İKTİSADİ KALKINMA VAKFI YAYINLARI
Yayın No: 278

TÜRKİYE'DE VE AB'DE KİŞİSEL VERİLERİN KORUNMASI

SivilDüşün

TÜRKİYE'DE VE AB'DE
KİŞİSEL VERİLERİN KORUNMASI

İktisadi Kalkınma Vakfı

Bu çalışma,
İKTİSADİ KALKINMA VAKFI'ndan
İKV Uzman Yardımcısı Ahmet CERAN tarafından hazırlanmıştır.

İSTANBUL, ARALIK 2015

İKTİSADİ KALKINMA VAKFI
Esentepe Mahallesi Harman Sokak TOBB Plaza No: 10 Kat: 7-8
34394 Levent İstanbul/Türkiye
Tel: +90 212 270 93 00 Faks: +90 212 270 30 22
E-posta: ikv@ikv.org.tr

Avenue Franklin Roosevelt 148/A 1000 Brüksel/Belçika
Tel: +32 2 646 40 40 Faks: +32 2 646 95 38
E-posta: ikvnet@skynet.be

www.ikv.org.tr

Bu yayın Sivil Düşün AB Programı Aktivist Desteği kapsamında
Avrupa Birliği desteği ile hazırlanmıştır.

ISBN: 978-605-5984-71-7

Yayına Hazırlık ve Baskı
ajans d
Genel Yönetmen: Gürhan Demirbaş
Genel Yönetmen Yardımcısı: Eser Soygüder Yıldız
Görsel Yönetmen: Hakan Kahveci
Editör: Yağmur Bahar Polat
Sayfa Tasarım: Şahin Bingöl

Dünya Yayıncılık A.Ş.
Globus Dünya Basınevi
100. Yıl Mah. 34204, Bağcılar - İstanbul
Tel: (212) 440 24 24

İÇİNDEKİLER

KISALTMALAR LİSTESİ

108 sayılı Avrupa Konseyi Sözleşmesi: Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı Sözleşmesi
AB: Avrupa Birliği
ABAD: Avrupa Birliği Adalet Divanı
ABD: Amerika Birleşik Devletleri
AİHM: Avrupa İnsan Hakları Mahkemesi
AİHS: Avrupa İnsan Hakları Sözleşmesi
AP: Avrupa Parlamentosu
BM: Birleşmiş Milletler
C20: Sivil 20
C-SIS: Merkezi Schengen Bilgi Sistemi (*Central Schengen Information System*)
Çerçeve Karar: Cezai Meselelerde Kolluk ve Adli İşbirliği Çerçevesinde İşlenen Kişisel Verilerin Korunmasına ilişkin 2008/977/JHA sayılı Karar
EDPS: Avrupa Veri Güvenliği Gözetmeni (*European Data Protection Supervisor*)
EDRIS: Avrupa Acil Durum Afet Bilgi Sistemi (*European Emergency Disaster Response Information System*)
Eurojust: Avrupa Yargı İşbirliği Kurumu
Europol: Avrupa Polis Teşkilatı
Eurosur: Avrupa Sınır Gözetim Sistemi
Eurostat: Avrupa Birliği İstatistik Kurumu
G8: 8'ler Grubu
G20: 20'ler Grubu
IATI: Uluslararası Yardım Şeffaflığı Girişimi (*International Aid Transparency Initiative*)
IBM: Uluslararası İş Makineleri (*International Business Machines*)
İKV: İktisadi Kalkınma Vakfı

LIBE: AP Medeni Haklar Komitesi
MİT: Milli İstihbarat Teşkilatı
NSA: ABD Ulusal Güvenlik Ajansı (*National Security Agency*)
N-SIS: Ulusal Schengen Bilgi Sistemi (*National Schengen Information System*)
OECD: Ekonomik Kalkınma ve İşbirliği Örgütü (*Organisation for Economic Co-operation and Development*)
PNR: Yolcu İsim Kaydı (*Passenger Namer Record*)
SIS II: Schengen Bilgi Sistemi (*Schengen Information System*)
TBMM: Türkiye Büyük Millet Meclisi
TTYO: Transatlantik Ticaret ve Yatırım Ortaklığı (*Transatlantic Trade and Investment Partnership*)
UYAP: Ulusal Yargı Ağı Bilişim Sistemi Projesi
VIS: Vize Bilgi Sistemi (*Visa Information System*)

SUNUŞ

İKV, kuruluşundan bu yana 50 yıldır, Türkiye-AB ilişkilerinde en öne çıkan konuları gündemine taşımaya ve bu alanlarda politika üretim süreçlerinde öncü rol üstlenmeye devam ediyor. "Türkiye'nin AB Uzmanı" sloganıyla çalışmalarına devam etmekte olan İKV, değerlendirme, analiz ve araştırmalarıyla, bütün paydaşlara AB üyeliği hedefi doğrultusunda destek veriyor ve bu doğrultuda kamuoyunu bilgilendirirken, güncel küresel eğilimlere de dikkat çekiyor.

Bilgi teknolojilerinin ve internetin hem sosyal yaşamda hem ticari ilişkilerde hem de devlet/vatandaş ilişkilerinde büyük önem kazanmasıyla ve bu teknolojilerin hızla gelişmesiyle birlikte, kişisel verilerin korunması ve sınır ötesi paylaşımına ilişkin tartışmalar; popüler bir küresel eğilim haline geldi. Kişisel verilerin taşıdığı ticari değerle birlikte, konunun temel hak ve özgürlüklere ve güvenliğe ilişkin boyutu; konunun çok farklı ve hassas çerçevelerde ele alınmasını gerekli kıldı. Küresel tartışmaların merkezindeki bu konu şüphesiz ki bir süredir AB'nin de ana gündem maddeleri arasında yer alıyor.

Kişisel verilerin korunması konusu; AB tarafından doğrudan temel hak ve özgürlükler açısından ele alındığı gibi; 2'nci Dünya Savaşı'ndan bu yana görülen en büyük göçmen kriziyle karşı karşıya olduğumuz bir dönemde sınır yönetiminin ve güvenlik politikalarının parçası olarak ve Dijital Tek Pazar tartışmaları sürerken dijital ekonomi ve TTYO müzakereleriyle bağlantılı olarak da değerlendiriliyor. AB'de, kişisel verilerin korunması alanında bütüncül bir mevzuatın oluşturulmasına yönelik çalışmaların devam ettiği bir dönemde; Türkiye'nin bu tartışmaların dışında kalmaması gerektiğini düşünüyoruz.

İKV'nin öncelikli çalışma alanlarını oluşturan "Katılım Müzakereleri", "Vize ve Geri Kabul" ile "Gümrük Birliği STA ve TTYO" alanlarının hepsi açısından kişisel verilerin korunması meselesi büyük önem taşıyor. Müzakere fasılları kapsamında Avrupa Komisyonu'nun öne sürdüğü kriterlerin yerine getirilmesi, dolayısıyla AB üyeliğinin gerçekleşebilmesi için Türkiye'nin AB standartlarında bir Kişisel Verilerin Korunması Kanunu'na sahip olması gerekiyor. Öte yandan Türk vatandaşlarına vizesiz Avrupa kapılarının açılabilmesi için de bu alandaki mevzuatını AB standartlarına getirilmesi gerekiyor. Ayrıca TTYO ve Gümrük

Birliği'nin güncellenmesi tartışmaları dahilinde önümüzdeki dönemde bu meselenin daha fazla gündeme geleceği muhakkak.

Dolayısıyla, kişisel verilerin korunması gibi temel hak ve özgürlüklerin, AB projesinin merkezinde yer aldığını dikkate alarak, bu çalışmanın konuya ilişkin AB standartlarını ve Türkiye'nin uyumu için gerekli adımları ortaya koyan bir rehber niteliği taşmasını amaçlıyoruz. Çalışmanın, Türkiye'nin AB üyelik sürecine katkı sağlamasını temenni ederiz.

Ayhan ZEYTİNOĞLU
İKV Yönetim Kurulu Başkanı

TANITIM

Tüm dünyada olduğu gibi ülkemizde de yeni iletişim teknolojileri ve bunların milyonlarca kullanıcıya sunduğu imkânlar, yakından takip edilerek, hızla uygulamaya geçiriliyor. Artan internet kullanımı ve internetin artık yaşamın her alanına hızlı ve yoğun şekilde nüfuz etmesi, bu ortamdaki içeriğin her geçen gün biraz daha fazla çeşitlenmesine sebep oluyor.

TÜİK'in 2015 yılında yayımladığı Hane Halkı Bilişim Teknolojileri Kullanım Araştırması, Türkiye'de internet kullanan bireylerin oranını %55,9 olarak gösteriyor. 2014 yılında %53,8 olan bu oranda, 2007 yılından bu yana ciddi bir hızlanma görülüyor.

İnternetin hızla yaygınlaştığı ülkemizde, kullanıcılar artık "internette sörf yapmanın ötesinde" iletişim kurmak, sosyal ağlarda yer almak, alışveriş ve ticaret yapmak gibi çok daha farklı amaçlarla interneti kullanıyor. Yine TÜİK araştırmasına göre, Türkiye'de hanelerin %96,8'inde cep telefonu veya akıllı telefon varken, bir kişinin cep telefonu veya akıllı telefonu olmaması, garipsenecek bir yaklaşım olarak algılanıyor.

Teknolojiyi bu kadar yakından takip eden ülkemiz, bir yandan da özellikle sosyal medyada dünya liderliğine oynuyor. Arama motoru Google'ın ülkemizde dahil olduğu 46 farklı pazarda internet alışkanlığını ölçtüğü Tüketici Barometresi araştırmasına göre Türkiye, sosyal medya kullanımında dünyada ilk sırada yer alıyor. Dünya genelinde internet kullanıcılarının sosyal medya kullanım oranı yaklaşık %40 iken, bu oran Türkiye'de %92.

Türkiye'yi %86 ile Arjantin ve %83 ile Brezilya takip ediyor. Yani Türkiye sadece lider olmuyor, yüzde 6 puanlık farkı ile ilk takipçisi ile de arayı ciddi şekilde açıyor. Akıllı telefonların "elimiz ayağımız olduğu" günümüze ilişkin son ilginç bir veri, ilginç olduğu kadar da düşündürücü. Tüketici Barometresi araştırması 35 milyonun üzerinde internet kullanıcısı olan Türkiye'de, 36 milyonun üzerinde aktif Facebook kullanıcısının olduğunu gösteriyor.

Elbette artan internet kullanımı ve bu ortamdaki Türkçe içeriğin gün geçtikçe genişlemesi, Türkiye'nin "çağı yakaladığının" önemli bir göstergesi. Ancak 35 milyon internet kullanıcısının bulunduğu Türkiye'de 36 milyon aktif Facebook hesabının bulunması, bir yerlerde hatanın olduğu izlenimini veriyor. Ve bu hataya yeri geldiğinde, belki bilmeden, kendi rızamızla düşmüyor muyuz? Bireysel özgürlüğümüzü korumak için elimizde kalan tek ve yegâne araç olan kişisel verilerimizi bu kadar kolay bir şekilde, bu derya-deniz ortama veren biz değil miyiz?

Elbette sadece kendi rızamızla değil, kamusal ve kimi özel alanlarda güvenliğin sağlanması ve suçla mücadele gibi amaçlarla görüntülerimizi, göz retinamızı, parmak izimizi hatta sesimizi kaydetmiyor muyuz? Doğru teşhis ve uygun tedavi için en mahrem sağlık bilgilerimizi; alışveriş yapmak için kullandığımız kredi kartları ile beğenilerimizi; spor salonlarına girerken verdiğimiz parmak veya el izi ile günlük rutinimizi; bizim dışımızdaki kurumlarla, haliyle de kişiler ile paylaşmıyor muyuz?

ATM'den para çekme sırasında bile, arkamızdaki kişinin nefesini ensemizde hissettiğimiz Türkiye'de kişisel verilerin korunmasının önemi, bir kat daha fazla; fakat öncelik bireysel farkındalığın sağlanmasında ve bireysel önlemlerin alınmasında geçiyor. Bu alanda devletten gerekli yasal ve hukuki düzenlemelerin yapılmasını talep etmeden önce, birey olarak bu konunun önemini ve ehemmiyetini doğru algılamamız ve kişisel verilerimizi önce kendimizin koruması gerekli. Elbette bireysel bilinçlenme kadar önemli olan bir diğer husus, bu alanda hukuki dilin oluşturulması ve bunu takiben, yasal düzenlemelerin etkin şekilde hayata geçirilmesi.

Bu noktada 2015 yılında üyelik müzakerelerinde 10'uncu yılı geride bırakacağımız AB üyelik süreci, Türkiye için önemli bir fırsat penceresi sunuyor. Son yıllarda gelişen teknolojinin ve bunun kişisel verilere ilişkin yarattığı handikapları daha fazla hisseden AB, kişisel verilerin korunması alanında çoktan düğmeye basmış durumda. Kişisel özgürlükler ile güvenlik ekseninde yürüyen tartışmalarda AB, Türkiye'den çok daha ileri bir pozisyonda bulunuyor. Bu çerçevede Türkiye'nin AB ve küresel düzeyde sürdürülen tartışmalara

kulak vermesi ve önce kendi vatandaşlarının refahı, özgürlüğü ve güvenliği için etkin kişisel verilerin korunması mekanizmalarını benimsemesi gerekiyor. Bu mekanizmanın oluşturulması ve etkin işletilmesinin, Türkiye-AB ilişkilerinin kronikleşen bir takım sorunlarına, Gümrük Birliği veya vizesiz Avrupa ideali gibi, çözüm oluşturacağını da unutmamak gerekiyor.

Kişisel veriler alanında hazırlanmış bu titiz çalışma, tüm boyutlarıyla kişisel verilerin korunmasının önemini vurgulamayı amaçlarken, bu alanda ülkemiz için uyarılarda bulunmayı da ihmal etmiyor.

Bu çalışmanın hazırlanmasında öncü olan ve yoğun emek harcayan İKV uzman kadrosundan Ahmet CERAN'a teşekkür ederken; çalışmanın ülkemizde hak ettiği ilgiyi göremeyen kişisel hakların korunması alanına yapıcı katkıda bulunmasını temenni ediyoruz.

Melih ÖZSÖZ
İKV Genel Sekreter Yardımcısı ve Araştırma Müdürü

GİRİŞ

İçinde bulunduğumuz bilgi çağında kişisel veriler; sigortacılık, bankacılık, ulaştırma, sosyal medya, arama motorları, reklamcılık gibi çok çeşitli sektörlerden; kolluk kuvvetleri, sınır kontrol birimleri, nüfus müdürlükleri gibi kamu kuruluşlarına kadar geniş bir yelpazeye yayılmış iş kollarında kullanılıyor. Bulut bilişim (*cloud computing*) ve benzeri, her gün gelişen teknolojiler sayesinde, "kişisel bir veri, internet aracılığı ile, Berlin'den işlenmek üzere Boston'a gönderilebiliyor ve Boston'da işlenen bu veri, depolanmak üzere Hindistan'ın silikon vadisi kabul edilen Bangalor'a çok kısa sürede ulaştırılabiliyor"[1]. Bu süreçler; bilgi teknolojilerindeki hızlı ilerleme ile birlikte sınırların belirsizleşmesi, kişilik haklarının zarar görmesi, ulusal denetimin zorlaşması, mevcut hukuki düzenlemelerin yetersiz kalması gibi sorunların ortaya çıkmasına sebep olabiliyor. Öte yandan kişisel verilerin korunması konusu, AB hukuku kapsamına giren; temel haklar, kişilerin serbest dolaşımı, sınır kontrolü ve komşuluk politikaları, şirketler hukuku, organize suç, terör ve insan ticareti ile mücadele gibi Türkiye-AB müzakerenin kilit alanları ile doğrudan bağlantılı.

Konunun temel hak ve özgürlüklerden sürdürülebilir kalkınmaya, ticari kazanımlardan iç ve dış güvenliğe kadar çok çeşitli alanlara etkisinden ötürü AB, vatandaşların hak ve özgürlüklerini garanti altına alacak kapsayıcı ve bütün AB ülkelerinde geçerli bir kişisel verilerin korunması sistemi oluşturmayı öncelikli gündemi haline getirdi. Essex Üniversitesi İnsan Hakları Hukuku Profesörü Steve Peers, AB'nin bu girişimini, 1985 tarihli bilim kurgu filmi "Geleceğe Dönüş" metaforuyla değerlendiriyor. Peers, AB'nin 2015 yılında; bu alanda, 1985 yılının hatta 1955 yılının teknolojileri dikkate alınarak oluşturulan prensiplere uyum sağlamaya çalışmasını, zaman makinası ile geçmişe dönemeye benzetiyor[2]. Türkiye'deki duruma bakıldığında ise geçmişten bu yana etkin bir mevzuatın oluşturulmadığı, geri dönülecek bir geçmişin dahi bulunmadığı dikkat çekiyor. Konuya ilişkin AB standartları dahi uluslararası konjönktürde tartışma konusu olurken, Türkiye'nin kişisel verilerin korunması alanında AB standartlarına uyumu, Türkiye'de temel hak ve özgürlüklerin gelişmesi ile paralel olarak Türkiye-AB Katılım Müzakerelerinin ileri aşamaya taşınmasına da büyük katkı sağlayacak.

