterli organizasyonel ve teknik önlemler verinin dolaylı olarak tanımlayabilir kalmasını sağlamaktadır. AB'de takma adlı veri olarak adlandırılan bu tür kişisel veriler risk bazlı yaklaşım ve sorumluluk açısından iyi bir örnektir. Çünkü verinin takma adlı veri olarak kalmasını sağlamak amacıyla veri sorumlusu verilerin tamamen ilişkilendirilebilir hale gelmesini engellemek amacıyla gereken tüm makul önlemleri almak zorunda kalacaktır. Takma adlı veri, kişisel veriyi anonim hale getirmeyip bir kimliksizleştirme yöntemi olarak, veri odaklı inovasyon açısından da son derece önemli olup, veri sorumlusu olarak karşımıza çıkacak KOBİ'lere ve genç girişimcilere veri işlemek açısından fayda sağlayacaktır.

2.3.7. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi

Madde 7 hükmü, Tasarı'nın AB düzenlemelerinden ayrıldığı noktalardan biridir. Kuruluşlara bu tür kısıtların getirildiği bir hukuk düzeni, uluslar arası yatırım ve pazara girmek isteyen şirketler açısından sorun olacak ve her defasında tekrar tekrar ilgili kişiden data istenmesi zorunda kalmak hem şirketler için maliyetli hem de ilgili kişi için yorucu olacaktır. AB, verilerin silinmesini yalnızca veri toplama amacı ortadan kalktığı için zorunlu tutmamaktadır. Veri işlemeye dayanak olan esas meşru amaç ortadan kalkmasına rağmen başka meşru amaçlar verinin muhafaza edilmesini gerekli kılabilir. Örneğin; verinin muhasebe, iadeler, güvenlik ve dolandırıcılığı önleme amaçlarıyla toplanması ancak meydana gelen bir hata

nedeniyle verilerin tekrar incelenmesi bu alanda verilebilecek örneklerden sadece birkaçıdır. Veri ekonomisinin iktisadi analizinin yapıldığı Bölüm 1'de de belirtildiği gibi, büyük veri uygulamalarıyla elde edilen etkinlikler birçok zaman farklı amaçlarla kullanılan veri setlerinin beraber değerlendirilmesinin sonucudur. Aynı veriyi ilgili kişiden tekrar talep edip iş süreçlerini devam ettirmek, hem ilgili kişi açısından yorucu hem de kuruluşlar için gereksiz maliyet ve zaman kaybı yaratmaktadır. Bu sakıncaları önlemek için mevcut hükmün aşağıdaki şekilde formüle edilmesinde fayda bulunmaktadır:

> *"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde, başka bir hukuki dayanak yoksa, kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir, takma adlı hale getirilir veya anonim hale getirilir".*

2.3.8. Veri Sorumlusu ve Veri Sorumluları Sicili

a) Veri Sorumlusu

Tasarı'da yer alan tanıma göre:

> Madde 3/ğ) *Veri sorumlusu: Veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,*

ifade etmektedir. Taslakta önerilen tanım, AB'deki mevcut tanıma dayanmaktadır ve yeni taslak Regülasyon ile uyumlu değildir. AB Direktifi ile ve diğer ulusal veri koruması yasal düzenlemelerine uyumluluğu sağlamak amacıyla, veri sorumlusunu Direktif md. 2/d hükmündeki gibi: *"gerçek ya da tüzel kişi, kamu kurumu ya da kuruluşu veya kişisel veri işleme amaçlarını birlikte ya da tek başına belirleyen diğer kişiler"* anlamında kullanılması önerilmektedir. Ayrıca uygulamada dikkat edilmesi gereken bir diğer nokta da; veri sorumlusu ile veri işleyenin rolleri çok net bir şekilde belirlenmesi gerektiğidir. Tasarı'ya göre de farklı sorumlulukları bulunan bu sıfatların bazen aynı kişide birleşmesi örneğin; şirketlerin bazı durumlarda veri sorumlusu bazı durumlarda veri işleyen olarak hareket etmektedir. Şirketler ayrıca alt işleyenlerle de iş yapabilmektedir. Bu nedenle rollerin çatışmaması için veri sorumlusu tarafından bir roller ve sorumluluklar haritası çıkartılması önemlidir. İlgili sektördeki codes of conduct'ta dahi bu haritalamaya ilişkin ilkeler ve süreçler konulabilir.

b) Veri Sorumluları Sicili

Tasarı'nın 15. Maddesinde kamuya açık bir veri sorumluları sicili tutulacağı (f.1) öngörülmekte ve kişisel verileri işleyen gerçek ve tüzel kişiler için, veri işlemeye başlamadan önce sicile kayıt zorunluluğu getirilmektedir (f.2).

Tasarı'da yer alan bu hüküm AB'deki taslak Veri Koruma Regülasyonundan şu noktalarda ayrılmaktadır: Tasarı, veri koruma kurumunun öncelikli kontrolüne ve veri tabanlarının bildirimine dayandırılmıştır. Avrupa Komisyonunun yeni yaklaşımı ise tam tersi olarak sonradan kontrol sistemine dayandırılmış, tüm bildirimleri ortadan kaldırmış ve yetkilendirmeleri en alt seviyeye indirmiştir. Bu nedenle Kanundaki detaylı kayıt yaklaşımının terk edilmesi ve yerine güvenlik ihlallerinde bildirim gereksinimlerinin getirilmesi tavsiye edilmektedir. AB'de veri sorumlularının Direktif'teki ilke ve yükümlülükleri hayata geçirebilmeleri için uygun ve efektif tedbirleri alması ve uygulaması gerekliliğini ifade eden *"hesap verilebilirlik"* ilkesi[108]; bu tür kayıt sistemleri kurulması yerine, iyi bir veri koruması veri koruması yönetişimi için veri sorumlularının sorumluluklarını artıran ve veri sorumluları üzerinden işleyecek *"sorumluluk esaslı mekanizmaların"* amaca daha çok hizmet edeceği vurgulanmaktadır[109][110]. Veri sorumluları sicili, Tasarı açısından değerlendirildiğinde, Veri Koruması Kurumu'nun denetim yapmasını ve önüne gelecek taleplerde daha kısa sürede karar vermesini sağlayacaktır. Ayrıca verisini hangi kuruluşun işlediği hakkında bilgi sahibi olmak isteyen ilgili kişiler için de faydalar sunmaktadır. Ancak dijital çağda big data ile uygulamalar geliştiren ve veri odaklı inovasyon konusunda çalışan kuruluşlar için, veri sorumlusu olarak, veriye temas ettikleri her bir an da sürekli bildirimde bulunmaları çok zor, maliyetli ve zaman alıcı olabilecektir.

2.3.9. Kişisel Verilerin İşlenme Şartları

Tasarı md. 5/f.1 kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenemeyeceğini ana kural olarak belirlemektedir. 2. fıkrada belirtilen hallerde ise kişisel verilerin açık rıza olmadan da işlenebileceğini öngörmektedir.

İlk olarak vurgulamak gerekir ki; **AB'de veri işleme şartlarının hepsi birbirine eşittir ve rıza diğer sebeplere karşı üstün tutulmamaktadır ve tutulması düşünülmemektedir**. Bu

[108] Opinion of Article 29 on the Principle of Accountability: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, s. 3.
[109] Opinion of Article 29 on the Principle of Accountability: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, s. 5-8.
[110] İlgili diğer belgeler için, bkz. Opinion of the Data Protection Supervisor on the data protection reform package; https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, s. 28.

durum oldukça önemlidir çünkü rızanın genel kural diğerlerin istisna olarak düzenlenmesi halinde, diğer sebeplerin son derece kısıtlı uygulanması gerekecektir.

İkinci olarak organizasyonların meşru amaçlarının veri işlemeye dayanak olabileceğine ilişkin bir düzenleme bulunmamaktadır. Bu, veri işleme bazlı geliştirme çalışmaları ve araştırmalarda gereken ancak kullanıcının bilgilerini doğrudan ifşa etmeyen veriler (çıkış bilgileri (log out)) açısından önemlidir.

Ayrıca rızanın temel kural olması halinde internet hizmetleri ekosistemlerinin tamamında kullanıcıların kimliklerinin her zaman belirlenmiş olduğu bir sistem doğabilecektir. Bu hüküm inovasyonu engellediği gibi, AB çapında kabul edilemez bir durum yaratabilir. Tasarı'da tercih edilen kavram olan *"açık rıza"* kavramının "informed consent" şeklinde değerlendirildiğini kabul ederek; mevcut hükmün aşağıdaki şekilde değiştirilmesinde fayda bulunmaktadır:

Kişisel Verilerin İşlenme Şartları

Madde 5- (1) Kişisel veriler sadece şu şartlarda işlenebilir:

a) Kanunlarda açıkça öngörülmesi,
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
d) Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması,
e) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
g) İlgili kişinin veri işleme amaçlarına yönelik bilgilendirilmiş rızasını vermesi,
h) İşlemenin sorumlu ya da diğer üçüncü kişilerce güdülen meşru amaçlar için gerekli olması halinde ve söz konusu amaçların ilgili kişinin kişisel verilerinin korunmasını gerektiren temel hak ve özgürlükleri ile çatıştığı haller saklı kalmak kaydıyla.

2.3.10. Kişisel verilerin aktarılması

Tasarının 8. maddesinde, kişisel verilerin yurtiçinde üçüncü kişilere aktarılması ile yurtdışına aktarılması arasında bir ayrım yapılmamıştır. Ancak her iki grup için, veri koruması ve özel hayatın gizliliği ile ilgili kaygılar farklıdır. Tasarı md. 8/f.1 ve 5'in lafzı her ne kadar hem

üçüncü kişilerle veri paylaşımı hem de yurt dışına veri transferine ilişkin gözükse de; maddenin diğer hükümleri dikkate alındığında bu düzenlemenin veri paylaşımı ile ilgili olmadığını, uluslararası aktarımla ilgili olduğunu belirtmek gerekmektedir. Bu maddenin konusunun uluslararası veri aktarımları olup verilerin paylaşılması olmadığı düşünülmektedir. Bu gerekçelerle Tasarı md. 8'in aşağıdaki şekilde tekrar ele alınmasında fayda bulunmaktadır:

Madde8 – (1) Bu kanunun kişisel verilerin işlenmesine ilişkin şartları bunların Türkiye dışına aktarılması bakımından da ayrıca aranır.

(2) Kişisel veriler, aşağıdaki şartlarından en az birinin bulunması halinde yurtdışına aktarılabilir:
a) Yabancı ülkede ya da yabancı ülkede bulunan faaliyet alanında yeterli koruma bulunması halinde aktarım yapılabilir. Kurul yeterli koruma bulunan ülkeleri tespit ve ilan eder. Avrupa Ekonomik Alanına dahil olan ülkelere veri transferinde bu koşul aranmaz.

b) İlgili kişinin aktarımla ilgili bilgilendirilmiş rızasını vermesi halinde aktarım yapılabilir.

c) Aktarım yapacak veri sorumlusu ya da işleyenin aynı grubun kontrolünde yer alan ve onların alt işleyenleri olan tüzel kişileri de kapsayan yeterli güvenlik önlemlerini kanıtlamaları halinde aktarım yapılabilir.

d) Veri sorumlusu ya da işleyenin kendi kontrolleri dışındaki üçüncü kişilere veri aktarımı yapmalarına rağmen yine de bu kanunla uyumlu olan yeterli koruma önlemleri bulunduğunu ispatlamaları halinde aktarım yapılabilir.

(3) Kurul ilgili kamu kurum ve kuruluşları ile diğer kişilerin görüşlerini alarak ve aşağıdaki şartların varlıklarını değerlendirerek bir ülkenin yeterli korumaya sahip olup olmadığını belirler:

a) Türkiye'nin taraf olduğu uluslararası sözleşmeler,

b) Kişisel verilere ilişkin taleplere ilişkin olarak Türkiye ile diğer ilgili ülke arasında karşılıklılık bulunması,

c) Veri aktarımına ilişkin uygulanabilir korumalar, süre, amaç ve verinin kalitesi,

d) Kişisel verilerin transfer edileceği ülkenin ilgili mevzuatı,

e) Uluslararası aktarımın gerçekleşeceği sektör veya bölgeye ilişkin kanıtlanmış güvenlik önlemleri.

2.3.11. Veri Sorumlusunun Aydınlatma Yükümlülüğü

Tasarı md. 9/f.1 AB Veri Koruması Direktifi ile uyumlu bir şekilde veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğünü düzenlemektedir.

Tasarı md. 9/f.2 ise; veri sorumlusunu, verileri üçüncü kişilerden alsa dahi, ilgili kişiyi bilgilendirmekle yükümlü kılmıştır. Bu durum AB'nin mevcut ya da taslak aşamadaki düzenlemeleriyle uyum göstermemektedir.

İlgili kişiden doğrudan toplanmayan verilere ilişkin bilgilendirme yükümlülüğüne dair 95/46 sayılı direktifin benimsediği orantılı yaklaşımın benimsenmesi önerilmektedir. Ayrıca bu durum veri tabanlı geliştirme çalışmalarını aksatabilir. Bu hükmün yorumunda orantılılık ilkesi büyük önem taşımaktadır. Bu nedenle; uygulamada ortaya çıkabilecek sorunları bir nebze olsun önleyebilmek adına; kişisel verilerin ilgili kişi dışında başka kaynaklardan elde edilmesi halinde veri sorumlusunun "uygulanabilir ve mümkün olması halinde" ilgili kişiye birinci fıkradaki bilgileri vereceğine ilişkin bir ekleme yapmak faydalı olacaktır. Orantılılık ilkesi çerçevesinde veri sorumlusunun bilgi verme yükümlüğünün değerlendirilmesi gerekmektedir. Bilgi vermenin veri sorumlusu için aşırı külfetli veya masraflı olacağı durumlarda bu hüküm, veri koruması yönetişimi açısından kurtarıcı nitelikte olacaktır. Aksinin kabulü yine veri odaklı inovasyona ters sonuçlar doğurabilecektir. Bu gerekçelerle md. 9/f.2 hükmüne aşağıdaki şekilde bir ekleme yapılmasını öneriyoruz:

> *MADDE 9 - (2) Kişisel verilerin, ilgili kişi dışındaki kaynaklardan edinilmesi hâlinde de veri sorumlusu, uygulanabilir ve mümkün olması halinde, ilgili kişiye birinci fıkradaki bilgileri verir.*

2.3.12. Kişisel Verilerin İşlenmesi ve İfade Özgürlüğü

Tasarı'da ne Kişisel verilerin işlenmesini tanımlayan md. 3/d hükmünde ne de "İstisnalar"'ı düzenleyen 22. Madde de açıkça ifade özgürlüğünden bahsedilmektedir. 22. Madde sadece "c" bendinde; kişisel verilerin, bu Kanunda belirtilen genel ilkelere, veri güvenliğine ilişkin tedbirlere ve mesleki davranış kurallarına uygun olarak *basın özgürlüğü çerçevesinde* işlenmesi halinde, veri koruması kanun tasarısı hükümlerinin uygulanmayacağını öngörmektedir. Oysa sadece habercilik amacına değil, daha geniş haklara ve amaçlara atıf yapan AB Veri Koruması Direktifi md. 9'a ve AB Temel Haklar Bildirgesinin ilgili maddelerine atıfta bulunacak ve aynı zamanda Tasarı'yı AB Direktifi ve Regülasyonu ile aynı çizgiye taşıyacak ifade özgürlüğüne ilişkin bir maddenin Tasarı'da yer alması önem taşımaktadır. Bilişim perspektifinden baktığımızda bu tür bir madde erişim sağlayıcılar, arama motorları ve sunucu hizmet sağlayıcıları gibi aracı/online platformları üçüncü kişilerin fiilleri dolayısıyla meydana gelen olaylardan sorumlu olmaktan kurtaracaktır. Her ne kadar iç

hukukumuzda 5651 Sayılı Kanun ve hali hazırda Meclis genel kurulunda bulunan Elektronik Ticaret Kanun Tasarısı'nda bu yönde hükümler mevcut ise de; veri korumasına ilişkin temel düzenleme içinde de ifade özgürlüğüne atıf yapılmasının faydalı olacağını düşünüyoruz.