Dolayısıyla, çalışma kapsamında ilk olarak bu alandaki uluslararası prensipler ile hukuki çerçeveye değinilmesi, sonrasında ilgili AB standartlarının üzerinde durulması öngörülüyor. Devamında ise Türkiye'de bu alanda tasarı halindeki yasal mevzuatın ele alınması ve Türkiye-AB ilişkilerinde kişisel verilerin korunmasına ilişkin ileri uyumun gerekli olduğu alanların değerlendirilmesi amaçlanıyor.

1.KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BASİT KAVRAMSAL VE HUKUKİ ÇERÇEVE

En temel tanımı ile kişisel veri; kişinin özel, profesyonel veya kamusal yaşamıyla ilgili her türlü bilgiyi içerir. İsim, fotoğraf, Twitter/Facebook/Whatsapp gibi sosyal medya iletileri, e-posta adresi, parmak izi, biyometrik ve tıbbi bilgiler gibi yaşamın her alanındaki çok farklı bilgi, bu kapsama giriyor. Türk yetkili makamları tarafından AB müktesebatına uyum kapsamında 2008 yılında hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı'nın 3'üncü maddesi'nde kişisel veriler; "Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlanıyor[3].

Kişisel veriler, ilk defa 1948 tarihli BM İnsan Hakları Evrensel Bildirgesi ve 4 Kasım 1950'de imzalanan Avrupa İnsan Hakları Sözleşmesi (AİHS) tarafından güvence altına alındı. Bununla birlikte, 1960'lı yıllardan itibaren bilgi teknolojilerindeki gelişmelerle, kişisel verilerin korunmasına yönelik daha kapsamlı uluslararası düzenlemelere ihtiyaç duyulmuş, Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı Sözleşmesi (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*) oluşturulmuştu. 108 sayılı Sözleşme, bu alanda bağlayıcılığı olan ilk düzenleme. Sözleşme'ye, Avrupa Konseyi üyesi olmayan Uruguay ve Fas gibi ülkeler de taraf durumda. Sözleşme'nin hükümleri, taraf ülkelerdeki özel sektörün ve kamu sektörünün tamamını bağlar nitelikte[4]. Türkiye ise 1988 yılında 108 sayılı Sözleşme'yi imzalamış olsa dahi daha onaylamadı ve yürürlüğe koymadı.

İlgili uluslararası düzenlemeler kapsamında, kişisel verilerin yanı sıra; özel koruyucu önlemleri gerekli kılan üç adet veri türü daha bulunuyor. Bu çerçevede:

Hassas veriler (*sensitive data*); ırksal kökeni, siyasi görüşleri, dinsel ya da diğer inançları açığa çıkaran kişisel veriler; kişinin sağlığı ya da cinsel yaşamı ile ilgili olan veriler ve cezai mahkûmiyetlere ilişkin veriler. Hassas veriler otomatik yollarla işlenemez[5]; yani manuel olmayan yollarla *"toplanamaz, kayıt altına alınamaz, depolanamaz, değiştirilemez.[6]"*

Tablo 1: Sınır Ötesi Veri Akışlarına ilişkin OECD Yönlendirici İlkeleri	
Sınırlandırma İlkesi	Verinin sadece yasalara uygun ve adil yollarla, verinin öznesinin bilgisi dahilinde toplanması;
Veri Kalitesi İlkesi	Verinin doğru, eksiksiz ve güncel olması;
Amacın Belirli Olması İlkesi	Verinin toplanmasının ardından, kullanım amacının değiştirilememesi;
Kullanımın Sınırlandırılması İlkesi	Verinin sadece verinin öznesinin rıza gösterdiği amaçlar doğrultusunda veya resmi yetkili makamların hükmü doğrultusunda kullanılması;
Koruyucu Tedbirler İlkesi	Kişisel verilerin, izinsiz erişim, kullanım ve izinsiz değişiklikler gibi risklere karşı korunması;
Açıklık İlkesi	Kişisel verilerin korunmasına ilişkin gelişmelere, politikalara ve uygulamalara açık olunması;
Bireysel katılım İlkesi	Kişinin, kendisine ilişkin veriyi kontrol altında tutanlarla etkileşime geçebilmesi;
Hesap verebilirlik İlkesi	Kişisel verileri kontrol altında tutanların, ilgili mevzuatla ve yukarıdaki ilkelerle uyumlu olması, bu doğrultuda şeffaflık sağlayabilmesi.

Anonim veriler (*anonymised data*); kişisel verilerin bütün tanımlayıcı öğelerinin ortadan kaldırılması ile geriye kalan veri türüdür. Bir kişisel veri, belli bir amaç doğrultusunda kullanıldıktan sonra, bu veri bilimsel, istatiksel amaçlarla sadece anonim halde muhafaza edilebilir.

Takma adlı veri (*pseudonymous data*) ise; bilginin, veri sahibi ile ilişkilendirilebilmesi için ek bilgilere ihtiyaç duyulan veri türüdür. Bu tür verilerin işlenmesi sürecinde, verinin sadece dolaylı yollarla tanımlanabilir kalmasını sağlama görevi, veriyi işleyen kişiye aittir[7].

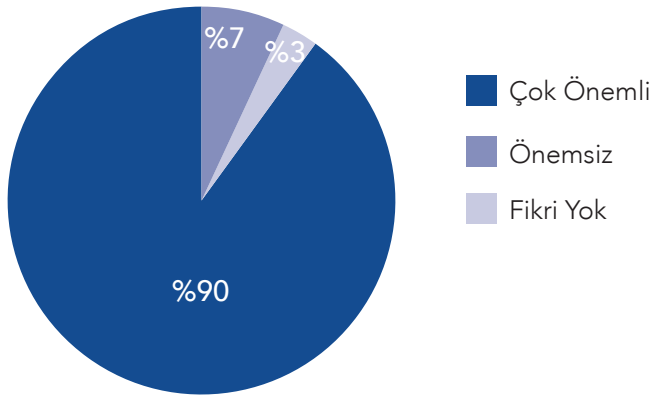
Farklı türlerine rağmen, bütün kişisel verilerin korunmasına ve veri akışının kontrol altına alınmasına yönelik olarak, OECD 1980 yılında sekiz yönlendirici ilke belirlemiştir. Günümüzde konuya ilişkin bütün ulusal ve uluslararası mevzuat, OECD yönlendirici ilkelerini dikkate almakta[8].

2.KİŞİSEL VERİLERİN KORUNMASINDA AVRUPA NE KADAR BAŞARILI?

Daha önce de belirtildiği üzere, kişisel verilerin korunması, bütün Avrupa'da, emredici (*jus cogens*) nitelikte temel haklar arasında kabul ediliyor. Fakat sınırları içerisinde günde 250 milyon bireyin aktif olarak internet kullandığı AB[9], kendi içerisinde ve üçüncü ülkelerle veri akışının tam kontrolünü sağlamakta ciddi zorluklarla karşılaşıyor. İkinci Dönem Barroso Komisyonu'nun (Şubat 2010 - Ekim 2014) Adalet, Temel Haklar ve Vatandaşlıktan Sorumlu Üyesi Viviane Reding, 1997'de Avrupa'da internet kullanımı oranının yüzde 1 olduğunu, günümüzde ise bilginin birkaç saniyede, AB içinde ve yeryüzünün diğer coğrafyalarında dolaşabildiğini ifade ediyor[10]. Öyle ki, konu Avrupa liderlerinin kendi iç kamuoylarında eleştirilmelerine bile sebep olabiliyor. Örneğin, 2013 yılında Alman vatandaşlarının internet üzerindeki kişisel verilerinin, İngiltere ve ABD istihbarat örgütleri tarafından ele geçirilmesi ve kullanılması tartışmaları, seçim döneminde Almanya Şansölyesi Angela Merkel'in karşısına çıkan en zorlu muhalif propaganda hamleleri arasında yer almıştı. Aynı şekilde Merkel'in ABD tarafından dinlendiğine yönelik iddialar, dünyanın iki önemli gücü Almanya ve ABD arasında kısa süreli gerginliğe sebep olmuştu[11].

AB hukuku çerçevesinde, kişisel verilerin korunmasına ilişkin, AİHS ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin ötesinde de, bir takım adımlar bulunuyor. İlk olarak, 1995 yılında kabul edilen 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında Yönerge (AB Kişisel Verilerin Korunması Yönergesi) ile, Birlik dahilinde verinin korunması alanında yüksek bir standart oluşturmaya çalışıldı. AB Kişisel Verilerin Korunması Yönergesi, yüksek seviyede veri güvenliği sağlanmadığı takdirde, AB iç pazarında malların, kişilerin ve hizmetlerin etkin serbest dolaşımının mümkün olamayacağı ana fikrine dayanıyor. Bu doğrultuda Yönerge, 108 sayılı Avrupa Konseyi Sözleşmesi'ne ek olarak, AB ülkelerinde bağımsız denetim organları kurulmasını öngörüyor. Öte yandan, gelişen teknolojilerin ve küreselleşmenin etkileriyle birlikte mevcut düzenlemelerin güncelliğini yitirmesi ve Birlik içerisinde veri güvenliğinin ideal ölçüde sağlanamaması, reform tartışmalarını gündeme taşıdı. Avrupa Komisyonu'nun resmi istatistik kurumu *Eurostat* tarafından, AB kamuoylarının belli konulardaki görüşlerini ortaya koyan düzenli Eurobarometre anket çalışmasının sonuçlarına göre, Avrupalıların %90'ı, kişisel verilere ilişkin Avrupa çapında eşit koruma talep ediyor[12].

Tablo 2: Kişisel verilerin toplandığı ve işlendiği ülke farketmezsizin bütün AB çapında eşit haklara ve korumaya sahip olmak Avrupalı İnternet kullanıcıları için ne kadar önemlidir?[13]



Devam eden reform tartışmalarıyla birlikte, Avrupa Komisyonu 2012 yılında, Avrupa Parlamentosu ve AB Konseyi'ne, 1995 tarihli AB Kişisel Verilerin Korunması Yönergesi'nin revize edilmesi ve bu yönergenin internet çağına ayak uyduracak hale getirilmesine yönelik bir teklif sundu. Teklifin öne sürdüğü;

- Tüm AB sınırları içerisinde geçerli tek Kişisel Verilerin Korunması Tüzüğü'nün oluşturulmasıyla birlikte, önemli mali tasarruflar ve kolaylıklar sağlanması;
- İhlal hallerinde veri sahibinin anında uyarılması ve veri öznesinin talebi üzerine verinin silinebilmesi;
- AB çapında bir kişisel verilerin korunması sistemi ile idari prosedürlerin azaltılması, böylelikle AB dahilindeki iş çevrelerine 2,3 milyar avro değerinde tasarruf sağlanması bekleniyor.

Avrupa Komisyonu'nun istatistiklerine göre, günümüzde verinin korunmasına ilişkin mevcut evrak işleri ve harcamalar, işletmelere yıllık 130 milyon avroya varan ek masraf getiriyor[14]. Dolayısıyla, yeni Tüzük ile birlikte sınır ötesi sorunlarda her üye ülkede bulunan tek durak noktasının (*one stop shop*) kurulduğu kapsayıcı bir sistemle, bürokratik süreçlerin önüne geçilmesi hedefleniyor. Fakat bu noktada ne tür verinin kişisel veri kabul edileceği; bireyin güvenliğinin mi yoksa verinin serbest dolaşımının mı ön plana çıkarılacağı ve hangi tür rızanın kişisel verilerin dolaşımı için yeterli olacağı soruları ekseninde AB ülkeleri ve AB kurumları çapında yoğun tartışmalar sürüyor. Güvenlik ile özgürlük kıskacında devam eden bu tartışmaların yakın gelecekte kolay bir çözüme ulaşacağını söylemek zor.

2.1.ABAD Kararı: Avrupalılar Unutulmak İstiyor

Kişisel verilerin korunmasına ilişkin her konuda geniş çaplı uzlaşıya varılamasa bile, 13 Mayıs 2014 tarihinde AB'nin gündemine oturan önemli bir AB Adalet Divanı (ABAD) kararı alındı. Daha önce de belirtildiği üzere, kişisel verilerin paylaşımı ve dolaşımı ancak kişinin rızasının olduğu hallerde veya hukukun zorunlu kıldığı durumlarda mümkün. Ayrıca, verinin paylaşımına sebep olan amaç gerçekleştiğinde, OECD ilkeleri gereği, kişisel veri başka bir amaç için kullanılamıyor. Öte yandan, kişisel verilerin korunması, kişinin kendisine ilişkin kişisel veriye her şartta ulaşabilmesini ve kendisine ilişkin verinin silinmesini talep edebilmesini de kapsıyor.

Tablo 3: ABAD'ın C-131/12 sayılı kararında öne çıkan konular
Kişisel verinin korunmasına ilişkin AB hukuku, Google ve benzeri arama motorlarına uygulanabilir mi?
Arama motorları, kişisel veriyi kontrol altında tutmaktadır. Dolayısıyla ilgili AB hukuku, arama motorlarına da uygulanabilmektedir.
Kişisel verinin korunmasına ilişkin AB hukuku, Google'ın veri sunucuları AB dışında, ABD'de bulunsa dahi, Google İspanya ofisine yönelik olarak uygulanabilir mi?
Veri sunucusu (*server*) fiziksel olarak AB dışında bulunsa dahi, arama motorunun AB ülkelerinde şubesi var ise, veriyi depolayan şirket, ilgili AB organının yer bakımından yargı yetkisine girmektedir.
Kişilerin, arama motorları aracılığıyla ulaşılabilinen kişisel verilerinin silinmesini talep etme (*right to be forgotten*) hakkı var mıdır?
Biliginin; hatalı, eksik, ilgisiz ve aşırı olduğu durumlarda, kişilerin arama motorlarından veya diğer veri depolayıcılarından, verilerinin silinmesini talep etme hakkı (*right to be forgotten*) bulunmaktadır.

Bu alandaki en ilginç gelişme, Costeja González isimli İspanyol vatandaşı, kendisiyle artık bağlantısı olmayan verilerin, dünya devi arama motoru Google'ın arama sonuçlarından silinmesine yönelik olarak 2010 yılında İspanyol yargı mercilerine başvuruda bulunmasıyla başladı. İspanyol mahkemeleri, davayı ABAD'a sevk ederken ABAD, 13 Mayıs 2014 tarihinde davaya (C-131/12) ilişkin üç konuda, AB içtihat hukukunun geleceğini doğrudan etkileyecek önemli kararlara imza attı[15].

Söz konusu davaya ilişkin ABAD kararında da ifade edildiği üzere, kişisel verinin silinmesini talep etme hakkı her durumda geçerli değil. İfade özgürlüğü, basın özgürlüğü ile kişisel verilerin korunması arasındaki dengenin günümüzde AB içerisinde halen kurulamamış olması, bu alanda büyük tartışmalara yol açmaya devam ediyor. Bu alanda özgürlük ve güvenlik dengesinin kurulabilmesi için, her vakanın kendi iç dinamiklerine göre değerlendirilmesi ve yeni kararlarla gelişen bir içtihat hukukunun dolayısıyla da; revize edilmiş mevzuatın oluşturulması gerekiyor.

2.2.AB'den Üçüncü Ülkelere Veri Akışı

İdeal bir dünyada, sınırların kontrolü ve iç hukuk düzenlemeleri kusursuz şekilde sağlansa dahi, gelişen teknolojilerle birlikte verinin AB dışına çıkışını tamamıyla kontrol altına almak mümkün değil. Güncel durumda, verinin üçüncü ülkelere nasıl ulaştığının belirlenmesi, AB ile Türkiye gibi üçüncü ülkeler arasındaki veri transferinin analiz edilebilmesi için ön şartlardan biri.

108 sayılı Sözleşme'nin Ek Protokolü'ne göre verinin üçüncü ülkelere transferi, belli bir verinin; yabancı yargı sistemlerinin yetkisi altındaki kişilere ulaşması anlamına geliyor[16]. Başka bir deyişle, sadece sınır ötesindeki belli bir kişiye yöneltilmiş belirli veriler, sınır ötesi veri akışına uygun kabul ediliyor. 108 sayılı Sözleşme'nin hükümleri doğrultusunda, devletlerin iç hukuku ihlal edilmediği sürece, taraf devletler arasındaki veri akışı önlenemez. Öte yandan, 108 sayılı Sözleşme'nin hükümleri ışığında, AB üyesi olmayan ülkelere doğru gerçekleşen veri transferinin uygunluğunu karara bağlanması, AB üye ülkelerin iç hukukuna bırakılmış durumda. AB ülkelerinin ilgili iç hukuk mevzuatı ise, Avrupa Komisyonu'nun tavsiye kararları ve yönergeleri doğrultusunda şekilleniyor. Buna

göre, başta kamu menfaatinin zarar görmesi olmak üzere, barış ve güvenliği tehdit eden durumlara sebebiyet verilmediği sürece, üçüncü ülkelere yönelik veri akışına, iç hukuk düzenlemelerince izin verilmelidir. Avrupa Komisyonu'nun sadece belirli veri türlerine yönelik iç hukuk düzenlemelerini öngören kararları da bulunuyor. Örneğin, AB ile belirli bir takım üçüncü ülkeler arasında kurulan hava ulaşım hatlarında yolcu isim kayıtlarının (PNR) karşılıklı paylaşımına yönelik anlaşmalara varılmıştı[17].