2.3.13. Co-regulation (Codes of Conduct)

Tasarı'da yer verilmesinin son derece önemli olduğunu düşündüğümüz bir diğer konu ise co-regulation'dır. Yasal düzenlemeler genel çerçeveyi çizdikten sonra, bu temel kurallar içinde hareket etme, veri koruması standartlarını uygulama esnekliğini ve içinde bulundukları sektör spesifik kuralları oluşturma özgürlüğünü sektörlere tanımalıdır. Bu hem özel sektörün kendi gereksinim ve isterleri özelinde kendisini regüle etmesini sağlayacak ve hem de Veri Koruması Kurulu'nun etkinliğini artıracaktır[111].

2.3.14. İlgili Kişinin Hakları

Tasarı md. 10, AB düzenlemelerinden iki noktada farkla ilgili kişinin haklarını düzenlemektedir. İlk olarak; md. 10/g hükmü; işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etmek hakkını ilgili kişiye vermektedir. Ancak burada kanaatimizce yine orantılılık ilkesi çerçevesinde bir değerlendirme yapılmalıdır.

İkinci olarak; md. 10/ğ hükmünde ilgili kişinin verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep edeceği öngörülmektedir. Bu tür bir tazminat veya zararın giderilmesi hükmü AB düzenlemelerinde yer almadığı için, hükmün tekrar değerlendirilmesinde fayda olacağı önerilmektedir. Hukukun genel kurallarına göre ilgili kişinin tazminat talep etme hakkı birçok yasal düzenlemede mevcuttur. Yine bu hüküm çerçevesinde aracı hizmet sağlayıcıların da yaptıkları işin doğası gereği tazminat

[111] Bu noktada başarılı bir örnek olarak Filipin Veri Koruması Yasası örnek olarak verilebilir: Cumhuriyet Kanunu No. 10173 (Filipin Veri Mahremiyet Kanunu) Madde 7j(j) kişisel bilgi denetçilerince ihtiyari olarak bağlanan mahremiyet kurallarını gözden geçirmek, onaylamak, reddetmek veya değişiklik talepetmek: mahremiyet kuralları işbu Kanun tahtında düzenlenen veri mahremiyeti prensiplerine bağlı kalması kaydıyla: bu tür mahremiyet kuralları dahil olan herhangi bir kişisel bilgi denetçisine karşı yapılacak şikayet başvuruları için özel uyuşmazlık çözüm yolları içermesi kaydıyla. Bu amaçla, Komisyon işbu Kanunda belirlenen standartları uygulayan mahremiyet kurallarının belirlenmesi ve idaresi sırasında kişilere, kuruluşlara, iş faaliyetlerine ve iş alanlarına göre bu kanun gereğince düzenleme yapmaya yetkili ilgili düzenleyici birimlere danışmalıdır: Nihai olarak Komisyon bu tür mahremiyet kurallarını gözden geçirebilir ve işbu Kanunla uyum sağlamak amacıyla ilgili değişiklikleri talep edebilir.

sorumluluklarının söz konusu olmayacağını her ne kadar 5651 Sayılı Kanun ve e-ticaret yasa tasarısı teyit ediyorsa da, burada bir kez daha vurgulamak isteriz.

2.3.15. Veri Koruması Kurulu

Tasarı'nın 18-21. Maddeleri, Tasarıda çizile hukuki çerçeve itibariyle kişisel verilere ilişkin görevleri yerine getirecek olan Kişisel Verileri Koruma Kurulu'na ilişkindir. Her ne kadar Kurulun, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, *bağımsız olarak yerine getireceği ve kullanacağı ifade ediliyorsa* da; md. 18/f.3'te Kurulun her türlü gideri, Adalet Bakanlığına bağlı Kişisel Verileri Koruma Genel Müdürlüğünün bütçesinden karşılanacağı belirtilmiştir. AB Veri Koruması Direktifi'nin önemini ısrarla vurguladığı veri koruma otoriteleri için "tam bağımsız" olarak çalışma kriteri açısından yaklaşıldığında, Kurulun sonradan kendi bütçesini oluşturma ve harcamalarını kendisi karşılaması yeteneğine kavuşması tam bağımsızlığı açısından önem taşımaktadır. Bu açıdan ikinci sorun ise Kurulun yapısına ilişkin olarak karşımıza çıkabilecektir. Tasarı md. 20/f.1 hükmüne göre; 7 üyeden oluşacak olan Kurulun dört üyesi Bakanlar Kurulunca seçilmektedir. Bu formülasyonun siyasi otoritenin etkisine açık bir Kurul yaratacağı şeklinde kaygılar oluşabileceğinden, seçim şekli ve yönteminin Ek 3'te yer alan bilgiler çerçevesinde yeniden değerlendirilmesi önerilmektedir[112].

2.3.16. İstisnalar

Tasarı açısından üzerinde tekrar durulması gereken diğer bir önemli nokta ise; md. 22/ç,d ve e bentlerinde yer verilen ve kamuya hemen her türlü amaçla son derece geniş bir kişisel veri işleme yetkisi veren hükümlerdir. Bu durum Tasarısı'nın daha ilk hükmü ile yani amacı ile çelişmektedir. Tasarı bireyi, kuruluşlara karşı korumak için, şirketlere kısıtlamalar getirmekte, oysa aynı dengeyi birey-devlet arası ilişkide gözetmediği için, AY md. 20/f.3'de veri korumasını temel bir insan hakkı olarak düzenlemenin ruhuna ters düşmektedir. Kamuya getirilen geniş istisnaların orantılılık ilkesinde yeniden düzenlenmesi ve kişisel verilerin korunmasına ilişkin düzenlemelerin özel sektör ve kamuya eş uzaklıkta durmasında fayda bulunmaktadır.

[112] Bkz. EK.3: AB Nezdinde "Güvenilir Ülke" Statüsünün Kazanımı: Bağımsız Bir Veri Koruma Otoritesinin Önemi.

2.3.17. Aracı Hizmet Sağlayıcı ve Sorumluluk Rejimi

Aracı hizmet sağlayıcı ve sorumluluk rejimi, Tasarı'da yer almayan ancak halihazırda Meclis Genel Kurulunda bulunan Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı'nda, Digital Millennium Copyright Act ve 5651 Sayılı Kanun paralelinde düzenlenen bir konudur. E-Ticaret Kanun Tasarısının Tanımlar başlıklı 2. maddesi aracı hizmet sağlayıcı'yı: *"Elektronik ticaret faaliyetlerini sürdürmeleri amacıyla kullanıcılarına elektronik iletişim araçları vasıtasıyla iletişim, sipariş verme, içerik ve ilan yayınlama, ödeme, tanıtım, pazarlama gibi hizmetleri sunan gerçek ve tüzel kişileri"* ifade eder şeklinde tanımlamakta ve aracı hizmet sağlayıcının sorumluluğuna ilişkin olarak ise; 9. Maddesinde: "Aracı hizmet sağlayıcılar, hizmet sundukları elektronik ortamı kullanan gerçek ve tüzel kişiler tarafından sağlanan içerikleri kontrol etmek veya bu içerik veya içeriğe konu mal ve hizmetle ilgili hukuka aykırı bir faaliyetin veya durumun söz konusu olup olmadığını araştırmakla yükümlü değildir" şeklinde düzenleme getirmektedir.

2.3.18. Cezai Hükümler

Tasarı'nın 16. maddesi veri korumasına ilişkin suçları düzenlemektedir. Maddenin 1. fıkrası *"kişisel verileri ele geçiren, kaydeden, bir başkasına veren veya yayanlar ya da yok etmeyenler"*in hürriyeti bağlayıcı cezalandırılacağını düzenleyerek, TCK'ya atıfta bulunmaktadır.

Maddenin 2. fıkrası ise kişisel verilerin yalnızca kaydedilmesinin değil, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, elde edilebilir hale getirilmesi, sınıflandırılması, kullanılmasının engellenmesi ve üçüncü kişilere aktarılmasının da TCK'nın 135. maddesine göre cezalandırılması öngörülerek, bir nevi, TCK'nın 135. maddesinin uygulama alanı genişletilmekte ve yeni hukuka aykırı fiiller için de hürriyeti bağlayıcı ceza öngörülmektedir. 3. fıkra ise; kişisel verileri silmeyen veya anonim hale getirmeyen veri sorumlusunun altı aydan bir yıla kadar hapis cezası ile cezalandırılacağını düzenleyerek yeni bir hürriyeti bağlayıcı ceza getirmektedir.

Ticari ve ekonomik konularda getirilen bu tür hürriyeti bağlayıcı cezalar, gerek Türk ve yabancı yatırımcılarının ilgili ticari konuyu riskli olarak değerlendirerek yatırımlarını farklı alanlara ve hukuk ikliminin yabancı yatırımcı için cazip olduğu ülkelere kaydırmasına olabilecektir. Yabancı sermayenin ve yatırımın teşvik edilmesi için, Tasarıda belirtilen diğer suçların yaptırımının hürriyeti bağlayıcı ceza yerine para cezası olarak belirlenmesinin uygun olacağı düşünülmektedir.

AB Veri Koruma Direktifi, ülkelerdeki veri koruma kanununun ihlali sonucu zarara uğrayanların, veri sorumlusundan ilgili zararı tazmin edebilmesi ile ilgili üye ülkelerin düzenleme yapmaları gerektiğini söylemekte; ihlal sonucu verilecek cezaları da ülkelerin belirleyeceğini belirtmektedir. Yeni Regülasyon taslağı da, Direktif ile benzer şekilde, zarara uğrayanların veri sorumlusundan ilgili zararı tazmin edebilmesi gerektiğini belirtmekte, aynı zamanda ülkelerin veri koruma otoriteleri tarafından verilecek idari para cezalarını düzenlemektedir. Ancak 1 Milyon Avroya ve şirketin global cirosunun %2'sine kadar çıkabilen cezalar oldukça yüksektir. İlgili idari para cezalarının bu şekilde yürürlüğe girip girmeyeceği henüz belli değildir.

Günümüzde, AB çapında, veri koruma kanunlarında hürriyeti bağlayıcı ceza öngörmeyen ülkeler bulunmakta, öngören ülkelerde de pratikte hürriyeti bağlayıcı ceza verilmesine oldukça ender olarak rastlanmaktadır.[113] Örneğin İngiltere Veri Koruma Kanununda, verilerin hukuka aykırı olarak kaydedilmesi de dahil olmak üzere, kişisel verilerin korunması ihlalleri ile ilgili olarak para cezası düzenlenmiş, hürriyeti bağlayıcı ceza öngörülmemiştir. Benzer şekilde İrlanda da veri koruma kanununda, kişisel verilerin korunması ihlalleri ile ilgili olarak para cezası düzenlemiş durumdadır.

Malum olduğu üzere, İngiltere ve İrlanda gibi ülkeler, oldukça yüksek oranda bilişim ve teknoloji yatırımı çekebilmekte ve ülke içindeki yatırımcı ve girişimcilerin de bu sektörlere yönlenmesini sağlayabilmektedir. Birçok yabancı bilişim şirketi, Avrupa alanındaki merkezlerini İrlanda'ya taşımakta ve İrlanda'yı bilişim sektöründe Avrupa'nın önemli ülkelerinden biri konumuna getirmektedir.

[113] Bullesbach, A., et al (ed). (2010) "Concise European IT Law". s.110.

3. SONUÇ

Bu raporda kişisel verilerin korunmasına ilişkin hukuki düzenlemeler ekonomik ve hukuki perspektiften tartışılmıştır.

Kişisel verilerin korunması Anayasa'yla düzenlenmiş temel bir insan hakkıdır. Ayrıca bu konuda iç hukukumuzda çeşitli kanunlarda dağınık hükümler bulunmaktadır. Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın yürürlüğe girmesiyle, hem Anayasa'da işaret edilen bireyin temel bir hakkı daha somutlaşmış olacak hem de diğer kanunlardaki hükümlerin uygulanmasında yaşadığımız sorun ve sıkıntılar giderilmiş olacaktır.

Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın yasalaşmasının ekonomimize en önemli faydalarından biri; kişisel verilerin korunmasına dair AB standartlarının karşılanması halinde, ülkemizin AB nezdinde veri gönderimi güvenli ülke statüsü kazanması olacaktır. Böylece, gerek yurtdışında operasyonları olan Türk şirketlerinin, gerekse Türkiye'de operasyonları olan yabancı şirketlerin veri transferinde aldıkları izinlere ilişkin önemli bir maliyet tasarrufu sağlanacaktır. AB nezdinde bu statüye kavuşabilmemiz için kişisel verilerin korunmasına ilişkin uygulamayı Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nda çizilen çerçevede yürütecek idari kurumun tamamen bağımsız olması temin edilmelidir.

Kişisel verilerin korunmasına dair yasal düzenlemeler yapılırken; kişisel verilerin korunmasının tüm dünyada tartışılan ve teknolojinin gelişimine bağlı olarak hızla evrilen bir hukuki alan olduğu dikkatten kaçırılmamalıdır. Büyük veri teknolojilerinin tüm ekonominin verimliliğini ve tüketicilerin faydasını artıracak yeni fırsatlar ortaya çıkarması, kişisel verilerin korunmasına ilişkin kanuni düzenlemelerin önemini artırmıştır. Veri işlenmesine ilişkin teknolojilerin hızlı gelişimi, temelinde verinin yer aldığı İnternet'in hayatımızın merkezine yerleşmesi, kişisel verilerin korunmasına ilişkin hukuki çerçevenin hem önemini artırmakta, hem de ekonominin tüm aktörlerini dikkate alan dengeli bir yaklaşımla oluşturulmasını zorunlu kılmaktadır. Tasarıya ilişkin önerilerimizde de vurguladığımız üzere; temel insan haklarından biri olan veri koruması hakkının, bireyin Anayasa'da tanımlanan diğer ilgili hak ve özgürlükleri ile birlikte ele alınması, orantılılık ilkesi ışığında gerek devlet gerek özek sektör karşısında bireye bir hukuki himaye sağlanması, bu hukuki korumanın verilerden katma değerli hizmetler geliştirilmesini sağlayacak, bireyin hayatına teknolojinin girmesine engel olmayacak, ağ ekonomisini, veri odaklı inovasyonu teşvik edecek ve özellikle bilgi toplumun köşe taşlarından olan aracı hizmet sağlayıcıların sorumlulukları noktasında

temel ilkelerden farklılaşan uygulamalara yol açmayacak doğrultuda değerlendirilmesi gerekecektir.

Ülkemizde de kişisel verilerin korunmasına dair kanunun, bireyin haklarını korurken, gelişen teknolojilerin sağladığı ekonomik fırsatları kısıtlamayacak ve inovasyonun önünü açacak sade bir çerçeve kanun niteliğinde bir an önce kanunlaştırılmasında fayda bulunduğunun altını önemle çizmek isteriz.