3.KİŞİSEL VERİLERİN KORUNMASI VE TÜRKİYE

Kişisel verilerin korunmasına ilişkin AB müktesebatı, üye ülkelerin iç hukuk mevzuatı el verdiği ölçüde üçüncü ülkelerle karşılıklı veri akışını mümkün kılıyor. Bu noktada, Avrupa Konseyi kurucu üyesi sayılan ve 2005 yılından bu yana AB ile üyelik müzakerelerini sürdüren Türkiye'nin durumu, diğer üçüncü ülkelere oranla bir nebze daha farklı. Türkiye'nin, jeopolitik konumundan ve AB ülkeleriyle süregelen ekonomik, siyasi ilişkileri ve adli işbirliğinden ötürü, veri güvenliğine ilişkin aktörler arası işbirliği, herhangi bir üçüncü ülke ile karşılıklı anlaşmanın çok ötesine geçen bir önem taşıyor.

Türkiye'nin kişisel verilerin korunması yolculuğu, ilk bağlayıcı antlaşma olan; 108 sayılı Avrupa Konseyi Sözleşmesi'ni 1988 yılında imzalamasıyla başladı. Sözleşme, taraf devletler arasındaki veri akışını serbest kılıyor. 1988 yılında imzaladığı bu Sözleşme'yi henüz onaylamamış ve yürürlüğe koymamış olan Türkiye, imzacı Avrupa Konseyi Üye Devletleri arasında Sözleşme'yi onaylamayan tek ülke[18]. Türkiye'nin Sözleşme'yi onaylamamasının temel nedeni olarak, Sözleşme'nin 4'üncü maddesi gerekçe gösteriliyor. Sözleşme'nin ilgili hükmüne göre taraf devletin, en geç Sözleşme'nin yürürlüğe girdiği tarihe kadar ilgili iç hukuk önlemlerini alması gerekiyor[19].

Türkiye'nin kişisel verilerin korunmasına yönelik iç hukuk serüveni, 2010 Anayasa Değişikliği Paketi kapsamında; Anayasa'nın özel hayatın gizliliğine ilişkin 20'nci maddesine; "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.*" ibaresinin eklenmesiyle hız kazandı[20]. Devam eden

süreçte, 2013 Demokratikleşme Paketi kapsamında Kişisel Verilerin Korunması Kanun Tasarısı'nın oluşturulması ve kabul edilmesi öngörülmüştü.

Avrupa Komisyonu, düzenli ilerleme raporları ve Vize Serbestliği Yol Haritasına İlişkin Birinci Değerlendirme Raporu'nun "Kamu Düzeni ve Güvenlik" Bloğu (Blok 3) kapsamında, Türkiye'ye kişisel verilerin korunmasına ilişkin bir takım eleştirilerde bulunuyor. Her iki raporda da, Kişisel Verilerin Korunması Kanun Tasarısı'nın, AB normlarına uygun bir şekilde yürürlüğü girmesinin ve 108 sayılı Sözleşme'nin imzalanmasının zorunlu olduğu vurgulanıyor. Bu zorunluluk doğrultusunda, müzakerelerde 23 ve 24 numaralı fasıllarda uyum düzeyinin karşılanması ve üyeliğin gerçekleşebilmesi için ilgili Yasa Tasarısı'nın, 95/46/EC sayılı Yönerge'yle uyumlu hale getirilmesi gerekiyor. 95/46/EC sayılı Yönerge'ye uyum kapsamında atılması gereken ilk adım; kişisel verilerin korunmasını denetleyici; bağımsız ve tarafsız bir kurumun tesis edilmesi oluşturuyor.

Avrupa Komisyonu ilerleme raporlarına göre, Türkiye ile AB kolluk kuvvetleri, sınır kontrol birimleri ve istihbarat teşkilatları arasında veri paylaşımını sağlayacak altyapı oluşturulmalı. Öte yandan bu alandaki reformlar, vize serbestliğinin sağlanması ve Geri Kabul Anlaşması'nın hükümlerinin yerine getirilmesi için de temel zorunluluklar arasında yer alıyor. Dolayısıyla 1 Aralık 2014 tarihinde açıklanan AB'ye Katılım için Ulusal Eylem Planı'nın II. Aşaması kapsamında da kişisel verilerin korunmasına yönelik adımlar yer alıyor. Eylem Planı'nın koyduğu hedef doğrultusunda, 2016 yılının birinci dönemine kadar, 108 sayılı Sözleşme'nin ve 181 sayılı Ek Protokol'ün onaylanması öngörülmüştü[21].

Bölgesel barış ve güvenliğin sağlanabilmesi için Türkiye ve AB'nin uyumu büyük önem taşıyor. Günümüzde veri dolaşımının geçirdiği evrimle birlikte, bu uyumun önemli bir unsuru ise veri paylaşımı. Dolayısıyla Türkiye'nin, ilgili Sözleşmeleri yürürlüğe koyarak mevzuatını AB standartlarına getirmesi; güvenlik, adalet ve temel haklar açısından kısa vadede atılabilecek, önemli bir adım. Özellikle, kişisel verilerin korunmasına yönelik AB içinde de tartışmaların sürdüğü ve üye ülkelerin dahi eleştirildiği bu dönemde atılacak adımların, ilgili başlıklara ilişkin yükümlülüklerin yerine getirilmesi konusunda olumlu bir hava oluşmasına sebep olması mümkün.

3.1.Türkiye'de Kişisel Verilerin Korunmasının "Aşırı" Kısa Serüveni

Aslında Türkiye'de kişisel verilerin korunmasına ilişkin serüven, zamanın ruhuna uygun bir şekilde, Avrupa Konseyi'nin 1981 yılında kabul ettiği Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme'yi aynı yıl imzalamasıyla başladı. Devam eden süreçte Türkiye, ilgili sözleşmenin öne sürdüğü yasal düzenlemeleri gerçekleştirmediği ve kurulması öngörülen denetim mekanizmasını hayata geçirmediği için sözleşmeyi imzalayamadı. Dolayısıyla Türkiye'nin, Avrupa Konseyi üyesi ülkelerle eş zamanlı ve küresel gelişmeleri yakalayan bir şekilde başladığı bu serüven, ilk etapta kısa sürmüş ve uzun bir süreliğine sekteye uğramış oldu[22]. Sürecin sekteye uğramasıyla birlikte, Türkiye'nin 30 yılı aşkın bir süredir beklediği Kişisel Verilerin Korunması Kanunu da tasarı halinden öteye geçemedi.

Türkiye'nin bir paragrafa sığan kişisel verilerin korunması serüveninde uzun sürenin ardından Eylül 2010 referandumunda ilk defa önemli bir hukuki gelişme yaşandı. Referandum sonucunda, artık kişisel verilerin korunmasının anayasal bir hak olarak düzenlenmesine karar verildi. Böylece Anayasa'nın, özel hayatın gizliliği ve korunmasına ilişkin 20'nci maddesine yapılan bir eklemeyle, kişilerin, kişisel verilerinin korunmasını isteme; bu verilere erişme; düzeltilmesini veya silinmesini isteme hakkı anayasal olarak kabul edilmiş oldu. Yine Anayasa'da belirtildiği üzere konuya ilişkin esas ve usullerin kanun ile belirlenmesi gerekiyor. Türkiye'deki güncel durumda, kişisel verilerin korunmasına ilişkin en temel sorun da işte tam olarak bu boşluktan kaynaklanıyor; çünkü Türkiye'de halihazırda geçerli ve kapsayıcı bir kanun bulunmuyor. Hatta Türkiye'de konuya ilişkin en detaylı düzenlenmiş hukuk metinlerinden biri olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik'ti. Fakat Danıştay tarafından Anayasa Mahkemesi'ne yapılan bir başvuru ile, ilgili düzenlemenin yürürlüğünün durdurulması talep edildi. Gerekçe olarak ise, Anayasa'nın 20'nci maddesine göre, kişisel verilerin korunmasının, yönetmelikle değil kanunla düzenlenmesi gereken bir konu olduğu gösterildi. Kişisel verilerin korunması konusu şüphesiz ki uluslararası normlara ve AB müktesebatına uyumlu bir şekilde hazırlanan kapsamlı bir kanunu gerekli kılsa da, halihazırda geçerli düzenlemelerin de iptal edilmesi ve kanun çalışmalarının sonuca ulaşmamasıyla

birlikte, Türkiye'deki kişisel verilerin korunması serüveninin ileri aşamaya taşınamadığı her geçen gün, resimden biraz daha silinmesine sebebiyet veriyor.

26 Aralık 2014 tarihinde ilgili kanun taslağının TBMM'ye gönderilmesinin ardından, sürecin olumlu bir ivme kazanması bekleniyor. Fakat bu noktada taslağının içeriği de tartışılmalı. Güncel durumda, Türk Ceza Kanunu, Medeni Kanun ve sektörel yasal metinlerde, düzenlemeler dağınık şekilde gerçekleşiyor. Bu dağınıklık da genel geçer temel prensiplerin ve yaklaşımların belirlenmesini, ortak istisnalar ortaya koyulmasını zorlaştırıyor ve ulusal bir denetim mekanizmasının kurulmasını imkansız kılıyor.

3.2.Neden Türkiye'nin Acilen AB Standartlarına Uygun Veri Güvenliği Düzenlemelerine İhtiyacı Var?

Türkiye ile AB arasındaki entegrasyon sürecini, ekonomik sebepleri ve uluslararası gereklilikleri bir kenara bırakırsak, AB standartlarında bir Kişisel Verilerin Korunması Kanunu en temelde anayasal bir gereklilik ve Türk vatandaşlarının temel hak ve özgürlüklerinin garanti alınması için 21'inci yüzyılda önemli bir ölçüt. Daha önce de belirtildiği üzere, vatandaşların kişisel verilerinin korunmasına ilişkin olarak Anayasa'nın 20'nci maddesinde, bu alandaki kanun hükümleri, temel ölçüt olarak belirlenmişti. Dolayısıyla kişisel verilerin korunmasının istisnalarının belirlenmesi de bu konuya ilişkin alanı düzenleyen bütüncül bir kanunu gerekli kılıyor. Halihazırda, farklı alanlarda geçerliliğini koruyan kanunların ortaya koyduğu farklı istisnai durumlar, temel hak ve özgürlüklerin zarar görmesine sebep olabiliyor. Bu noktada, Türkiye'nin temel hak ve özgürlükler ile iç güvenlik alanlarında çıpa olarak kabul ettiği AB'nin temel sözleşmeleri arasında yer alan AB Temel Haklar Şartı da, kişisel verilerin korunmasını temel bir hak olarak 8'inci maddesi kapsamında vurguluyor.

Meselenin Türkiye-AB ilişkileri boyutuna bakıldığında, bu alanda AB standartlarında bir kanun tasarısının TBMM tarafından kabul edilmesi, Türkiye-AB Katılım Müzakerelerinin geleceği açısından hayati önem taşıyor. Bu noktada ilginç bir konunun altının çizilmesi gerekiyor. Çalışmanın hazırlık aşamasında

gerçekleştirilen geniş kaynak taramasının ardında fark edildi ki; Türkiye ile AB arasında kişisel verilerin korunması alanındaki uyuma ilişkin en geniş kapsamlı ve derin değerlendirmeler, 2008 ve 2014 yıllarında TBMM'ye sunulan kanun tasarılarının genel gerekçe bölümlerinde yer alıyor. Dolayısıyla konuya ilişkin şöyle bir çıkarımda bulunmak mümkün: Türk kanun yapıcılar ve karar vericiler konuya ilişkin yeterli ve derinlikli teknik bilgiye sahipken, bu alanda siyasi irade ve reform hevesi zayıf kalıyor. Güncel konjönktürde Türkiye'nin neden AB standartlarında bir kişisel verilerin korunması düzenlemesine ihtiyaç duyduğunu, Türkiye-AB müzakereleri açısından dört boyutta değerlendirmek mümkün. İlk olarak, Türkiye-AB müzakerelerinin temel hak ve özgürlüklere ilişkin çerçevesini belirleyen 23 numaralı fasıl kapsamındaki kriterlerin yerine getirilebilmesi için bu alanda reformların gerçekleştirilmesi gerekiyor. İkinci olarak; Adalet, Güvenlik ve Temel Haklar'a ilişkin 24 numaralı fasıl kapsamında, Türkiye ile AB arasındaki uyumun artırılması için de ilgili kanunun TBMM tarafından kabul edilmesi büyük önem taşıyor. Özellikle 24 numaralı faslın öngördüğü, tarafların adli kolluk ve sınır güvenliği birimleri arasındaki işbirliğinin artırılabilmesi için Türkiye'nin bu düzenlemeleri yapması gerekiyor. Türkiye'de kişisel verilerin korunmasına ilişkin bütüncül bir düzenlemenin bulunmaması, AB'nin adli kolluk birimleri Europol ve Eurojust ile işbirliğinin artırılması, elektronik veri paylaşımının sağlanmasının önündeki en temel engel olarak ortaya çıkıyor. Öte yandan aynı sebepten ötürü, Fransa ve Belçika gibi bir takım AB üye ülkelerle ikili güvenlik ve yargı alanında operasyonel işbirliği anlaşmaları gerçekleştirilemiyor.

Üçüncü olarak, Türkiye ile AB arasında devam eden Vize Serbestliği Diyaloğu'nda ilerleme kaydedilebilmesi için de, AB standartlarına uygun bir kişisel verilerin korunması kanununun yürürlüğe girmesi gerekiyor. Bu kapsamda Avrupa Komisyonu tarafından ortaya koyulan Vize Serbestliği Yol Haritasının ilgili kriterlerinin karşılanması için Türkiye'nin, 1981 yılında kabul ettiği 108 sayılı Sözleşme'ye ve AB Kişisel Verilerin Korunması Yönergesi'ne uyumlu reformlar gerçekleştirmesi gerekiyor. Daha da net bir ifadeyle, Türk vatandaşları için vizesiz Avrupa'nın kapılarının açılabilmesi için, Türkiye'nin bu alanda AB standartlarında bir kanun çıkarması, temel kriterler arasında yer alıyor. Türkiye-AB Vize Serbestliği Diyaloğu'nun, günümüzde Türkiye-AB ilişkilerinde ilerlemeye en açık ve en önemli boyutlardan birini oluşturduğunu dikkate alırsak, bu konunun önemi bir kez daha ortaya çıkıyor.

Türkiye'nin AB standartlarında kişisel verilerin korunması düzenlemeleri gerçekleştirmesini gerekli kılan son boyutu ise, Türkiye ile AB arasındaki ekonomik işbirliği. Uluslararası ticaretin dijital ortama taşınması ve verilerin ticari değerindeki artış, küreselleşen ticaretin önemli bir unsuru haline geldi. AB merkezli şirketlerin Türk paydaşları ile etkin ticareti ve AB merkezli sermayenin Türkiye'deki yatırımlarını etkin şekilde yönetebilmesi için, Türkiye'de işler halde bir veri güvenliği mevzuatı şart. Aynı şekilde Türk iş adamlarının yurt dışındaki paydaşları ile yatırımlarına ve ortaklıklarına ilişkin veri paylaşımının önünün açılması için etkin veri güvenliği büyük önem taşıyor[57]. Gümrük Birliği'nin revizyonunun hız kazandığı bir dönemde, farklı ülkeler ile Serbest Ticaret Anlaşmaları imzalama gayreti gösteren, TTYO'ya dahil olmayan çalışan Türkiye için, haliyle bu konu çok daha fazla önem kazanıyor.

3.3.İlgili Kanun Tasarısının Getirdikleri ve Zamanı İleri Almak

Çalışmanın başında örnek olarak kullandığımız "Geleceğe Dönüş" filmi metaforuyla devam edecek olursak, filmin ana karakteri Marty Mcfly (Michael J. Fox), 1985 yılından, 1955 yılına yolculuk ederek, 30 yıl geriye gidiyordu. Bilindiği üzere Türkiye'de 108 sayılı Sözleşme'nin imzalanması ile başlayan kişisel verilerin korunması serüveni de 30 yılı geride bırakmış durumda.

Filmde Marty Mcfly, ailesinin geleceğini kurtarabilmek ve aile fotoğraflarının silinmesini önleyebilmek için ebeveynlerinin 30 yıl önceki hallerini bulup onları bir araya getiriyordu. Böylelikle ailesi, 1985 yılında bir arada, mutlu şekilde hayatlarını sürdürüyor ve aile fotoğraflarında bütün aile bireyleri tekrardan görünür hale geliyordu. Filmden farklı olarak, Türkiye'de, "aile fotoğrafından silinmekte olan" kişisel verilerin korunması reformunu gerçekleştirebilmek için 30 yıl önceye veya ilgili AB yönergesinin imzalandığı tarihe geri dönmek gerekmiyor. Aynı şekilde, etkin düzenlemeler gerçekleştirmek için de zaman yolculuğuna hiç gerek yok. Güncel uluslararası düzenlemeleri ve AB müktesebatını dikkate alarak, hızlı davranarak ve kamu-iş dünyası ve sivil toplum diyaloğunun etkin bir örneğini sergileyerek, geçmişte kaybedilen zaman telafi edilebilir ve günümüzün uluslararası yapısına ve insan hakları normlarına uygun bir kanun oluşturulabilir. Öte yandan filmle benzer olarak, Marty Mcfly'ın ailesinin mutluluğu ve birlikteliği için 1955 yılında gerçekleştirdiği aksiyonların 1985 yılında ailesinin mutluluğunu ve

huzurunu olumlu etkilediği gibi, Türkiye'nin de kişisel verilerin korunmasına ilişkin bugün atacağı olumlu ileri adımlar, Türkiye'de temel insan haklarının ve AB katılım müzakerelerinin geleceği için önemli etkiler yaratacak. Dolayısıyla tasarı halindeki kanun metninin içeriği, geçmişten bağımsız şekilde büyük önem taşıyor.

26 Aralık 2014 tarihinde TBMM'ye gönderilen, 9 bölümden oluşan kanun tasarısı, kişisel verilerin işlenmesinin disiplin altına alınmasını ve temel hak ve özgürlüklerin korunmasını amaçlıyor. Kanun, kişisel verileri işlenen kişilerin ve işleyen tüzel kişilerin durumunu düzenliyor. İlgili kanun tasarısı, kamu sektörü ve özel sektöre ilişkin bir ayrımda bulunmuyor. Taslağın yasalaşmasıyla birlikte, kişisel veriler sadece bu kanunda ve diğer kanunların ilgili hükümlerinde öngörülen usul ve esaslara dayanarak işlenebilecek. Tasarıya göre kişisel verilerin işlenmesine ilişkin en temel ölçüt, **kişisel verilerinin işlenmesi öngörülen kişinin açık rızası.** Açık rızadan kasıt; özgürce, yeterli bilgiye dayanarak, tereddüte yer bırakmayacak açıklıkta, sadece belirtilen işlem için gösterilen rızadır. Tasarıda belirtildiği üzere kişinin, rızasını istediği zaman geri çekme hakkı bulunmakla birlikte, rızanın Türkçe olarak ifade edilmesi de şart değil. Tasarıya göre 18 yaşından küçükler için kişisel verilerin işlenmesine ilişkin rızayı gösterme kararı ebeveynlere bırakılmış durumda. Bunların yanında, kişisel verisi işlenen gerçek kişiler, veriyi işleyenlerin yaptığı hataların düzeltilmesini talep etme, verinin geri çekilmesini talep etme, verinin silinmesini talep etme ve veri depolayan bu tüzel kişilerin verileri depolayıp-depolamadığını sorgulama hakkına sahip.

Öte yandan belirli istisnai hallerde, kişisel verilerin, kişinin açık rızası olmadan da işlenebilmesi öngörülüyor. Tasarıda düzenlendiği haliyle, kişinin rızası olmadan kişisel verilerin işlenebilmesi için aşağıdaki istisnai durumlardan en az birinin gerçekleşmesi gerekiyor:

- Kanunlarda açıkça öngörülmesi,
- Kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya iflası için taraflara ait kişisel verilerin işlenmesinin zorunlu olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

- Bir hakkın tesisi, kullanılması veya korunması için verinin işlenmesinin zorunlu olması,
- Kendisine ilişkin kişisel verinin, kişinin kendisi tarafından kamuoyuna açıklanması.

3.4.Tasarının Öngördüğü Denetim Mekanizması: Kişisel Verileri Koruma Kurulu

Türkiye ile AB arasında sürmekte olan katılım müzakerelerinin temel hak ve özgürlükler ile güvenlikli alanlarındaki en temel kriterlerinden biri, kişisel verilerin korunmasına ilişkin etkin bir kanunun oluşturulmasının yanı sıra, sürecin etkinliğinden ve kontrolünden sorumlu bir denetim mekanizmasının da kurulması. İlgili tasarıda düzenlendiği üzere, kişisel veriyi işleyen sorumlu tüzel kişiler gerekli önlemleri almadığı ve veri sahibinin taleplerine karşılık vermediği takdirde, veri sahibi kişiler, 30 gün içerisinde Kişisel Verileri Koruma Kuruluna başvurma hakkına sahip. Dolayısıyla Kurulun yapısı, Türkiye'de kişisel verilerin korunması konusundaki seviyenin belirlenmesi için büyük önem taşıyor.

Kurulun yapısı, tasarının 6'ncı bölümünde düzenleniyor. 7 üyeden oluşması öngörülen kurulun, 2 üyesi mesleğinde en az 10 ay deneyimli avukat veya hakim, 1'i 10 yıl deneyimli öğretim üyesi, 4'ü kamuda veya özel sektörde en az 10 yıl çalışmış kişiler arasından Bakanlar Kurulu tarafından seçiliyor. Kurulun, Adalet Bakanlığı'yla işbirliği içerisinde ve bağlantılı şekilde çalışması, ilgili kanunla düzenlenmiş durumda. Öte yandan tasarıya göre Kurulun görev ve yetkilerini bağımsız ve kendi sorumluluğu altında yerine getirmesi gerekiyor.

Tasarının yasalaşmasıyla birlikte kurulması öngörülen Kişisel Verileri Koruma Kurulu'nun görevleri ise şu şekilde sıralanıyor:

- Kişisel verilerin Kanun hükümlerine uygun işlenmediğine dair ihbar ve şikayetlere ilişkin inceleme veya denetleme yapması;
- Telafisi güç veya imkansız zararlar oluşması ihtimali doğduğu takdirde geçici önlemler alması;
- Kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemler gerçekleştirmesi;

- Ulusal ve uluslararası paydaşlarla işbirliği kurması;
- Diğer kurum ve kuruluşlar tarafından hazırlanan kişisel verilerin korunmasına ilişkin düzenleme içeren mevzuat hakkında görüş vermesi;
- Kanunla öngörülen idari yaptırımlara karar vermesi;
- Konuya ilişkin gelişmelerin takip edilmesi araştırmaların, incelemelerin ve eğitimlerin icrası;
- Kanunla öngörülen diğer görevleri gerçekleştirmesi.

3.5.Tasarının Getirdikleri ve Üçüncü Ülkelere Veri Transferine ilişkin Gelişmeler

Türk hukuk sisteminde, Türk Ceza Kanunu'nun kişisel verilerin hukuksuz toplanması ve transferine ilişkin genel hükümleri haricinde, üçüncü ülkelere veri transferine dair kapsamlı düzenleme bulunmuyor.

Tasarıda öngörüldüğü üzere, herhangi bir kişisel verinin üçüncü ülkelere aktarılabilmesi için en temel kriter kişinin açık rızası. Öte yandan, sadece açık rızanın gerekmediği istisnai hallerde, verinin üçüncü ülkelere aktarılabilmesi için ilgili ülkedeki kişisel verilerin korunması düzenlemelerinin ve altyapısının yeterli seviyede olması da gerekiyor. İlgili üçüncü ülkede yeterli veri güvenliği bulunmadığı hallerde, verinin üçüncü ülkeye aktarılabilmesi için iki ülkede de yer alan veri sorumlularının karşılıklı taahhüdü, kişinin açık rızası ve Kişisel Verileri Koruma Kurulu'nun izni gerekiyor. Öte yandan tasarıya göre, özel nitelikli verilerin (*sensitive data*) yeterli veri güvenliği bulunmayan ülkelere aktarımı söz konusu değil; bu tür verilerin sadece kanunlarda özellikle öngörüldüğü hallerde, yeterli koruma bulunan ülkelere aktarımı mümkün.

Özel nitelikli verinin paylaşımına ilişkin açık rızanın olduğu hallerde ise Kurulun izni dahilinde bu veriler üçüncü ülkelere aktarılabiliyor. Kişisel Verileri Koruma Kurulu'nun yapısı ve yetkinliği, bu konuda da büyük önem taşıyor; çünkü verinin aktarılması öngörülen üçüncü ülkelerde etkin bir korumanın olup olmadığı, Kurul tarafından verilen kararla belirleniyor.

Yukarıda belirtilen, tasarı halindeki bu düzenlemeler, yürürlüğe girdikleri takdirde şüphesiz ki Türkiye'de kişisel verilerin korunması alanında bir standardın

ve güven ortamının oluşmasını sağlayacak. Öte yandan güncel konjönktürde, sivil toplum temsilcileri, iş dünyası ve akademi çevreleri tasarıyı düzenli olarak eleştirmeye ve tasarının eksiklerini işaret etmeye devam ediyor. Dolayısıyla bu durum, tasarının AB standartlarına uygun olup olmadığı konusunda soru işaretleri yaratıyor. "Geleceğe Dönüş" filminde, Marty Mcfly, 30 yıl geri gidip, 1955'te krizleri öngörülenden de başarılı şekilde aştıktan sonra 1985'e döndüğünde, ailesinin eskisinden de iyi durumda olduğu bir tabloyla karşılaşıyordu. Aynı şekilde Türkiye'nin geçmişte kaybettiği zamanı telafi etmesi için, geleceği de dikkate alarak, öngörülenden de ileri düzenlemeler gerçekleştirmesi gerekiyor. Türkiye-AB katılım müzakereleri, çoğu zaman AB'nin Türkiye'ye yönelik taleplerini düzenli olarak artırdığı ve seslendirdiği bir süreç. Dolayısıyla özellikle temel hak ve özgürlükler alanında tartışmaların önüne geçebilmek için AB'nin talep ettiğinin ötesinde düzenlemeler gerçekleştirilmesi (*better regulations*), müzakerelerde Türkiye'nin elini çok daha güçlendirebilir. Özellikle kişisel verilerin korunması gibi, ileri standartların ve uluslararası iyi örneklerin bulunduğu bir alanda, halihazırda üzerinde çalışmalar süren tasarının eksiklerinin giderilmesi, ve iyi örnek ve uygulamaların dikkate alınması gerekiyor.

3.6.Tasarıya ilişkin Temel Çekinceler

2003 yılında, AB müktesebatının üstlenilmesine ilişkin Türkiye Ulusal Programı'na da aktarıldığı üzere, Türkiye'nin veri güvenliği alanında ulaşmayı hedeflediği seviye AB normlarıdır. Dolayısıyla tasarı halindeki kanunun eksik kaldığı yönler değerlendirilirken, AB Kişisel Verilerin Korunması Yönergesi, tasarı halindeki Kişisel Verilerin Korunması Tüzüğü ve AB'de sürmekte olan güncel tartışmaların da dikkate alınması gerekiyor. Türkiye'de tasarıya ilişkin en yoğun tartışmalar ve eleştiriler temelde üç konu etrafında şekilleniyor:

- Tasarı kapsamında rıza kavramının nasıl ele alındığı;
- Kişisel verilerin izinsiz işlenebileceği istisnai haller;
- Kişisel Verileri Koruma Kurulu'nun yapısı.

Daha önce belirtildiği üzere açık rıza, kişisel verilerin işlenebilmesi için en temel kriterlerden birini oluşturuyor. Bu konuda tasarıya ilişkin eleştiriler, açık rıza tanımının metinde net bir şekilde yer almadığı yönünde. Öte yandan rızaya

ilişkin koşullar, ilgili AB mevzuatında ayrı bir maddede düzenlenmiş durumda. Dolayısıyla AB müktesebatıyla uyum ve muğlaklığın giderilmesi açısından, konunun temel hak ve özgürlüklere ilişkin en önemli boyutunu oluşturan açık rıza konusunda, net tanım ve unsurlar ortaya koyulmalı.

Açık rıza, kişisel verilerin işlenebilmesi için tek şart değil. Tasarının 5'inci maddesinde öne sürülen 6 unsurdan en az birinin oluştuğu hallerde de kişisel veriler işlenebiliyor. Bu unsurlar arasında kamuoyunda en fazla tartışılan ve AB normları ile uyum açısından tartışma yaratabileceği öne sürülen unsur, "kanunlarda açıkça öngörülme" hali. Kanunlarda açıkça öngörülme halinin kapsamının çok geniş olduğu ve suiistimale açık olabileceği değerlendirilebilir. Kanunlarda açıkça öngörülme hali, ilgili hükümlerin yer aldığı kanunlar düzenlendiği takdirde kamu kurumları tarafından her türlü amaçla kişisel verilerin işlenebilmesi ve kişilerin özel verilerine ulaşılabilmesi ihtimalini doğuruyor. Bu çerçevede örneğin, 6532 sayılı MİT Kanunu'na, 17 Nisan 2014 tarihinde getirilen değişikliklerle; dış istihbarat, milli savunma, terörle mücadele, uluslararası suçlar ve siber güvenlikle ilgili MİT'in yürüttüğü bütün görevlerde, kamu kurum ve kuruluşlarının, kamu niteliğindeki meslek kuruluşlarının, Bankacılık Kanunu kapsamındaki meslek kuruluşlarının ve diğer düzel kişi ve tüzel kişiliği bulunmayan kurumların, MİT tarafından talep edildiği takdirde her türlü veriyi sağlaması zorunluluğu getirildi. Dolayısıyla MİT tarafından kişisel verilerin kullanılması, MİT Kanunu'nda da öngörüldüğü için, Kişisel Verilerin Korunması Kanun Tasarısı'na göre de meşru istisnai haller arasında kabul edilecek. Bu durum, ulusal güvenlik ile kişi temel hak ve özgürlükleri arasındaki dengenin bozulacağı durumlar oluşmasına sebep olabilir.

İkinci olarak, Tasarının 6'ncı maddesine göre, "sır saklama yükümlülüğü altında bulunan kişiler tarafından işlenmesi" de özel nitelikli verilerin işlenebileceği istisnai haller arasında yer alıyor. Sır saklamakla yükümlü kişilere örnek olarak Tasarının gerekçesinde, Sağlık Bakanlığı ve Sosyal Güvenlik Kurumu gösteriliyor. Öte yandan Tasarıyı eleştiren çevreler, bu kapsama MİT, Jandarma ve Emniyet gibi istihbarat ve güvenlik birimlerinin de girebileceğini öne sürüyor. Dolayısıyla, özel nitelikli verilerin hangi kişiler tarafından işlenebileceğinin, güvenlik ve özgürlük arasındaki dengenin sağlanabilmesi için daha net tanımlanması gerekiyor. Unutulmamalıdır ki AB'nin bu konuya son dönemde verdiği önemin

en temel sebebi, teknolojik gelişmelerle birlikte artan hukuksuz dinlemelerin ve fişlemelerin önüne geçilmesi ve kişi mahremiyetinin etkin şekilde korunabilmesi. Bu çerçevede ilgili AB Yönergesi ve tasarı halindeki Tüzük, ifade özgürlüğünü de düzenlemelerin merkezine koyuyor. Dolayısıyla tasarı dahilinde kişisel verilerin işlenebileceği ve işlenmesinin yasak olduğu haller düzenlenirken de AB normlarına uyuma yönelik olarak; ifade özgürlüğü vurgusu çok daha net bir şekilde yapılmalı.

Tasarıya ilişkin tartışılan konulardan bir diğeri şüphesiz ki, tasarıyla birlikte kurulması öngörülen Kişisel Verileri Koruma Kurulu'nun yapısı. Türkiye'de gerçek ve tüzel kişilerin, kişisel verileri işleyebilmek için müracaat etmesi gereken ve bu müracaatları kayıt altına alınan bir kurum bulunmuyor. Aynı şekilde kişisel verilerin işlenmesi süreçlerini kontrol eden ve denetleyen bir kurum da mevcut değil. Tasarının 6'ncı bölümü bu gereklilikleri karşılayacak bir kurulun oluşturulmasına ve oluşturulacak bu kurulun yapısına ilişkin hükümleri içeriyor. Tasarı halindeki Kanunun 6'ncı bölümü incelendiği takdirde, ilgili AB Yönergesi ile uyumunun tartışmalı olduğu bir takım hükümler göze çarpıyor.