Referanslar ve Kaynakça

[1] American Chamber of Commerce to the European Union. (2012) "AmCham EU position on the General Data Protection Regulation"

[2] Article 29 Working Party. (1998) "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive"

[3] Article 29 Working Party. (2010) "Opinion 3/2010 on the principle of accountability"

[4] Barua, A., Mani, D. ve R. Mukherjee. (2011) "Measuring the Business Impacts of Effective Data". *University of Texas*

[5] BCG. (2012). "The Internet Economy in the G-20".

[6] BCG. (2013). "Follow the Surplus: European Consumers Embrace Online Media".

[7] BCG. (2013). "Follow the Surplus: How U.S. Consumers Value Online Media".

[8] Bensinger, G. (2014). "Amazon Wants to Ship Your Package Before You Buy It"

[9] Bhaskaran, V. "Online Research: A Handbook for Online Data Collection". *Survey Analytics, Issaquah, WA, USA*. 2005.

[10] Brynjolfsson, E. vd. (2011). "Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?" *Working Paper.*

[11] Bullesbach, A., et al (ed). (2010) "Concise European IT Law".

[12] Capgemini Consulting. (2013). "The Open Data Economy: Unlocking Economic Value by Opening Government and Public Data".

[13] Cate, F. ve M. Staten. (2001). "Protecting Privacy in the New Millenium: The Fallacy of "Opt-In"."

[14] Center for Democracy & Technology. (2012) "CDT Analysis of the Proposed Data Protection Regulation".

[15] Christensen, L. vd. (2013). "The Impact of Data Protection Regulation in the EU".

[16] Copenhagen Economics. (2012). "Online Intermediaries".

[17] Danish Enterprise and Construction Authority. (2010). "The Value of Danish Address Data".

[18] Del Aguila-Obra, A. ve A. Padilla-Melendez. (2006). "Organizational Factors Affecting Internet Technology Adoption". *Internet Research.*

[19] Eğitim Reformu Girişimi. (2013). "Fatih Projesi Eğitimde Dönüşüm için bir Fırsat Olabilir Mi?"

[20] Erixon, F. Vd. (2013). "EU Policies on Online Entrepreneurship: Conversations with U.S. Venture Capitalists". *ECIPE.*

[21] European Commission, IP/10/1430, "Data Protection: Commission to refer Austria to Court for lack of independence of data protection authority

[22] Evans, P. C. & M. Annunziata. (2012). "Industrial Internet: Pushing the Boundaries of Minds and Machines"

[23] Executive Office of the President of the USA. (2014). "Big Data: Seizing Opportunities, Preserving Values".

[24] Frontier Group. (2009). "California Budget Transparency 2.0"

[25] GigaSpaces (2013). "Real-Time Stream Processing and Cloud-Based Big Data Increasing in Today's Enterprises".

[26] GTM Research (2013). "The Soft Grid 2013-2020: Big Data & Utility Analytics for Smart Grid".

[27] Hustinx, P. (2012). "Opinion of the European Data Protection Supervisor on the data protection reform package"

[28] IAB Basın Bülteni. (2014)

[29] Intel IT Center. (2013). “Big Data in the Cloud: Converging Technologies”. *Intel Solution Brief.*
[30] Isley, S.C. (2013). “Opt-In, Opt-Out; Why Not Forced Choice?” *Rand Blog.*
[31] Industry Coalition for Data Protection. (2012) “Paper on Proposals for a ‘New EU Legal Framework on Data Protection”
[32] International Association of Privacy Professionals. (2011) “Data Protection Authorities 2011 Global Survey”
[33] Jappelli, T. ve M. Pagano. (2005). “Role and Effects of Credit Information Sharing”. *Centre for Studies in Economics and Finance.* Working Paper No: 136.
[34] Johnson, E.J. v.d. (2002). “Defaults, Framing and Privacy: Why Opting In-Opting Out?” *Marketing Letters.*
[35] KMPG. (2013). “Bulut Bilişim ve Bankacılık Sektörü”. *KPMG Gündem.*
[36] Komorowski, M. (2012). “A History of Storage Cost”.
[37] Mani, D. vd. (2010). “An Empirical Analysis of the Impact of Information Capabilities Design on Business Process Outsourcing Performance”. *MIS Quarterly*. 34(1).
[38] McAfee, A. ve E. Brynjolfsson. (2012). “Big Data: The Management Revolution”. *HBR.*
[39] McDonald, A. ve L. Cranor. (2008). “The Cost of Reading Privacy Policies”. *Journal of Law and Policy for Information Society.*
[40] McKinsey Global Instituite. (2013). “Open Data: Unlocking Innovation and Performance with Liquid Information”
[41] McKinsey Global Institute. (2011). “Big Data: The Next Frontier for Innovation, Competition and Productivity”.
[42] McKinsey Insights&Publications. (2012). “Navigating a Changing Health Care Environment: An Interview with Pfizer’s Kristin Peck”.
[43] McKinsey. (2013). “Bilgi Toplumu Stratejisinin Yenilenmesi Projesi İhtiyaç Tespiti ve Öneriler Raporu”.
[44] Mettler, A. ve A. D. Williams. (2012). “Wired for Growth and Innovation”. *Lisbon Council Policy Brief.*
[45] MICUS. (2009). “Assessment of the Re-use of Public Sector Information”.
[46] Moore, G.E. (1965). “Cramming More Components Onto Integrated Circuits”. *Electronics Magazine.*
[47] National System Research Institute for Policy Research. (2012). “Economic Impact of September 9th Power Outage”. *Policy Brief.*
[48] Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, Kanun No: 6493, 2013.
[49] OECD. (2010). “The Economics of Personal Data and the Economics of Privacy”. *OECD Background Paper.*
[50] OECD. (2013). "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data" ". *OECD Digital Economy Papers.* 222
[51] Open Data Portal. (2012). “Characterization Study of the Infomediary Sector”. *Annual Report*
[52] Posner, R. (1978). “The Right of Privacy”. *Georgia Law Review*. 12(3).
[53] Sökmen, A. (2014). “İnternette Yeni Bir Fırsat Şimdi Bulut Bilişime Kafa Yorma Zamanı!” *TEPAV Politika Notu.*
[54] Staten, M. ve F. Cate (2003). “The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA”. *Duke Law Journal.* 52:745

[55] Stigler, G. (1980). "An Introduction to Privacy in Economics and Politics". *Journal of Legal Studies.* 9(4).
[56] T.C. Başbakanlık. (2010). "T.C. Başbakanlık (2011-2015) Stratejik Planı".
[57] T.C. Cumhurbaşkanlığı Devlet Denetleme Kurumu. (2013) "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları".
[58] TBB. (2014). Mobil Bankacılık İstatistikleri.
[59] TC Kalkınma Bakanlığı. (2013). "Bilgi Toplumu Stratejisinin Yenilenmesi Projesi".
[60] Tene, O. ve J. Polonetsky. (2012). "Privacy in the Age of Big Data: A Time for Big Decisions". *Stanford Law Review.*
[61] Schütz, P. (2012) "Comparing formal independence of data protection authorities in selected EU Member States"
[62] Varian, H. (1996). "Economic Aspects of Personal Privacy".
[63] Vickery, G. (2011). "Review of Recent Studies on PSI Re-use and Related Market Developments". *Information Economics.*
[64] Widjaya, I. (2011). "Cloud Computing Allows Big Business to be as Nimble as Small Business". *Cloud Business Review.*
[65] World Economic Forum. (2013). "Unlocking the Value of Personal Data: From Collection to Usage". *Industry Agenda*
[66] Yun S. ve S. Pearson. (2011). "Privacy Enhancing Technologies: A Review". *HP Laboratories.*
[67] Zhu, K. v.d. (2003). "Electronic Business Adoption by European Firms: A Cross-Country Assessment of the Facilitators and Inhibitors". *European Journal of Information Systems.* 12.
[68] Zhu, K. v.d. (2006). "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on e-Business". *Management Science.* 52(10).

EK-1: Avrupa Birliği Bakanlığı'nın Tasarı ile ilgili Resmi Olmayan Görüşü

2010 Anayasa Değişikliği ile Anayasa'nın "Özel Hayatın Gizliliği" başlıklı 20. maddesi değiştirilerek, bireylere kişisel verilerin korunmasını isteme hakkı tanınmış, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme madde kapsamına alınmıştır.

Her ne kadar, Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümü altında 1 Haziran 2005 tarihinde yürürlüğe giren Türk Ceza Kanununun 135 ve devamı maddelerinde; kişisel verilerin hukuka aykırı olarak kaydedilmesi, yayımlanması, başkalarına aktarılması suç haline getirilmişse de, kişisel verilerin korunması hukukunun tüm ilke ve kurumlarıyla hayata geçirilebilmesi için başka yasal düzenlemelere de ihtiyaç bulunmaktadır Sadece, 2002/58/AT sayılı direktife paralel şekilde Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, 28363 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Demokratikleşme Paketi kapsamında Kişisel Verilerin Korunması Kanunu Tasarısının yasalaşması öngörülmüş olup, bu konudaki çalışmalar sürdürülmektedir.

Kişisel verilerin korunmasına yönelik Kanun Tasarısı Taslağının kabul edilerek bu alanda genel hukuki çerçeveyi oluşturan bir yasal düzenlemenin mevcudiyeti Sermayenin Serbest Dolaşımı (4. Fasıl) , Bilgi Toplumu ve Medya (10. Fasıl), Yargı ve Temel Haklar (23. Fasıl) ve Adalet, Özgürlük, Güvenlik (24.Fasıl) fasılları bakımından önem taşımaktadır.

Kanun Tasarısı 95/46/AT sayılı Direktif; 2006/24/AT ve 2009/136/AT değişiklikleri ile 2002/58/AT sayılı Direktif; 2001/497/AT sayılı Komisyon Kararına uygun olacak şekilde, kişisel verilerin korunması, işlenmesi ve üçüncü taraflarla ile paylaşılması hususundaki mevzuat boşluğunu giderecektir. 95/46/AT sayılı direktifle önerilen ve AB Komisyonu tarafında kendi içinde 45/2001 sayılı Tüzükle kurulan Kişisel Veri Koruma Otoritesi de kurulacaktır.

Sermayenin Serbest Dolaşımı Faslı çerçevesinde, Kara Paranın Aklanması ve Terörizmin Finansmanı ile Mücadele kapsamında da, AB Üyesi Ülkelerin Malvarlığı Geri Alım Birimleri (Asset Recovery Offices-ARO) Arasında Suçtan Elde Edilen Kazançların ve Suçla İlişkili Diğer Malvarlıklarının Tespiti ve Takibi Alanında İşbirliğine İlişkin 2007/845/JHA sayılı Konsey Kararına uyuma yönelik olarak Kişisel Verilerin Korunması Kanunu'nun çıkarılması gerekmektedir. Kişisel verilerin korunması konusu, müktesebat olarak Yargı ve Temel Haklar Faslı (23. Fasıl) kapsamında da yer almakla birlikte, Adalet, Özgürlük, Güvenlik Faslı (24. Fasıl) alanında organize suçlarla mücadele ve insan ticareti konularında da öneme sahiptir. Bu kapsamda kişisel verilerin korunmasına münhasır bir kanun olmaksızın ve Europol ile operasyonel bir işbirliği anlaşması imzalanamamaktadır.

2010 yılı Anayasa Değişikliği ile kişisel verilerin korunmasını isteme hakkı Anayasal güvenceye kavuşmuştur. Söz konusu Kanunla birlikte 2010 Yılı Anayasa değişikliğine uygun olarak, kişisel verilerin korunmasını isteme hakkına ilişkin kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usuller mevzuatla düzenlenmiş olacaktır.

Kişisel veriler, mal ve hizmetlerin ihtiyaca uygun üretimi ve dağıtımı için çok önemli bir kaynaktır. Mal ve hizmet üreten ve dağıtan gerçek ve tüzel kişiler bu kaynaktan etkin bir şekilde istifade edebilmelidir. Tasarının etki ettiği birinci grup bu türde gerçek ve tüzel kişilerden oluşmaktadır. Hakkında kişisel verilerin toplandığı gerçek ve tüzel kişiler ise tasarının etki ettiği ikinci grubu oluşturmaktadır. Kişisel verilerin gelişigüzel bir biçimde toplanıp ve açıklanması durumunda, bu ikinci grubun kişilik hakları bu işlemlerden zarar görebilecektir.

Tasarı bu iki grubun çıkarlarını koruyarak dengeleyerek ve kişisel hak ve hürriyetleri koruma altına alacaktır.

Tasarı kişisel verilerin, bazı istisnai haller hariç, sadece kişinin rızası neticesinde işlenebilmesini öngörmektedir. Ayrıca ırk, siyasi düşünce ve felsefi inanç gibi özel niteliği olan verilerin işlenmesini de yasaklamaktadır.

EK-2: Sektörün Bakışı: TÜBİSAD ve TÜSİAD Görüşleri

Tasarının kanunlaşması ile bilişim sektörü de yakından ilgilenmektedir. Özellikle kişisel verilerin korunması konusunda AB seviyesinde bir kanun olmaması sonucu AB ile kişisel veri transferi yapamamamız durumunun, AB şirketlerinin birçok konuda Türkiye'deki bilişim şirketlerinden dış kaynak temin etmelerinin önünde büyük bir engel oluşturması, uzun süreden beri sektörü etkileyen bir durumdur.

Konu ile ilgili TÜBİSAD Bilişim Sanayicileri Derneğinin görüşü, sektörün konuya yaklaşımını anlamak açısından önem teşkil etmektedir. Kişisel verilerin korunması konusunda TÜBİSAD'ın görüşü şu şekildedir;

Kişisel verilerin korunması konusunda ülkemizde yaşanan düzenleme eksikliği, bilgi toplumuna giden yolda sektörümüzün ve ülkemizin en önemli eksikliklerinden birini oluşturmaktadır. Dünyada "veri temelli ekonomi- data driven economy" kavramı tartışılmakta, bilgi ekonomisi olma yolunda "verileri işleme" ile ilgili açık bir yasal mevzuata sahip olmayan ülkeler rekabetçilerini giderek kaybetmektedir.

Türkiye bilgi ve iletişim teknolojileri sektöründe son yıllarda yaptığı atılımlarla çok önemli bir mesafe almıştır. Sektörün kendisi geliştiği gibi diğer sektörlere de küresel düzlemde rekabetçi olmaları yolunda önemli bir katkı sağlamaktadır. Sektörün büyüme hızı ve "bilgi ekonomisinde" motor güç olması noktasındaki konuma maalesef istenilen düzeyde değildir. Bunun birçok kurumsal sebebi olmasının yanında en temel nedenlerinden birinin Türkiye'nin "kişisel verilerin korunmasına" ilişkin açık ve Avrupa Birliği ile uyumlu bir düzenleme çerçevesine sahip olmaması gösterilebilir.

Türkiye'de kurumsal birçok şirket yurtdışı iştirakleri başta olmak üzere tüm alt yapılarını Türkiye'de kurdukları IT sistemleri üzerinden yönetmek istemektedirler. Bunun yanında çağrı merkezi, içerik dağıtım ağları – CDN, bulut servisleri, e-ticaret uygulamaları gibi birçok katma değerli servisin de Türkiye'den sunulması noktasında çok güçlü bir irade ve niyet bulunmaktadır. Türkiye bölgesinde finansal merkez olma ve finans sektörünün kalbi olan finans sektörüne yönelik IT servislerini de Türkiye merkezli olarak sunmak istemektedir. Türkiye mevcut insan gücü ve teknolojik alt yapısıyla Türkiye merkezli olarak sunulacak birçok IT servisine de ev sahipliği yapabilme potansiyeline sahiptir.