İlgili AB Yönergesi ve AB ülkelerinin ulusal düzenlemeleri, ulusal kişisel verileri koruma mekanizmalarının tam bağımsız olması gerektiğini vurguluyor. Fakat tasarının yasalaşmasıyla birlikte oluşturulacak bu Kurulun giderleri, Adalet Bakanlığı'na bağlı bir bütçeden karşılanacak. Dolayısıyla Kurulun mali açıdan bağımsızlığı, önümüzdeki dönemde tartışılacak konular arasında yer alacak. Kurulun yapısına ilişkin ikinci tartışmalı konu ise, Kurulun üyelerinin hangi yetkili makamlar tarafından belirleneceği. Tasarıda belirtildiği üzere 7 kişiden oluşması öngörülen Kurulun 4 üyesinin Bakanlar Kurulu tarafından atama usulüyle göreve getirilmesi öngörülüyor. Elbette ki, 4 üyenin Bakanlar Kurulu tarafından belirlenecek olması, Kurulun tam bağımsız olmayacağı anlamına gelmiyor. Ancak bu konuya ilişkin daha açık değerlendirmeler yapılabilmesi için, Kurulun uygulamalarının ve işleyişinin görülmesi gerekiyor. Bu çerçevede, Kurulun olabildiğince akademi çevrelerini, iş dünyasını ve sivil toplumu kapsayıcı paydaşlar tarafından belirlenmesi, konuya ilişkin mesleki yeterlilik ve tecrübe aranması ve daha kapsamlı bir oylama süreci öngörülmesi, Kurulun etkin işleyişinin garanti altına alınması için dikkate alınmalı. Nihayetinde, Türkiye'nin AB ülkeleri tarafından kişisel verilerin korunması alanında güvenilir ülke statüsü kazanması

ve Türkiye ile AB arasında etkin veri transferinin mümkün olabilmesi için AB'nin gözettiği kriterlerin başında tam bağımsız ve etkin bir kişisel verileri koruma mekanizmasının kurulması yer alıyor. Bu mekanizmanın yapısına ilişkin olarak bir standart oluşturulması konusu, son dönemde AB gündeminin de merkezinde.

4.AVRUPA TEK DURAK MEKANİZMASINI TARTIŞIYOR

12-13 Mart 2015 tarihlerinde gerçekleştirilen AB Adalet ve İçişleri Konseyi Toplantısı'nda, uluslararası ticari ilişkileri doğrudan etkileyecek önemli bir konuya ilişkin anlaşmaya varıldı. AB Adalet ve İçişleri Bakanları, kişisel verilerin korunması alanında AB çapında geçerli bir denetim mekanizmasının kurulmasına (tek durak mekanizması, *one stop shop mechanism*) ve veri akışında AB'nin denetimi tek elden yürütmesine karar verdi. Böylelikle bürokratik engellerin önüne geçilmesi, veri akışının hızlanması, konuya ilişkin hukuki çerçevenin belirginleştirilmesi ve dijital ekonominin güçlendirilmesi hedefleniyor.

Bilindiği üzere, AB çapında hâlihazırda geçerli Kişisel Verilerin Korunması Yönergesi yerine, daha kapsamlı bir tüzüğün hazırlık çalışmaları, 2012 yılından beri devam ediyordu. Kurulması öngörülen tek durak mekanizmasıyla bir ticari işletme, eğer 28 AB ülkesinin tamamında operasyonlarını sürdürüyorsa, kişisel verilerin korunmasıyla ilişkili sorunlarda, merkezinin bulunduğu AB ülkesindeki tek yetkili veri güvenliği kurumuyla etkileşime girecek. Aynı şekilde, eğer üye ülkelerin birinde kayıtlı olan bir şirket örneğin bir İspanyol şirketi, başka bir AB ülkesindeki kişilere ilişkin verileri hukuka aykırı şekilde kullanırsa, kişilerin bu İspanyol şirketine karşı hukuki işlem başlatabilmeleri için İspanya'ya gitmeleri gerekmeyecek; kendi ülkelerindeki yetkili kuruma başvurmaları yeterli olacak[23]. Üzerinde anlaşma sağlanan metinde, kişisel veri sahibi için en etkili korumanın sağlanmasının hedeflendiği ifade ediliyor. Adalet ve İçişleri Konseyi Toplantısı'nın ardından yapılan basın açıklamasında da, tek durak mekanizmasıyla birlikte, uluslararası işletmelerin gereksiz maliyetlerden kurtarılacağının, böylelikle de dijital ekonominin büyümesine katkı sağlanacağının altı özellikle çiziliyor.

Avrupa Komisyonu'nun Adalet, Tüketici ve Cinsiyet Eşitliğinden Sorumlu Üyesi Věra Jourová da tek durak mekanizmasının şirketlerin hayatını kolaylaştıracağı

görüşünde. Konunun temel haklar boyutuyla ilgili olarak Jourova, vatandaşlara, kişisel verilerin korunmasından sorumlu, kendilerine en yakın yetkili kuruma başvurma hakkının sağlanmasıyla, AB çapında daha fazla koruma ortamının oluşacağının altını çiziyor. Jourová'nın ifade ettiği üzere, temel unsurunu tek durak mekanizmasının oluşturduğu veri güvenliği reformunun gerçekleşmesi, Dijital Tek Pazar'a geçilmesi ve dijital ekonomiden tam verimin alınabilmesi için kilit önem taşıyor[24].

Konsey'in konuya ilişkin yaklaşımıyla ilgili olarak ise, önemli eleştiriler yöneltiliyor. Özellikle, Konsey'in, şirketlerin çıkarlarını, özel yaşamın gizliliği hakkının üzerinde tuttuğu yönünde eleştiriler var. AP'ye ise sivil toplum kuruluşlarının, özellikle temel hakların güçlendirilmesi yönünde yoğun baskı yaptığı biliniyor. Dolayısıyla tek durak mekanizmasının kurulmasına yönelik nihai karar, hukuki ve ticari boyutun ötesinde siyasi olarak Konsey ile AP arasında gerçekleşecek müzakerenin ardından netleşecek[25].

Konunun siyasi boyutunun ötesinde AB ülkelerinde iş yapan tüm şirketler için aynı veri güvenliği kurallarının geçerli olmasının ve AB ülkelerinin tamamının bu kurallara uyum sağlamasının, şirketlere yıllık 2,3 milyar avroya kadar tasarruf sağlayacağı öngörülüyor. Öte yandan AB ülkelerinde işlemlerini sürdüren şirketlere, müşterilerine ortak hukuk kurallarına dayanan bir güvence sunma fırsatı sağlanacak[26]. Fakat bu noktada, AB kurumlarının veri güvenliği reformuna ilişkin duruşu net: "her şey üzerinde anlaşılmadan, hiçbir şey üzerinde anlaşmaya varılmış sayılmaz"[27].

Konsey Toplantısı'nda varılan, AB çapında veri akışı denetiminin tek elden yürütülmesi yönündeki anlaşma sonrasında gözler, AB ülkelerindeki ulusal karar vericilere ve küresel iş çevrelerine çevrildi. Bazı AB üye ülkelerinin ulusal yetkili makamları, Apple ve Facebook gibi büyük teknoloji şirketleri üzerindeki yargı yetkilerini kaybedecekleri için, öngörülen sistemi olumsuz karşılıyor. Örneğin, pek çok uluslararası bilişim şirketine ev sahipliği yapan İrlanda, geçtiğimiz dönemde işletmeler için hukuki açıdan diğer AB üye ülkelerine oranla daha cazip geliyordu. Apple, Google ve IBM gibi büyük teknoloji şirketlerinin oluşturduğu Veri Güvenliği Sanayi Koalisyonu, tasarı aşamasında bulunan bu mekanizmanın eski sistemden daha hantal işleyeceği ve gereksiz idari yük oluşturacağı görüşünde.

Tüzüğün, AB'de varlığını sürdüren üçüncü ülke şirketlerini doğrudan etkilemesi bekleniyor. Düzenlemelerin doğrudan etkileyeceği şirketlerin başında ise AB sınırları içerisindeki tüketicilerin kişisel verilerini işlemekte olan ABD şirketleri yer alıyor. ABD Başkanı Barack Obama, çeşitli AB çevrelerinin kişisel verilerin korunmasına ilişkin korumacı yaklaşımının ulusal ticari çıkarlara dayandığı görüşünde. AB içerisinde, AP ve Alman kanun yapıcıların başını çektiği bir grup ise, AB vatandaşlarının kişisel verilerinin Amerikan şirketleri tarafından işlenmesinin önünü açan anlaşmanın sonlandırılmasına yönelik baskılarını sürdürüyor[28]. Öte yandan başını ABD'li şirketlerin çektiği iş dünyası temsilcilerinin çağrısı, AB'de veri kaynaklı ekonomik ve sosyal kazanımların artmasını sağlayan özgürlükçü ve esnek politikalar geliştirilmesi ve veri hizmetlerinin yerelleştirilmesinin önüne geçilmesi yönünde[29].

Önümüzdeki günlerde Avrupa'da gündemi çok daha fazla meşgul edeceği kesin olan tek durak mekanizmasına ilişkin tartışmaların Türkiye'de nasıl yankılandığına bakılırsa, tartışmaların Türkiye'de duyulduğu bile şüpheli. Türkiye, AB'nin tek durak mekanizmasına hiçbir mekanizmayla cevap veremiyor. AB ile katılım müzakerelerine devam eden, AB'ye vizesiz seyahat hedefine ulaşmaya her zamankinden daha yakın olan, Gümrük Birliği'nin güncellenmesi ve TTYO'ya dahil olunması yönünde azami gayret gösteren Türkiye'nin, kişisel verilerinin korunmasına ilişkin bağımsız bir denetim mekanizması kurması, temel bir zorunluluk.

4.1.AB'nin Tek Durak Mekanizmasına Türkiye'den Bakış

AB çapında geçerli Kişisel Verilerin Korunması Yönergesi gereğince, Türkiye ve AB arasında etkin veri transferinin sağlanabilmesi için, Türkiye'nin AB standartlarında hukuki düzenlemeler gerçekleştirmesi, başka bir deyişle "güvenilir ülke" statüsü kazanması gerekiyor. Türkiye'nin, AB ile ticari ilişkilerin güçlendirilmesine önemli katkılar sağlaması öngörülen güvenilir ülke statüsüne sahip olabilmesi için temel şartlardan biri, kurulacak olan veri koruma otoritesinin **tam bağımsızlığı.** AB standartlarına göre, veri güvenliğinden sorumlu kurumların bağımsız üyelerle, tamamen bağımsız şekilde çalışması gerekiyor. TÜSİAD, 19 Ocak 2015 tarihinde kamuoyuyla paylaştığı görüşünde, Kurul üyelerinin doğrudan Bakanlar Kurulu tarafından belirlenmesini eleştirmiş ve ilgili temsil

kuruluşları, sektör temsilcileri ve yargı gibi geniş bir kesimin göstereceği adayların TBMM'de nitelikli çoğunlukla seçildiği bir yapıyı tavsiye etmişti[30]. Dolayısıyla Türkiye'nin hazırlayacağı kanunun genel çerçevesi ve uygulamadaki temel yaklaşımlar, Türkiye'nin güvenilir ülke statüsü kazanıp kazanamayacağı konusunda belirleyici olacak.

AB'nin 1995'ten bu yana düzenleme yaptığı kişisel verilerin korunması ve dolaşımı, günümüzde uluslararası asimetrik çatışmaların ve istihbarat haberlerinin ana temasını oluşturmakla da kalmıyor. Önümüzdeki dönemin en önemli ticari trendleri arasında yer alan mega ticaret anlaşmalarının temel müzakere başlıklarından da birini oluşturuyor.

5.TTYO MÜZAKERELERİNDE KİŞİSEL VERİLER: ODADAKİ FİL Mİ? YENİ PETROL MÜ?

5.1.21'inci Yüzyılın Yeni Petrolü: Veriler

Kişisel verilerin korunması, AB tarafından temel hak ve özgürlükler arasında kabul edilse de; isim, kredi kartı bilgileri, doğum tarihleri, e-posta adresleri ve telefon numaraları gibi çeşitli kişisel veriler, uluslararası ticaretin de önemli bir parçası. Kişisel verilerin ticaretteki önemi, bilişim ve iletişim teknolojilerindeki hızlı gelişmeyle birlikte uluslararası tartışmaların her geçen gün daha da merkezine oturuyor. Veriler, şirketlerin, tüketicilerin eğilimlerini anlamak için kullandığı iyi bir araç, bunun yanı sıra ürünün de kendisi haline geliyor. Avrupa Komisyonu'nun Adalet ve İçişlerinden Sorumlu Eski Üyesi Viviane Reding, Kasım 2013 tarihinde konuya ilişkin yaptığı açıklamada, 2020 yılında AB vatandaşlarının kişisel verilerinin değerinin yıllık 1 trilyon avroya ulaşacağını ifade etmişti[31]. Öte yandan pek çok güncel tartışmada, kişisel verilerden, yeni bir para birimi hatta **yeni petrol** olarak bahsediliyor.

Kişisel verilerin uluslararası ticaretteki konumuna bağlı olarak, bu alanda AB vatandaşlarının temel haklarının garanti altına alınıp alınamadığı yönündeki kaygılar da artıyor. Avrupa Komisyonu'nun konuya ilişkin kamuoyu algısını ölçmek üzere gerçekleştirdiği 24 Haziran 2015 tarihli Eurobarometre anketinin

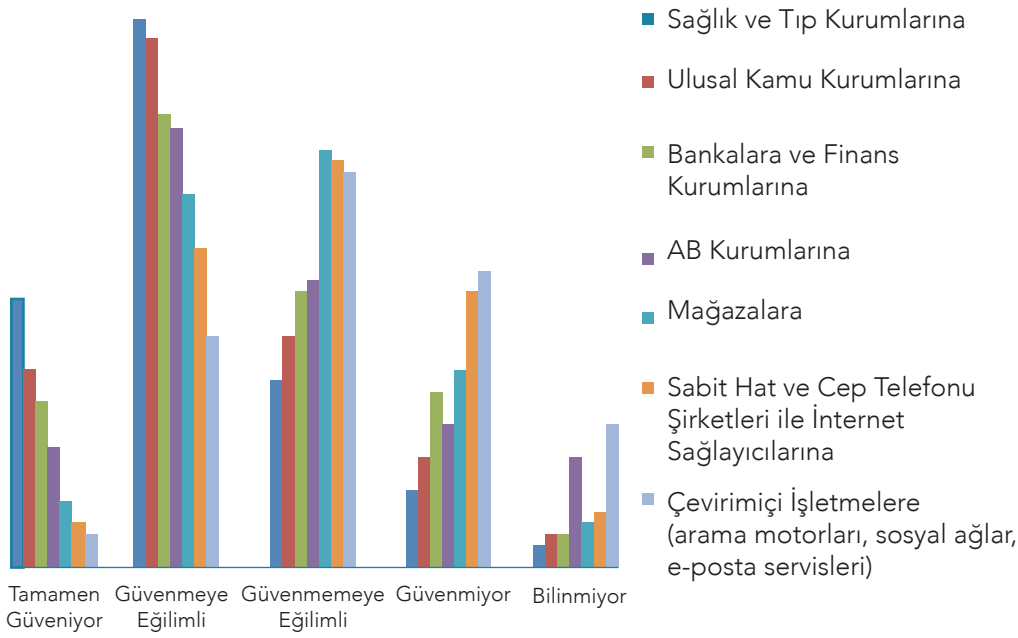
sonuçlarına göre, AB vatandaşlarının sadece %4'ü, internet sağlayıcılarının ve telefon şirketlerinin, kişisel verilerini koruduğuna tamamen güveniyor. Öte yandan katılımcıların sadece %3'ü arama motorlarının ve sosyal ağların AB vatandaşlarının kişisel verilerini koruma altına aldığını düşünüyor[32].

5.2.Odadaki Fil: Kişisel Verileri Müzakere Etmek

Güncel konjönktürde, uluslararası ticaret kapsamında karşılıklı veri akışının en yoğun gerçekleştiği coğrafyalar ABD ve AB. ABD tarafından paylaşılan resmi rakamlara göre, ABD ile AB arasındaki mal ve hizmet ticareti, yıllık 1.06 trilyon dolara ulaşmış durumda. Başka bir ifadeyle, dünya çapında bir yıl içerisinde gerçekleşen uluslararası ticaretin üçte biri, ABD ile AB arasında. Öte yandan 2010 yılı verilerine göre, ABD'de dijital ortamda sunulan hizmetler, ABD'nin toplam hizmet ihracatının yüzde 61'ini oluşturuyor. Dolayısıyla, ABD ile AB arasındaki karşılıklı ticarette hukuki engellerin kaldırılmasını ve mevzuatı karşılıklı olarak uyumlaştırılmasını öngören, mega ticaret anlaşması müzakereleri TTYO'nun da en tartışmalı ve kritik alanlarından biri, veri akışı ve veri güvenliği meselesi. Uluslararası ticaret sisteminde köklü değişikliklere sebep olması öngörülen TTYO müzakerelerinde; e-ticaret, bulut bilişim, fikri mülkiyet, uluslararası mali veriler ve PNR gibi konular tartışılırken kişisel verilerin korunması ve gizlilik meselesinin mutlak suretle masada olduğu aşikar. Fakat temel hak ve özgürlükler boyutundan dolayı, konunun TTYO kapsamına girmediği mesajı verilerek, bir süredir deyim yerindeyse "top taca atılıyor". Yapılan yorumlarda, TTYO müzakereleri kapsamında kişisel verilerin korunması tartışmalarından "odadaki fil" veya müzakerelerin "olağan şüphelisi" olarak bahsediliyor.