Yukarıda belirtilen tüm bu hedeflerin hayata geçirilmesinde en önemli engel Türkiye'nin "kişisel verilerin korunması" konusunda yeterli düzeyde koruma sağlayan bir mevzuata sahip olmaması, Avrupa Birliği düzenlemeleri kapsamında uluslararası veri transferi bakımından "güvensiz ülke" sayılmasıdır. Bunu aşmak için ilk adım Avrupa Birliğinin belirlediği esaslara uygun "Kişisel Verileri Korunması Hakkında Kanun Tasarısı"nın bir an önce yasalaşması olacaktır.

Tasarı uzun süredir Yasalaşmayı beklemektedir. Dünyanın "veri temelli ekonomiye" geçtiği, "mahremiyete saygılı ürün geliştirmenin – privacy by design" uluslararası rekabetin bir parçası yapıldığı bir dünyada, "kişisel verilerin korunmasına" ilişkin düzenlemesi ve bu yönde bir pratiği olmayan bir ülkenin küresel rekabetin dışında kalacağı da yadsınamaz bir gerçektir. Türkiye bu alanda bir an önce bir düzenlemeye kavuşmalı, düzenlemenin çerçevesi ve uygulama sektörün ihtiyaçları- bireylerin mahremiyet hakları- başta Avrupa Birliği olmak üzere uluslararası hukukun temel normlarına uygun bir kapsamda gelişim göstermelidir.

Türk Sanayici ve İşadamları Derneği (TÜSİAD) da, "Bilgi Toplumu Stratejisi Güncelleme Çalışmaları Hakkında TÜSİAD Görüş ve Önerileri"nde, kişisel verilerin korunması kanununun gerekliliği ve önemine vurguda bulunmuş ve yapılacak düzenlemede hangi noktalara önem verilmesi gerektiğine dikkat çekmiştir. TÜSİAD'ın konuyla ilgili görüşü şu şekildedir;

- Kişisel verilerin korunması alanında yapılacak yeni düzenlemelerde konu ile ilgili mevcut düzenlemelere dikkat edilmesi, kanunlar arası ihtilaf durumuna yol açılmaması, farklı düzenlemelerde farklı kişisel veri tanımına yer verilmemesi, sektör spesifik alanlardaki mevcut düzenlemelerin genel hukuki çerçeveyle uyumlu olması gereklidir.

- Kişisel verinin işlenmesi ve saklanması açısından kritik kamu ve özel kurumlarda "privacy officer" gibi roller barındırılmalı ve bu rollere sahip kişilerden ortak bağımsız bir grup oluşturarak, iyi uygulamalar, yeni yaklaşımlar ve stratejiler, sinerjik kararlar, sektör ve uygulama standartları oluşumu gibi konularda yararlanılmalıdır.

- Kişisel verilerin üzerinde tutulduğu / tutulacağı ortamlara yönelik düzenli olarak zayıflık ve sızma testlerinin yapılması ve sonuçlarının bağımsız / üst düzey bir otoriteye raporlanarak, aksiyonlarının takip edilmesinin sağlanması önemlidir. Kişisel

verilerin üzerinde barındırıldıkları sistemlerin felaketten kurtarma ve iş sürekliliği testlerinin düzenli olarak yapılması ve sonuçlara göre sürekli iyileştirilmesi gereklidir.

• AB üyeliği perspektifiyle, kişisel verilerin korunması kanunu düzenlemesinin ve oluşturulacak kurul yapısının, AB ile Türkiye arasındaki kişisel veri transferinin önünü açması sağlanmalıdır.

• Kişisel verilerin korunması hakkında farkındalığın arttırılması ve tüketicilerin kişisel verilerin işlenmesi ile ilgili oluşabilecek yanlış algılarının düzeltilmesi için bilgilendirme çalışmalarının yapılması gereklidir.

EK-3: AB Nezdinde "Güvenilir Ülke" Statüsünün Kazanımı: Bağımsız bir Veri Koruma Otoritesinin Önemi

Türkiye ile AB arasında kişisel veri transferinin önünün açılabilmesi için Avrupa Komisyonu'nun Türkiye'nin yeterli seviyede koruma sağlayan bir ülke olduğuna dair karar vermesi gerekmektedir. Ancak Avrupa Komisyonun bu şekildeki bir kararı sonucu Türkiye ile AB arasında kişisel veri transferi yapılabilecek bir durum oluşacaktır. Komisyonun bu şekilde bir karar vermesi için de, Türkiye'nin AB standartlarında bir veri koruması düzenlemesine sahip olması gerekmektedir. Komisyonun AB ile kişisel veri transferi yapmasına izin verdiği ülkeler şu şekildedir;

Andorra, Arjantin, Avustralya, Kanada (ticari kurumlar), İsviçre, Faroe Adaları, Guernsey, İsrail, Isle of Man, Jersey, Yeni Zelanda, Uruguay ve ABD (Güvenli Liman prensipleri çerçevesinde).[114]

Ülkemizdeki AB mevzuatı çerçevesinde Tasarı ile ilgili ayrıntılı görüşlere raporun önümüzdeki bölümlerinde yer verilecektir. Ancak burada, kısaca, AB ülkelerindeki veri koruma otoriteleri ile ülkemizde Tasarı ile kurulması öngörülen veri koruma otoritesi arasında kısa bir karşılaştırma yapılmak istenmektedir. Zira Avrupa Komisyonunun, ülkemizin yeterli seviyede koruma sağlayan bir ülke olup olmamasını değerlendirmesinde, ülkemizdeki veri koruma otoritesinin bağımsızlığının da önemli bir role sahip olacağı düşünülmektedir.

Avrupa Veri Koruması Direktifine göre, veri koruma kurumlarının, kendilerine tevdi edilen işlemleri yerine getirirken "tamamen bağımsız" hareket etmeleri gerekmektedir. Veri koruma kurumlarının tamamen bağımsız hareket etmeleri gerekliliği, Veri Koruması Direktifinin yanı sıra Avrupa Adalet Divanı ve Avrupa veri koruma kurumlarının temsilcilerinden oluşan çalışma grubu (Madde 29 Çalışma Grubu) tarafından da üzerinde durulan bir konudur. Avrupa Adalet Divanı, Almanya'ya karşı açılan bir davanın kararında, tamamen bağımsız olabilmek için, kurumların, doğrudan ya da dolaylı her türlü dış etkenden bağımsız karar alma gücüne sahip olmaları gerektiğini söylemiştir.[115]

Kurumların bağımsızlığı konusunda Avrupa'daki görüş, kurumların, bütçe ya da personel konusunda idari olarak başka devlet kurumlarına kaçınılmaz olarak bağlı olabilecekleri; ancak

[114] Daha fazla bilgi için, bkz: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (İngilizce).
[115] Commission v Germany (2010) (OJ C 113)

bunun veri koruma kurumlarının görevsel bağımsızlığını engellememesi gerektiğidir. Bu sebeple, veri koruma kurumunun başka bir devlet organından, görevi ile ilgili herhangi bir şekilde talimat alması, kurumun "tamamen bağımsız" çalışmasının önünde bir engel teşkil edecektir. Kurumun başka bir devlet kurumunun altında örgütlenmiş bir alt birim olarak kurulması kaçınılmaz olarak bu sonucu doğuracaktır.

Avrupa Komisyonu, 2010 yılında Avusturya veri koruma kurumunun Direktifte belirtildiği gibi tamamen bağımsız olamadığını belirtmiştir. Komisyonun bunun için gerekçelerinden biri, kurumun kendi personelinin ve bütçesinin olmaması dolayısıyla organizasyon ve bütçe açısından federal hükümete bağlı olmasıdır.[116]

Bahsedildiği üzere, AB – Türkiye arası kişisel veri transferinin sağlanabilmesi için, Avrupa Komisyonu'nun Türkiye'nin kişisel verilerin korunması konusunda yeterli seviyede koruma sağlayan bir ülke olduğuna dair karar vermesi gerekmektedir. Madde 29 Çalışma Grubu bu konu ile ilgili bir rapor hazırlamış ve raporunda, AB dışındaki bir ülkenin "yeterli seviyede" koruma sağlayabilmesi için, gerekli kanunların çıkarılmasının yanı sıra kurulacak kurumun, şikayetleri bağımsız olarak inceleyebilmesi ve yine tamamen bağımsız olarak karar alabilmesi ve ceza verebilmesi gerektiğini vurgulamıştır.[117]

Veri koruma kurumlarının tamamen bağımsız hareket edebilmeleri konusunda kurumun yetkileri, personel sayısı, personel atamaları, kurum başkanının görevden alınma prosedürü, kurumun bütçesi ve idare şekli önem teşkil etmektedir.

Bu konularda AB ülkelerindeki durum aşağıda tablolar ile özetlenmeye çalışılmıştır.[118]

Personel Sayısı

Avrupa'da veri koruma kurumlarının personel sayısı değişiklik göstermektedir. Örneğin Birleşik Krallık'ta veri koruma kurumunda 319 personel çalışırken, bu sayı İsveç'de 43'tür. Sayıların değişmesindeki en büyük etkenlerden biri ülkenin nüfusudur. Örneğin Birleşik Krallık'taki 319 personel, ülke nüfusu dikkate alındığında her 191,577 kişiye 1 kurum

[116] European Commission, IP/10/1430, "Data Protection: Commission to refer Austria to Court for lack of independence of data protection authority

[117] Article 29 Working Party, "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive"

[118] Rakamsal bilgiler için, bkz. International Association of Privacy Professionals, "Data Protection Authorities 2011 Global Survey"; Philip Schütz, "Comparing formal independence of data protection authorities in selected EU Member States" (2012)

çalışanına denk gelirken; personel sayısı yalnızca 67 olan Bulgaristan'da her 107,533 kişiye 1 kurum çalışanı denk gelmekte, dolayısıyla kişi başına düşen personel sayısı Birleşik Krallık'ın önünde yer almaktadır.

AB'de Örnek Ülkelerde Veri Koruma Kurumu Çalışan Sayısı:

Ülke	Kurum Çalışan Sayısı
Birleşik Krallık	319
Fransa	132
Polonya	121
İtalya	120
Hollanda	82
Bulgaristan	67
İsveç	43

AB'de Örnek Ülkelerde Bir Veri Koruma Kurumu Çalışanı Başına Düşen Vatandaş Sayısı:

Ülke	Bir Çalışan Başına Düşen Vatandaş Sayısı
Birleşik Krallık	191.577
Fransa	488.031
Polonya	318.041
İtalya	484.385
Hollanda	203.854
Bulgaristan	107.533
İsveç	210.690

Bütçe ve İdare

Avrupa'daki veri koruma kurumlarının yıllık bütçeleri, kurumların çalışan sayısı ve ülkelerin gayri safi milli hasılalarına göre değişiklik göstermektedir. Ülkelerin veri koruma kurumlarının yıllık bütçelerini git gide artırdıkları görülmektedir. Ülkeler bütçelerini en çok idari işler, şikayetler sonucu yapılan işlemler ve tahkikat/yaptırım için kullanmaktadır

AB'de Örnek Ülkelerde Veri Koruma Kurumlarının Yıllık Bütçeleri:

Ülke	Yıllık Bütçe
İtalya	24.500.000 Avro
Birleşik Krallık	22.395.759 Avro
İspanya	15.425.160 Avro
Almanya	8.798.253 Avro
İsveç	3.600.000 Avro
Polonya	3.475.126 Avro
Bulgaristan	1.308.871 Avro

Görüldüğü üzere, İtalya, Birleşik Krallık, İspanya, Almanya gibi yüksek nüfusa ve nispeten büyük ekonomiye sahip olan ülkeler, veri koruma kurumlarının yıllık bütçelerini de yüksek tutmaktadır.

Veri Koruma Kurumu, Kurum Başkanı ve Çalışanlarının Atanması / Görevden Alınması

Avrupa'da veri koruma kurumlarının devlet içerisinde nasıl yer aldıkları, kurum başkanlarının ve çalışanlarının atanmasında ve görevden alınmaları hususunda farklı yaklaşımlar bulunmaktadır. AB'de ilgili veri koruması direktifi ülkelere bu konularda belirli bir dayatma getirmemektedir. Burada önemli olan nokta, hangi yöntem seçilirse seçilsin, kurumun tamamen bağımsız olarak görev yapabilmesinin sağlanmasıdır.

Örneğin Polonya'da kurum başkanının seçilmesi ve görevden alınması Senato'nun da onayıyla yalnızca meclis tarafından gerçekleştirilebilmektedir. Hiçbir bakanlığa bağlı çalışmayan kurum, faaliyetleri ile ilgili yıllık raporunu doğrudan meclise vermektedir. Birleşik Krallık'ta ise kurum başkanının ataması Başbakan'ın önerisi sonucu Kraliçe tarafından yapılmaktadır. Fakat başkanın görevden alınması ancak iki meclisin (Lordlar Kamarası ve Avam Kamarası) kararı ile olmaktadır.

AB'de Örnek Ülkelerde Kurum Başkanlarının Seçilmesi:

Ülke	Seçim
İtalya	Parlamento tarafından oylama
İspanya	Danışma kurulu tarafından seçim, parlamento tarafından oylama
İsveç	Hükümet tarafından seçim
Polonya	Seçim
Almanya	Seçim
Bulgaristan	Seçim

AB'de veri koruma kurumlarının personel sayısı, personel atamaları, kurum başkanının görevden alınma prosedürü, kurumun bütçesi ve idare şekli konusunda bir yeknesaklık bulunmamaktadır. Ancak AB'de, farklı işleyişler de olsa, kurumların, Veri Koruması Direktifinde belirtildiği üzere tamamen bağımsız çalışmaları esastır. Kişisel Verilerin Korunması Kanunu çıktıktan sonra, Türkiye ile AB arasında kişisel verilerin transfer edilebilmesi için Avrupa Komisyonu'nun Türkiye'nin yeterli seviyede koruma sağladığına ilişkin karar vermesi gerekecektir. Avrupa Komisyonu bu kararı doğrultusunda Türkiye'deki Kişisel Verileri Koruma Kurulu'nun ne derece bağımsız olduğunu da değerlendirecektir. Avusturya'yı tamamen bağımsız bir kurum kuramadığı nedeniyle Avrupa Adalet Divanı'na sevk eden Avrupa Komisyonu'nun bu konu üzerinde önemli durduğu söylenebilir.

Tasarı ile ülkemizde getirilmesi düşünülen düzenlemenin, Avrupa Komisyonunu tatmin edip etmeyeceği ve Komisyonun AB-Türkiye arasında veri transferinin önünü açmasını sağlayıp sağlamayacağını şimdiden kesin olarak söylemek imkansızdır. Ancak Avrupa Komisyonunun, Avusturya'nın veri koruma otoritesinin organizasyon ve bütçe açısından federal hükümete bağlı olmasının otoritenin bağımsızlığını engellediği iddiasında olduğu göz önüne alınması gereken bir durumdur. Bu nedenle, AB-Türkiye arasında kişisel veri transferinin önünün açılması için, kurulacak olan yapının mümkün olduğunca bağımsız hareket etme kabiliyetinde olmasına özen gösterilmesi gerekmektedir.

Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi

21.05.2014
v. 01