Portekiz merkezli bir düşünce kuruluşu olan *Lisbon Council ve Progressive Policy Institute* işbirliğiyle hazırlanan bir çalışmaya göre ise, AB'nin dört büyük ekonomisini oluşturan Fransa, Almanya, İtalya ve İspanya, dijital verileri işleme ve veri akışı kapasitelerini İngiltere seviyesine ulaştırırsa, ulusal ekonomilerine yıllık %2 oranında, ABD seviyesine ulaştırırsa da yıllık yüzde dört oranında katkı sağlamış olacak[34]. Diğer yandan mesele, sadece transatlantiğin iki tarafındaki devletlerin çıkarlarını ilgilendiren bir konu olmanın çok ötesinde bir boyut kazandı. Uluslararası pazarın %85'ini oluşturan ABD merkezli, Google, Amazon gibi bulut bilişim şirketleri ve bağlantılı diğer sektör temsilcileri; AB'nin Gümrük Birliği ortağı Türkiye gibi,

Tablo 4: AB Vatandaşları, Kişisel Verilerinin Korunmasına ilişkin Hangi Kurumlara Güveniyor?[33]



taraflarla geniş kapsamlı ikili ticaret anlaşmaları yürüten ülkeler; Çin, Rusya, Brezilya, Hindistan, Güney Afrika gibi, yakın gelecekte internet ve küresel bilişim sektörüne ilişkin konularda karar verici konuma gelmeyi hedefleyen ülkeler de sürecin etkilerini kestirmeye çalışıyor. Açık toplum, insan hakları, gizlilik hakkı ve yolsuzlukla mücadele gibi alanlarda çalışmalarını sürdüren uluslararası sivil toplum ve Avrupa değerlerinin korunduğunu garanti altına almaya çalışan AP de müzakerelerin veri güvenliği boyutunu, taraflar kadar yakından ve ilgiyle takip ediyor.

Mega ölçekte bir ticaret anlaşmasına, kişisel verilerin korunması gibi hak temelli bir konuyu eklemenin şüphesiz ki büyük zorlukları var. Ticaret anlaşmaları, ruhu gereği, taraflar arası uyumun artırılması ve engellerin kaldırılmasını hedeflerken, bu kapsamda kişisel verilerin korunması gibi hak temelli ve taraflar arası yaklaşım farklılığı bulunan konularda standartlar belirlemek oldukça zor[35]. Kişisel verilerin korunmasına ilişkin olarak AB, kapsayıcı ve kuralcı bir yaklaşım benimserken; ABD'de konuya ilişkin kapsayıcı bir düzenlemenin bulunmamasının

yanı sıra, konuya ilişkin düzenlemeler sektörel bazda gerçekleşiyor ve eyaletlere göre farklılık gösteriyor[36]. Hal böyle olunca, güncel gelişmelerle de birlikte, müzakerelerin tarafları, müzakere turlarını her fırsatta bu sorunun kenarından dolanarak geçmeyi tercih ediyor.

5.3.İnce Çizgi: İnsan Hakları

TTYO müzakerelerinin tarafları, kişisel verilerin korunması meselesini gündeme getirmemeye meyilli olsa da özellikle AB, yakın geçmişte bu konuda oldukça net değerlendirmelerde bulundu. Avrupa Komisyonu'nun Adalet ve İçişlerinden Sorumlu eski Üyesi Viviane Reding, veri güvenliği konusunun TTYO kapsamında müzakere edilmeyeceğini, insan haklarıyla bağlantılı bu konunun bir ticaret anlaşmasından bağımsız ele alınması gerektiğini belirtmiş, üst düzey AB yetkilileri de bu yaklaşımı zaman zaman vurgulamıştı. Hatta, Avrupa Komisyonu'nun AB kamuoyunu TTYO müzakerelerinde hizmetler sektörüne ilişkin bilinçlendirmek üzere hazırladığı bilgi notunda dahi, veri güvenliği standartlarının müzakere konusu olmayacağı ve AB hukukunun korunacağı açıkca ifade edilmişti[37].

AB'nin Transatlantik ilişkilerde, veri güvenliğine dair korumacı yaklaşımı ise temel bir sebebe dayanıyor. ABD Ulusal Güvenlik Ajansı (NSA)'nın, PRISM adlı sistem aracılığıyla Google, Facebook ve Outlook gibi internet devlerinde depolanan kişisel verileri kullanabildiğini öne süren gizli belgelerin uluslararası basına sızması, ABD ve AB arasındaki siyasi ve ticari ilişkileri de doğrudan etkiledi. Hatırlanacağı üzere PRISM programına ilişkin gizli bilgilerin sızdırılması, uluslararası kamuoyunda büyük yankı bulmuştu. PRISM programına ilişkin spekülasyonlara, Almanya Başbakanı Angela Merkel'in telefonunun NSA tarafından dinlendiği yönündeki sızıntılar da eklenince, ABD-AB arası kişisel veri akışı konusu, AB'nin resmi gündemine taşınmıştı. Hatta, ABD ile AB arasındaki etkin, hızlı ve güvenli veri akışını düzenleyen anlaşmanın askıya alınması bile gündeme gelmişti. Öte yandan ABD yönetimi de PRISM programına ve üst düzey AB yetkililerinin verilerinin sızdırılmasına ilişkin iddiaları yalanlamadı. Bu durum, veri güvenliğinde kapsamlı ve temel hak ve özgürlüklere dayalı, bireyin korunmasını ön planda tutan yaklaşımı benimseyen AB kurumları ve başta Almanya olmak üzere AB ülkeleri tarafından büyük eleştiriye ve güvensizliğe sebep oldu. Dolayısıyla bu güvensizlik atmosferinde, AB'nin konuya ilişkin temel

yaklaşımına göre, herhangi bir kişisel verinin AB'den ABD'ye ulaştırılabilmesi için, ABD'nin AB mevzuatına ve standartlara uyum sağlaması gerekiyor. Başta Yeşiller Grubu ve Sosyalist ve Demokratlar İttifakı olmak üzere AP de süreci yakından takip ediyor ve ABD'nin hukuk dışı gözetlemelerini eleştirilerinin merkezine koyuyor. AP Medeni Haklar Komitesi (LIBE) ise AB vatandaşlarının kişisel verileri garanti altına alınmadığı takdirde, TTYO'ya destek vermeyecekleri yönünde bir görüş benimsiyor[38].

Diğer bir yaklaşıma göre, AB'nin kişisel verilerin korunmasına ilişkin hukuki düzenlemelerde aşırı korumacı bir tutum benimsemesinin sakıncalı boyutları bulunuyor. ABD merkezli *Skyhigh Network* adlı danışmanlık şirketinin gerçekleştirdiği bir çalışmaya göre, tasarı halindeki AB tüzüğünün kabul edilmesi durumunda, dünya çapında sadece 11 ülke AB ile veri transferi yapabilecek. AB standartlarıyla uyumlu olduğu öne sürülen bu 11 ülke ise şunlar: Andora, Arjantin, Kanada, Faroe Adaları, Guernsey, Man Adası, İsrail, Jersey, Yeni Zelanda, İsviçre ve Uruguay[39].

PRISM Sızıntıları

2013 yılında İngiliz the Guardian gazetesi tarafından, ABD Ulusal Güvenlik Teşkilatı'nın (NSA) 10 milyonlarca kişinin kişisel verilerini topladığı yönündeki gizli belgelerin kamuoyu ile paylaşılması, uluslararası gündemi her yönüyle etkiledi. The Guardian gazetesi, kısa bir süre sonra, sızıntıların kaynağının Edward Snowden isimli, CIA'da sözleşmeli sistem analistliği yapan, Booz Allen Hamilton personeli olduğunu açıkladı. Snowden'ın sızdırdığı gizli sunum dosyalarında en öne çıkan konu ise NSA'nın yürüttüğü PRISM Programı oldu.

PRISM Programı; Gmail, Facebook, Outlook, Yahoo gibi ABD merkezli internet hizmet sağlayıcılarının kullanıcılılarına ilişkin verilere, NSA tarafından ulaşılabilmesini sağlayan bir sistem. Başka bir değişle, PRISM programı, ABD Hükümetinin internet üzerinden ABD vatandaşı olmayan kişilerin kişisel verilerine ulaşabilmesini sağlıyor. PRISM Programı'nın ABD'deki hukuki dayanağını, Yurtdışı İstihbarat Gözetimi Kanunu'nun 702'nci bölümü oluşturuyor. Snowden'ın sızdırdığı dokümanlarda öne çıkan diğer bir konu ise ABD'nin, AB'nin Washington'daki daimi temsilciliklerini ve BM binasındaki ofislerini de gözetlemesi oldu. Öte yandan Almanya Başbakanı Angela Merkel'in de aralarına dahil olduğu 35 dünya liderinin ABD tarafından dinlendiği yönündeki iddialarla da birlikte, Almanya Hükümeti, ABD Büyükelçisini geri çağırmıştı.

İkinci olarak ise, halihazırda küresel sistemde bulut bilişim firmalarının önemli bir bölümüne ev sahipliği yapan ABD'nin AB ile karşılıklı veri akışı tesis edememesi durumu, bilişim alanındaki küresel gelişimi olumsuz etkileyecek ve kişilerin bilgi edinme hakkı dahil çeşitli hak ve özgürlükleri zedeleyecek. Dolayısıyla, bu alanda gerçekleştirilecek hukuki düzenlemelerin çok yönlü ele alınması ve geçerli konjonktürden daha olumsuz bir duruma sebep olmaması gerekiyor.

5.4.Konunun Temel Hukuki Dayanağı

Konuya ilişkin iki tarafı da bağlayıcı nitelikteki en temel uluslararası düzenleme olarak ise, BM Sivil ve Medeni Haklar Sözleşmesi'nin 17'nci maddesi ön plana çıkıyor. Fakat daha detaylı düzenlemeler dikkate alındığında 95/46/EC sayılı AB Yönergesi büyük önem taşıyor. Çünkü ilgili Yönergenin 25'inci ve 26'ncı maddeleri, AB merkezli olmayan veri işleme firmalarının AB'de iş yapabilmeleri için gerekli kriterleri ortaya koyuyor.

AB ülkelerinde iş yapmak isteyen ABD firmaları, kişisel verilerin korunmasına ilişkin AB düzenlemelerini dikkate almak, bu kriterlere uyum sağlamak zorunda. Fakat AB ile ABD arasında kişisel verilerin paylaşımı alandaki etkileşimin artırılması ve kolaylaştırılmasına yönelik olarak taraflar, uzun bir süredir Yönerge ile uyumlu çeşitli ikili anlaşmalara imza atma yoluna gidiyor. Özellikle ABD şirketleri ile AB ülkeleri arasındaki sınır ötesi veri akışını kolaylaştırmaya yönelik üç mekanizmadan bahsetmek mümkün;

- Güvenli Liman (*Safe Harbour)* Anlaşması;
- Standart Sözleşme Maddeleri (*the Standard Contractual Clauses*);
- Bağlayıcı Şirket Yasaları (*Binding Corporate Rules*)[40].

Bununla birlikte, taraflar arasında kabul edilen bir dizi ikili anlaşma ile birlikte, özellikle adli kovuşturma ve suçla mücadele alanlarında da tarafların yetkili birimleri arasında karşılıklı veri paylaşımı sağlanıyor.

TTYO müzakereleri ile birlikte, yukarıda bahsi geçen bütün bu sınır ötesi veri paylaşımı anlaşmalarının kapsamı, gerekliliği ve önemi tekrardan tartışmaya

açıldı. Özellikle ABD istihbarat birimi NSA ve PRISM Programına ilişkin sızıntılar, Güvenli Liman (*Safe Harbour*) Anlaşmasının durdurulması veya güncellenmesi meselesini AB'nin ana gündemine taşıdı[41].

5.5.Güvenli Liman ve Şemsiye Anlaşma Çerçevesinde İşbirliğinin Tesisi

AB'den ABD'ye kişisel verileri akışının önünü açan Güvenli Liman (*Safe Harbour*) Anlaşması, taraflar arasında 2000 yılında imzalandı. O tarihten itibaren 4.000'e yakın ABD şirketi, Güvenli Liman mekanizmasının parçası oldu. Mekanizma kapsamında AB ile veri transferi gerçekleştirmek isteyen ABD şirketlerinin, AB'de geçerli veri güvenliği hukukuna yeterli ölçüde uyum sağlaması gerekiyordu. ABD şirketlerinin Güvenli Liman mekanizmasına uyumunu ve ihlallerini, ABD'de Federal Ticaret Komisyonu inceliyordu. Öte yandan AB ülkelerindeki ulusal veri koruma kurumları da prosedürü yakından takip ederken bu alanda çok sayıda ihlalin gerçekleşmekte olduğuna işaret ediyordu. AP ise uzun süredir Güvenli Liman'a yönelik temkinli bir tutum sergiliyor. PRISM skandalının ardından AP, Avrupa Komisyonu'nu Güvenli Liman Anlaşması'nı gözden geçirmeye çağırmıştı. AP temsilcileri, ABD şirketlerinin kişisel verilerin korunmasına ilişkin standartları ihlal ettiğini ve AB vatandaşlarının kişisel verilerinin ABD istihbarat birimlerine servis edildiğini öne sürdü.

2015 yılına gelindiğinde ise, TTYO müzakerelerinin hız kazandığı bu dönemde, eş zamanlı olarak Güvenli Liman mekanizmasına ilişkin de büyük kırılmalar yaşanıyor. Özellikle 23 Eylül 2015 tarihinde ABAD Başsavcısı Yves Bot, *Maximilian Schrems v Data Protection Commissioner* C-362/14 başlıklı davaya ilişkin sunduğu istişari mütalaada, bu haliyle Güvenli Liman Anlaşması'nın AB hukukuna uygun olmadığını ve ABD'de geçerli kişisel verilerin korunması düzenlemelerinin AB standartlarının altında olduğunu ifade etti. Bağlayıcı olmamasına rağmen bu görüş, AB ve ABD kamuoylarında çok büyük yankı buldu[42]. Bilindiği üzere Edward Snowden'ın PRISM programını ifşasının ardından, *Maximilian Schrems v Data Protection Commissioner C-362/14* başlıklı davanın tarafı Max Schrems, Facebook'un AB merkezi olan Facebook İrlanda'nın, vatandaşların kişisel verilerini, hukuk dışı şekilde ABD'ye aktardığı iddiasıyla, ilgili İrlanda mahkemesine dava açmıştı. İrlanda Mahkemesinin, Facebook'un veri aktarımının Güvenli Liman'a dayandığına hükmetmesinin ardından Schrems,

davasını ABAD'a taşımıştı[43]. Başladığı tarihten bu yana dava, Güvenli Liman mekanizmasının geleceği açısından büyük önem taşıyor. Dolayısıyla, ABAD Başsavcısının bağlayıcı olmayan ve Güvenli Liman mekanizmasını eleştiren istişari mütalaası, ABAD'dan nasıl bir karar çıkabileceğinin de ipucu niteliğindeydi.

Sürecin devamında ABAD, 6 Ekim 2015 tarihinde Schrems Davasına ilişkin verdiği kararında, ABD merkezli özel şirketler ile AB arasında karşılıklı veri akışının önünü açan Güvenli Liman Anlaşması'nı geçersiz kıldı. ABAD'ın kararına göre, üçüncü ülkelerin AB ile karşılıklı veri akışı sağlayabilmesi için, AB Temel Haklar Şartına ve ilgili AB Yönergesi'ne uyumlu kişisel verilerin korunması mevzuatına sahip olması gerekiyor. Öte yandan ABAD, kişisel verilerin korunması gibi temel haklara ve gizliliğe ilişkin bir konuda, Güvenli Liman gibi ikili anlaşmaların, AB üye ülke yetkili makamlarını veri güvenliği ihlallerini soruşturmaktan alıkoyamayacağını öne sürdü. ABAD'ın bu kararının, transatlantik ticaret ilişkilerinde bir takım belirsizliklere sebep olacağını söylemek şimdiden mümkün.

Öte yandan, AB ve ABD arasında veri aktarımı alanındaki işbirliğinin geleceğine olumlu bulanlar da var. Özellikle tarafların kolluk kuvvetleri arasında işbirliğinin güçlendirilmesi amacıyla yüksek seviye veri güvenliği standartlarının oluşturulması için bir süredir devam eden müzakereler, 8 Eylül 2015 tarihinde sonuçlandı. ABD-AB Veri Güvenliği Şemsiye Anlaşması'nın (*USA-EU Data Protection Umbrella Agreement*) imzalanmasıyla, suç fiilinin önlenmesi, tespiti, kovuşturması ve cezalandırılmasına yönelik her türlü karşılıklı kişisel veri paylaşımının önü açıldı.

Anlaşma kapsamında veri paylaşımı sadece yukarıda belirtilen amaçlar doğrultusunda gerçekleşebilecek. Bu çerçevede, ticari sebeplerle veri paylaşımı kapsama dışında kalıyor. Anlaşmanın imzalanması ile birlikte ortaya çıkan en önemli gelişme, gizlilik ilkesinin ihlali halinde, AB vatandaşları da ABD vatandaşları ile eşit şartlara sahip olarak ABD mahkemelerine başvuruda bulunabilecek. Bu hallerde, AB vatandaşlarının ABD'de ikamet etmesi gerekmeyecek. PRISM skandalı ve gizlilik ihlallerinin gün yüzüne çıktığı dönemin ardından imzalanan Şemsiye Anlaşma, TTYO müzakereleri kapsamında veri güvenliğinin müzakere edilmesi ve AB kamuoyunun ve karar vericilerin güveninin kazanılması yönünde atılan en önemli adım kabul ediliyor.

Sürecin devamında, tarafların, TTYO müzakerelerinde kişisel verilerin korunması tartışmalarına ilişkin daha şeffaf olmaları bekleniyor. Tartışmalardan en çok etkilenen, Facebook, Google ve Microsoft gibi bilişim devleri; kişisel verileri tartışmaların merkezinde olan vatandaşlar ve süreci büyük bir tedirginlik ve tedbirle takip eden uluslararası sivil toplum ancak yeterli seviyede şeffaflık ve açıklık sağlanabilirse sürece dahil olabilir. Nihayetinde veri güvenliği meselesinin müzakerelerin önemli bir parçası olmadığı yönünde gösterilen tavrın gerçeği yansıtmadığı ortada. Veri devrimi olarak addedilebilecek bu dönemde, bütün paydaşların süreçten kazanımlarının garanti altına alınması gerekiyor. Müzakerelere ilişkin verilerin açık ve ulaşılır olması, Avrupa Komisyonu'nun benimsediği ve önem verdiği "açık veri" (*open data*) politikası ve vatandaşların karar alma süreçlerine katılımı açısından da büyük önem taşıyor. Bilindiği üzere bu konuda AB Ombudsmanlık Makamı, TTYO müzakerelerindeki şeffaflık sorununa ilişkin bir soruşturma başlatmış ve Komisyon'a, müzakerelerde şeffaflığın artırılmasına yönelik tavsiyelerini sunmuştu[44].

6. TTYO MÜZAKERELERİYLE AB'DE ALEVLENEN TARTIŞMA: AÇIK VERİLER

Avrupa Komisyonu yetkililerinin, TTYO müzakerelerine kişisel verilerin korunması konusunun dahil edilmeyeceği yönünde demeçleri AB kamuoyunu yeterince tatmin etmemiş olacak ki, mesele, daha geniş çaplı bir tartışmanın parçası haline geldi. AP temsilcilerinin ve AB sivil toplumunun bu konudaki şeffaflık ve müzakere belgelerine erişim çağrıları, AB Ombudsmanlık Makamı'nda yankı buldu. AB Ombudsmanlık Makamı, Temmuz 2014 tarihinde, TTYO müzakerelerinde şeffaflığa ilişkin kamuya açık bir soruşturma başlatarak Ocak 2015'te Avrupa Komisyonu ile daha şeffaf müzakerelere yönelik tavsiyelerini paylaştı[45].

Ombudsmanlık Makamı'nın, Avrupa Komisyonu'na yönelik tavsiyeleri; kamuoyuna açık ve kapalı bütün TTYO belgelerinin listesinin kamuoyu ile paylaşılmasını, müzakereleri yürüten yetkililere ilişkin bilgilerin paylaşılmasını ve müzakere belgelerinin kamuoyuna açılmasını içeriyor. İlgili açıklamada, Avrupa Ombudsmanı Emily O'Reilly, Avrupa Komisyonu'nun, AB vatandaşlarının bilgiye

erişim hakkını garanti altına almakla yükümlü olduğunu ifade etti. Öte yandan Avrupa Komisyonu, konuya ilişkin değerlendirmelerinde, bir takım bilgilerin paylaşımının ve kamuya açıklanmasının, kişisel verilerin korunması bakımından ihlal oluşturabileceğini öne sürdü[46]. Dolayısıyla kişisel verilerin korunmasına ilişkin bir müzakerede alevlenen bu tartışmalar, bilgi çağının en önemli fenomenini oluşturan "verilerin" bir diğer önemli boyutu gündeme getirdi: açık veriler.

Günümüz uluslararası sisteminde, kişisel verilerin korunması kadar, kamu verilerine ulaşım hakkı da gelişen teknoloji ile birlikte vazgeçilmez bir temel hak haline geliyor. Pek çok gelişmiş ve gelişmekte olan ülke gibi, AB projesi de kişisel verilerin korunması ve verilerin kamuoyuna açılması arasındaki ince çizgiyi, temel hak ve özgürlüklere ve iyi yönetişime ilişkin önemli bir tartışma konusu kabul ediyor. Günümüzde kamu kurumlarına ilişkin çok çeşitli verilere sivil toplumun ve bireylerin ulaşım; karar alma süreçlerinde katılımcılığın artırılması, daha yenilikçi ve kapsamlı çıktılara etkin şekilde ulaşılması ve yolsuzlukla etkin mücadele gibi bir takım olumlu gelişmelerin önünü açıyor.

6.1.Uluslararası Sistemin Popüler Fenomeni Açık Veriler Nedir?

Artan bir hızla gelişen teknolojilerle birlikte eş zamanlı olarak hem devletlerin, şirketlerin, sivil toplum örgütlerinin ve bireylerin topladığı/paylaştığı verilerin sayısında büyük bir artış yaşanıyor hem de bu verileri analiz edebilecek ve değerlendirebilecek yöntemler çeşitlilik kazanıyor. Bu verilerin açık veri formatında kamuoyu ile paylaşımı, devletlerin kritik alanlarda gösterdikleri ilerlemenin takibi, insan kaynağı ve hizmetlerin en etkin şekilde aktarılacağı alanların belirlenmesi ve süreçlerin şeffaf, hesap verilebilir gerçekleşmesi için büyük önem taşıyor.

Devletlerin bulundurduğu verilerin açık veri kabul edilebilmesi için verilerin, bütün paydaşlar tarafından bilgisayarda okunabilir formatta kullanıma, yeniden kullanıma ve dağıtıma açık olması gerekiyor[47]. Devlet verilerinin açık formatta paylaşımının temelde üç alanda kamu hizmetlerinde etkinliği artırabileceğini söylemek mümkün. Bu alanlar:

Tablo 5: *Open Data Barometer* Sıralamasında İlk 10 Ülke[50]	
Ülke	**Barometre Sıralaması**
Birleşik Krallık	1
ABD	2
İsveç	3
Fransa	4
Yeni Zelanda	4
Hollanda	6
Norveç	7
Kanada	7
Danimarka	9
Almanya	10

- Bilginin daha hızlı yayılmasının sağlanması ve bireylerin bilgiye erişim hakkının tesisi;
- Politika üreticilere daha etkin üretim alanı sağlanması;
- Doğru kaynaklara doğru mekanizmalar üzerinden ulaşımın mümkün olması.

Böylelikle açık veriler, bürokratik yüklerden ve şeffaflıktan uzak devlet-birey etkileşiminden kurtulmaya yönelik önemli bir araç olarak karşımıza çıkıyor[48]. ABD merkezli danışmanlık şirketi *McKinsey* tarafından 2013 yılında gerçekleştirilen bir araştırmaya göre, eğitimden sağlığa uzanan 7 ana sektörde kamu kurum ve kuruluşlarına ait verilerin, açık veri formatında yayınlanması, küresel ekonomiye yıllık 3 trilyon dolar değerinde katkı sağlayabilir[49]. Öte yandan *Omidyar Network* tarafından 2014 yılında gerçekleştirilen bir diğer araştırma ise açık verilerin G20 ülkelerinin tamamı için toplam değerinin 2,6 trilyon dolara ulaştığını ortaya koyuyor. Yapılan araştırmalar, açık verilerin halihazırda geçerli hizmetlerin maliyetlerinin azalması, yeni iş ve girişimlere fırsat oluşturması, inovasyona ve dijital pazara katkı sağlaması gibi çok çeşitli ekonomik faydalarını gözler önüne seriyor.

Hal böyle olunca, 2009 yılında herhangi bir ülkenin ulusal açık veri politikasından bahsedilmezken, 2014 yılına gelindiğinde 50'den fazla devletin açık veri portalları ve girişimleri yürüttüğü görülüyor. Tabloyu daha net görebilmek için, bu alanda yapılmış en kapsamlı araştırmalardan biri olan, *2013 Open Data Barometer* büyük önem taşıyor. 77 farklı ülkedeki açık veri potansiyelinin değerlendirildiği araştırmada, ülkelerin %55'inden fazlasının açık veri politikaları uyguladığı görülüyor. Öte yandan, 2015 yılında genişletilen ve 86 ayrı ülkenin değerlendirildiği son çalışmada ülkelerin açık veri potansiyelleri değerlendirildiğinde, en etkin açık veri politikalarına sahip ülkelerin sıralamasında ilginç bir sonuç ortaya çıkıyor. Sıralamada ilk 10'da yer alan ülkelerin 6'sının AB üyesi olduğu görülüyor (Birleşik Krallık 1'inci, İsveç 3'üncü, Fransa 4'üncü, Hollanda 6'ncı, Danimarka 9'uncu, Almanya 10'uncu). Dolayısıyla 2015 yılında, Türkiye'nin katılım müzakerelerini sürdürdüğü ve bu kapsamda veri güvenliği mevzuatını uyumlaştırmakla yükümlü olduğu AB'nin, açık verilere ilişkin politikaları da veri güvenliği meselesi gibi gündemine aldığını söylemek mümkün.

AB'de konunun bir yönü, yani veri güvenliği boyutu halihazırda karışık ve yoğun tartışmalara ortam oluştururken, diğer bir yönü olan açık veri meselesinin nasıl ele alındığının incelenmesi, Türkiye'de standartların belirlenmesi ve önümüzdeki dönemde bu alanda temel hak ve özgürlüklerin garanti altına alınabilmesi için de büyük gereklilik taşıyor.

6.2.AB'nin "Büyüme" Merkezli Açık Veri Stratejisi

AB'de, kurumlara ve üye ülkelere ilişkin verilerin kamuoyuna açılması fikri temelde AB'nin 2020 Stratejisinin önemli bir parçasını oluşturuyor. Bu kapsamda AB'nin dijital gündemi; akıllı, sürdürülebilir ve kapsayıcı bir ekonomi modeli çerçevesinde açık verileri ve e-devlet fikrini ön plana çıkarıyor. Başka bir deyişle, AB'nin açık verilere verdiği önemin temelinde potansiyel ekonomik kazanımlar yatıyor. AB'nin 2011 yılında yayımlanan Açık Veri Stratejisi'nde belirtildiği üzere, AB'de kamu kurumlarına ilişkin verilerin kullanıma, yeniden kullanıma ve dağıtıma açılmasıyla birlikte toplamda yıllık 40 milyar avroluk bir kazanım elde edilmesi mümkün[51].

Sadece verilerin paylaşılmasının da ötesinde, vatandaşların çevrimiçi yollarla karar alma süreçlerine katılımıyla, büyük ekonomik kazanımlar söz konusu olabilecek. Örneğin Avrupa Komisyonu'nun verileri, AB çapında bütün kamu ihalelerinin çevrimiçi yollarla, elektronik ihale yöntemiyle gerçekleşmesinin, AB için yıllık 100 milyar avro civarında tasarruf sağlayabileceğini gösteriyor. AB çapındaki bu kazanımın yanı sıra ülkeler bazında bir inceleme yapıldığında da benzer bir tablo ortaya çıkıyor. Örneğin, Portekiz'de kurulan e-devlet sisteminin vatandaşlara ve işletmelere sağladığı tasarrufun toplamda 56,1 milyar avroya ulaştığı belirtiliyor[52].

AB hukuku kapsamında bu alandaki ilk düzenleme, 31 Aralık 2003 tarihinde 2003/98/EC sayılı AB Yönergesi'nin (*PSI Directive*) yürürlüğe girmesiyle gerçekleşti. Yönerge, AB üye ülkelerde ulusal, bölgesel, yerel seviyelerde idarelerle birlikte bakanlıklar, belediyeler ve diğer kamu kurumları tarafından muhafaza edilen verilerin yeniden kullanıma açılmasını öne sürüyor. Devam eden süreçte, AB'nin dijital gündeminin önem kazanması, bilgi teknolojilerindeki ve kamu yönetimi stratejilerindeki gelişmelerle birlikte 2011 yılına gelindiğinde Avrupa Komisyonu, yeni Açık Veri Stratejisi'ni kamuoyu ile paylaştı. AB'nin Açık Veri Strateji'si üç temele dayanıyor:

- Verilerin yeniden kullanımına yönelik birincil/ikincil hukuk kaynaklarının, politika önlemlerinin ve araçların oluşturulması;
- Bu alandaki ARGE ve altyapı çalışmalarını destekleyen mali araçların tesisi;
- AB çapında iyi örneklerin paylaşımının sağlanması.

2013 yılında ise ilgili AB Yönergesi'nin kapsamı genişletildi ve AB ülkelerindeki müze, kütüphane ve arşivlerin de Yönerge'nin kapsamı içerisinde ele alınmasına başlandı. Gelinen noktada, AB çapında kamu sektörüne ilişkin verilerin paylaşımının ve yeniden kullanımının önündeki engelleri aşmaya yönelik en önemli reform hamlesi, AB Açık Veri Portalı'nın (*EU Open Data Portal*) Aralık 2012 tarihinde açılması ile geldi. AB Açık Veri Portalı aracılığıyla, Avrupa Komisyonu ve diğer AB kurum/kuruluşları tarafından muhafaza edilen 7.800'den fazla veri seti erişime açıldı. AB Açık Veri Portalı üzerinden, AB resmi istatistik kurumu Eurostat'tan, Avrupa Havacılık Güvenliği Ajansı'na veya Avrupa Yatırım Bankası'na kadar çok çeşitli kurumların verilerine ulaşılabiliyor. AB vatandaşları

tarafından en fazla sayıda görüntülenen ilk üç veri seti ise; AB müktesebatının üye ülkelerin resmi dillerinde gerçekleşen çevirileri, Avrupa'nın yükselti haritası ve Horizon 2020 projesi kapsamında mali destek kazanan projelerin listesi. Aralık 2012'den bu yana AB kurumlarına ilişkin çok sayıda açık veriye Açık Veri Portalı üzerinden ulaşmak mümkün olsa da AB'nin bu alandaki stratejisinin merkezinde, AB ülkelerinin ulusal ve yerel kamu kurumlarına ilişkin verilerin de bütün AB vatandaşlarının kullanımına ve yeniden kullanımına açılacağı bir açık veri portalının altyapısını oluşturmak (*Pan European Data Portal*) yatıyor. Çalışmaları devam eden bu proje tamamlandığında, bir AB vatandaşı, ortak bir açık veri portalı aracılığıyla herhangi bir AB ülkesinin kamu kurumları tarafından paylaşılan açık verilere ve AB kurumlarının yayımladığı verilere, tek bir portal üzerinden farklı dillerde ulaşma fırsatı bulabilecek[53].

AB, açık veri projesine ekonomik kazanım odaklı yaklaşıyor olsa da, AB Açık Veri Portalı'nın ve AB'nin açık veri politikalarının iyi yönetişim, şeffaflık ve katılımcılığı büyük ölçüde ön plana çıkaran, diğer ulusal, bölgesel ve uluslararası yapılara örnek oluşturabilecek bir takım uygulamalarından da bahsetmek gerekiyor. Bilindiği üzere, güncel konjönktürde kapsayıcı ve sürdürülebilir kalkınma ve büyümenin önemli bir boyutunu, kriz bölgelerine yapılan insani yardımların yönetimi ve etkinliği oluşturuyor. Toplam miktara bakıldığında, AB ülkeleri ve kurumları, dünyanın en büyük bağışçısı konumunda. Dolayısıyla, AB'nin hem bu mali yardımları etkin şekilde gerçekleştirebilmesi hem de vatandaşlarına hesap verilebilirliğin sağlanabilmesi için AB Yardım Gezgini (*EU Aid Explorer*) adı altında bir tek durak mekanizması oluşturuldu. Bu araç sayesinde, AB'nin 60'tan fazla ülkede gerçekleştirdiği kalkınma yardımlarına ve insani yardımlara ilişkin tam ve net bilgilere ulaşmak mümkün hale geldi. Böylelikle AB vatandaşları, vergileri ile gerçekleştirilen küresel çaptaki insani yardımların hangi kaynak aracılığıyla, hangi proje dahilinde, hangi araçlarla ve hangi tarih aralığında olduğu gibi çeşitli soruların yanıtlarına ulaşabilme ve süreçlerin gözetimini sağlayabilme fırsatı buldu. AB Yardım Gezgini'nde muhafaza edilen açık veriler, OECD, EDRIS, IATI gibi çok sayıda uluslararası kaynaktan elde ediliyor[54].

İkinci olarak, AB karar alma süreçlerinin milyonlarca insanın hayatını doğrudan etkilediği gerçeğinden yola çıkarak, açık veriler, bu karar alma süreçlerine katılım

ve gözetime yönelik önemli bir rol oynuyor. AB Şeffaflık Portalı (*Transparency Portal*) ve Şeffaflık Sicil'i (*Transparency Register*), açık verilerin, şeffaflığın ve iyi yönetişimin tesisindeki önemini ortaya koyan uluslararası örnekler olarak ön plana çıkıyor. Şeffaflık Portalı, AB'nin karar alma süreçlerinin takibi ve sivil toplumun katılımı için gerekli bilgilere doğrudan ulaşımı sağlayan bir portal niteliği taşıyor. Şeffaflık Portalı üzerinden, AB kurumları tarafından oluşturulan ve oluşturulmakta olan AB mevzuatına, bu süreçteki kamuoyu görüşlerine, AB bütçesinden alınan pay ve bu payı kimlerin aldığına ulaşım fırsatı sunuluyor. Şeffaflık Sicili ise, Avrupa Komisyonu ve AP'de seslerini duyurmakta olan ve AB karar alma süreçlerini etkilemeyi amaçlayan danışmanlık/hukuk firmalarının, lobi firmalarının, sivil toplum örgütlerinin, düşünce kuruluşlarının, dini örgütlerin ve yerel yönetim unsurlarının gönüllülük esasıyla kayıtlı oldukları bir yapı. Bu internet sitesi aracılığıyla 8.559 farklı kuruma ilişkin açık verilere ve AB kurumlarında hangi alanlarda savunuculuk faaliyetlerini sürdürdüklerine, amaçlarına ilişkin bilgilere ulaşmak mümkün. Şeffaflık siciline kayıt, gönüllülük esasına dayansa da; kayıtlı organizasyonlarla Komisyon üyelerinin bir araya gelebileceği etkinlikler düzenlenmesi, kayıtlı organizasyonlara otomatik görüş talebi gönderimi, kayıtlı örgütlere AP'ye özel erişim sağlanması gibi bir takım avantajlar sunuluyor[55].

Öte yandan şeffaflık ve yönetişim üzerine çalışan AB merkezli sivil toplumun, AB kurumlarında açıklık katılımcılığa ilişkin çekinceleri sürüyor. Özellikle karar alma süreçlerinde süren müzakerelerin kapalılığı ve süreçlerin karmaşıklığı ile Şeffaflık Sicili'ne kaydın zorunlu tutulmaması; başlıca eleştirileri oluşturuyor[56]. Bu çalışma kapsamında bahsi geçen TTYO müzakereleri örneği de, bu görüşü destekler nitelikte. Sadece ilgili mevzuatın değil, politika üretme süreçlerindeki bütün toplantı tutanaklarının ve müzakerelerin de kamuoyu ile paylaşımı talep ediliyor. Öte yandan AB karar alma süreçlerine ilişkin önemli miktarlarda açık veri paylaşılmakta olsa da esasında bu verilerin sunumunun daha anlaşılır, daha ulaşılır ve sistematik olması büyük önem taşıyor.

Politika üretme süreçlerinde her türlü verinin kamuoyu ile paylaşılamamasının temel sebeplerinden biri olarak, kişisel verilerin korunması, gizlilik ve kamu güvenliği gösteriliyor. Bu çekinceler bir noktaya kadar doğruluk payı taşıyor.

Çalışma boyunca pek çok kere vurgulandığı üzere, güvenlik ile özgürlükler arasındaki dengenin kurulması, günümüz uluslararası sisteminin ve toplumsal yapıların karşı karşıya kaldığı zorluklardan birini oluşturuyor. Eş zamanlı olarak bilgiye ulaşımın ve bilgiyi paylaşımın hızlandığı; her geçen gün daha fazla verinin dijital ortamda dolaşıma girdiği günümüzde, veri güvenliği ihlallerinin önüne geçilmesi de öncelikli olarak üzerinde durulması gereken bir konu haline geliyor. Bir yandan bilgiye ulaşım hakkının agresif savunuculuğunu yaparken, kişisel verilerin korunmasının önemini göz ardı etmemek gerekiyor.

6.3.Temel Haklar Körfezi'nin İki Yakası: Kişisel Veriler – Açık Veriler

Dünyanın neresinde olursa olsun bireylerin, kamu kurumlarıyla girdikleri etkileşimde, daha önce ibraz ettikleri belgeleri, başka bir kamu kurumu için yeniden düzenlemeleri ve sunmaları gerekebiliyor. Örneğin, bir Türk vatandaşının ehliyet başvurusu için ikametgâh belgesi sunduktan sonra, yakın dönemde başka bir kamu kurumuna gerçekleştireceği başka bir başvuruda yeni bir ikametgah belgesi çıkartması ve bu belgeyi yeniden sunması gerekebiliyor. Bu durum hem bireylerin hem de kamu kurumlarının vakit ve verimlilik kaybına sebep olurken aslında tahmin edilenden çok daha büyük bir soruna işaret ediyor.

Avrupa Komisyonu'nun değerlendirmelerine göre, vatandaşların ve şirketlerin kamu kurumlarına başvurularının yarısından azında, daha önce başka bir kamu kurumuna sunulan verilerin yeniden kullanımı söz konusu. Yeniden kullanım yaklaşımının AB çapında benimsenmesi durumunda, 2017 yılına kadar, yıllık 5 milyar avro tasarruf sağlanması öngörülüyor. Dolayısıyla kamu kurumlarına sunulan kişisel verilerin yeniden kullanımı, etkin bir kişisel verilerin korunması mevzuatına dayandığı takdirde, önemli kazanımlar sağlayabilir. Bu noktada kritik olan durum, kişisel verilerin kamu kurumları tarafından yeniden kullanımının kesinlikle temel hak ve özgürlükleri ihlal etmemesi gerektiğidir. Öte yandan kişisel verilerin şirketler veya diğer bireyler tarafından yeniden kullanımı ise "açık veri" politikalarının kapsamına girmiyor. Dolayısıyla bir kamu kurumu tarafından tutulan kişisel verilerin, başka bir birey tarafından rızasız kullanımı, AB'de geçerli mevcut veri güvenliği düzenlemelerine aykırıdır. Aynı şekilde yeniden kullanımların, fikri mülkiyet hukukuna da uygun olması gerekiyor.

AB hukukunda konuya ilişkin düzenlemelere bakıldığında, kişisel verilerin yeniden kullanımı söz konusu olduğunda hem ilgili açık veri yönergesinin hem de AB Veri Güvenliği Yönergesi'nin dikkate alınması gerekiyor. Kamu kurumları tarafından tutulan ve yeniden kullanımının tartışmalı olduğu bir takım verilerin kişisel bilgiler içerdiğini söylemek mümkün, örneğin: tapular, şirket yönetim kurul üyelerine ilişkin bilgiler, ticari siciller. Bu hallerde, vatandaşların kişisel bilgilerini içeren verilerin açık veri formatında yayınlanıp yayınlanamayacağı, AB ülkelerinin ulusal mevzuatına bırakılıyor[58]. Uzun vadede, geniş kapsamlı açık veri girişimleri yürütmeyi hedefleyen AB'nin bu alanda daha belirgin standartlar ortaya koyması ve belirsizlikleri ortadan kaldırması, Türkiye gibi AB mevzuatını yüklenmekle yükümlü ülkeleri de büyük ölçüde etkileyecek.

AB'nin 2013 yılında, G8 Açık Veri Şartı'nı (*G8 Open Data Charter*) onaylaması ve ileri uyum için eylem planı oluşturması bu açıdan olumlu bir gelişme olarak kabul ediliyor. G8 Açık Veri Şartı dahilinde düzenlenen 8'inci taahhüt, AB üye ülkelerinin açık veri mevzuatını ve politikalarını, 2013 yılında ortaya koyulan G8 prensipleri ile uyumlu hale getirmeyi öngörüyoruz. Dolayısıyla AB'nin bu taahhüdü yerine getirebilmesi için, AB ülkelerinin ilgili AB yönergesine uygun düzenlemeler gerçekleştirmesi; AB kurumlarının ise standartları ileri aşamaya taşıyacak genel prensipleri oluşturması gerekiyor. Burada dikkat çeken ise, G8 Açık Veri Şartı'na AB'nin uyum durumunu ortaya koyan ilgili belgede de eğer kişisel verilerin açık veri formatında yayımlanması söz konusu olursa, AB'nin ilgili kişisel verilerin korunması yönergesinin dikkate alınacağı ve gerektiğinde, verinin anonim hale getirilmesi gibi önlemlerin alınacağının belirtiliyor olması[59].

AB daha ileri açık veri girişimlerinin hayata geçirilmesine yönelik çeşitli yollarla sivil toplumun da katılımını sağlayacak eylemler ortaya koyuyor. Bu desteğin temelinde ilgili sivil toplum projelerine mali yardım aktarımı, kaynakların açılması ve teknik altyapı oluşturulması, danışma ve deneyim paylaşım toplantıları düzenlenmesi gibi bir takım aktiviteler ön plana çıkıyor[60]. Fakat sivil toplumun bu çerçevede danışma ve tavsiye mecrası olma rolünün ötesinde denetleme, gözetleme ve ortak üretimin parçası olma rolleri de bulunuyor.

91 ülkeden 500'e yakın sivil toplum kuruluşunun temsilcileri, 15-16 Eylül 2015 tarihlerinde son haline getirdikleri C20 Bildirgesi aracılığıyla, G20 yapısı çerçevesinde AB'nin de aralarında bulunduğu G20 üyelerine özellikle açık verilerin iyi yönetişimi, şeffaflığı ve katılımcılığı öne çıkaran yönlerini dikkate alan tavsiyelerde bulundu. G20'nin sivil toplum açılım grubu C20, G20 liderlerine; aralarında devlet bütçeleri, kamu ihaleleri, petrol, doğalgaz, maden vb. çıkarma ödemeleri, inşaat ve altyapı projeleri, düzenleyici etki analizleri ve kişilerin, şirketlerin ve ülkelerin ismen tespit edilmesine de imkân veren tüm mahkeme kararlarının da yer aldığı, kamu kurumları tarafından tutulan ve yolsuzlukla mücadelede önem taşıyan çeşitli veri setlerinin açık veri formatında yayınlanmasını tavsiye etti. Öte yandan C20, ilgili diğer tavsiyeleri aracılığıyla AB ülkelerini, Türkiye'yi ve diğer G20 üyelerini, Gerçek Lehdarlık Sicil Sistemlerinin ve kamu ihalelerinin her aşamasının kamuya açık hale getirilmeye çağırdı[61].

6.4.Türkiye Bütün Bu Tartışmaların Neresinde?

Bütün dünyanın dikkatle takip ettiği TTYO müzakerelerinden en fazla etkilenecek üçüncü ülkelerin başında AB ile 1996 yılından bu yana Gümrük Birliği ilişkisi içerisinde olan Türkiye geliyor. TTYO müzakereleri kadar gündeme yansımamakta olsa dahi, bilgiye erişim hakkı, sivil toplumun katılımı, şeffaflık ve hesap verebilirlik gibi iyi yönetişimin temel unsurları; Türkiye-AB ilişkileri açısından da büyük önem taşıyor. Türkiye-AB Katılım Müzakerelerinin pek çok boyutu, süregelen ikili görüşmeler, toplantılar, müzakere turları, üst düzey diyalog toplantıları, eylem planları ve raporlar üzerinden devam ediyor. Bu süreçlere sivil toplumun ve kamuoyunun erişebilirliği ise önemli bir soru işareti. Türkiye-AB ilişkilerinin daha ileri aşamaya taşınabilmesi için ilgili belgelere, kamuoyunun tam, zamanında ve kolay ulaşımı sağlanmalıdır. Özellikle önümüzdeki dönemde Gümrük Birliği'nin güncellenmesi ve vize serbestliği diyaloğuna ilişkin verilerin daha şeffaf şekilde ve zamanında paylaşımı, şüphesiz ki bu alanlarda bütün paydaşlar tarafından üretimin artmasına ve süreçlere olan güvenin tazelenmesine katkı sağlayacaktır.

Türkiye ile AB arasındaki Gümrük Birliği'nin güncellenmesi tartışmalarının gündemin merkezine oturduğu konjönktürde, Türkiye'nin önümüzdeki dönemde bir takım ileri adımlar atması, çeşitli hukuki düzenlemeler gerçekleştirmesi bekleniyor. TTYO'nun imzalanması halinde, anlaşmanın ortaya koyduğu yüksek hukuki standartlar sebebiyle, Türkiye'nin Gümrük Birliği için gerçekleştireceğinin de ötesinde bir takım adımlar atması zorunlu olabilir. Bilindiği üzere, Gümrük Birliği'nin güncellenmesi tartışmaları kapsamında fikri mülkiyet hukuku standartlarının ve kamu alımlarının da tartışmaya açılması bekleniyor. Bu iki alan, kişisel verilerin korunmasına ilişkin hukuki çerçeveyle doğrudan bağlantılı ve TTYO müzakereleri kapsamında da müzakere edilen konular. Özellikle Türkiye'de elektronik ihale mekanizmalarının kurulmasına ve işleyişine ilişkin çalışmalar kapsamında depolanan kişisel verilerin korunması ve transferi konusu, hem Türkiye-AB katılım müzakereleri, hem Gümrük Birliği'nin güncellenmesi hem de TTYO çerçevesinde gündeme gelebilecek konular arasında.

İkinci olarak, TTYO müzakerelerinde e-ticaret ve bulut bilişim teknolojileri kapsamında kişisel verilerin korunması ve aktarımı konusunun gündeme gelebileceği belirtilmişti. Dolayısıyla Türkiye'nin de müzakerelerin bu boyutunu dikkatle takip etmesi ve mevzuatını bu alanda AB standartlarına şimdiden, TTYO öncesi dönemde yakınlaştırması gerekiyor.

AB ve ABD arasında kişisel verilerin korunması ve paylaşımına ilişkin etkin bir mekanizmanın kurulması, Türkiye ile AB arasında sürmekte olan ve Türk vatandaşlarına yönelik vize uygulamasının kalkmasıyla sonuçlanması öngörülen diyalogla da bağlantılı. ABD gibi Türkiye de halihazırda AB standartlarında kapsayıcı kişisel verilerin korunması düzenlemelerine sahip olmayan ülkeler arasında. Dolayısıyla bu durum, Türkiye ile AB arasındaki veri paylaşımını ve işbirliğini büyük ölçüde sınırlıyor. Fakat Avrupa Komisyonu'nun Türk yetkili makamlara sunduğu Vize Serbestliği Yol Haritası dahilinde Türkiye'nin yerine getirmekle yükümlü olduğu kriterler arasında AB standartlarında, kapsayıcı bir Kişisel Verilerin Korunması Kanunu oluşturması yer alıyor.

7.TÜRK VATANDAŞLARI İÇİN "VİZESİZ AVRUPA" VE KİŞİSEL VERİLER

BM İnsan Hakları Evrensel Beyannamesi'nin 13'üncü maddesi ile de garanti altına alındığı üzere, kişilerin bir devletin toprakları üzerinde dolaşım hakkı, en temel insan hakları arasında yer alıyor. Öte yandan bu serbestlik, AİHS 4 No'lu Protokol kapsamında da ilkesel olarak tanınmış durumda. AB'de halihazırda geçerli hukuk sistemine bakıldığında, Avrupa'nın da bu temel insan hakkına verdiği özel önem dikkat çekiyor. AB değerler sisteminin temel taşını oluşturan AB Temel Haklar Şartı'nın dibaçe bölümünde, malların, hizmetlerin ve sermayenin serbest dolaşımı ile birlikte kişilerin serbest dolaşımının ehemmiyeti vurgulanıyor.

Özellikle küresel sistemin en başarılı entegrasyon ve serbest dolaşım projesi olan; AB içerisinde sınırların kaldırılmasına dayalı Schengen Sistemi, AB üye ülke vatandaşlarının diğer AB ülkelerine usulüne uygun olduğu sürece, kısa süreli seyahatlerine serbestçe giriş yapabilmelerini ve seyahat edebilmelerini mümkün kılıyor. Schengen Sistemi aracılığıyla AB üye ülke vatandaşlarına sağlanan diğer AB ülkelerine vizesiz seyahat özgürlüğü, Norveç, İzlanda, İsviçre gibi bir takım AB üyesi olmayan ülkelere de sağlanırken, AİHS 4 No'lu Protokol ve Schengen Düzenlemeleri uyarınca ve AB hukuku tarafından benimsendiği üzere; bu haklar sadece ulusal güvenlik, kamu emniyeti, kamu düzeninin korunması, suçun önlenmesi ve başkalarının hak ve özgürlüklerin korunması için demokratik bir toplumda zorunlu hallerde sınırlandırılabiliyor. Bununla birlikte; Romanya, Bulgaristan ve Hırvatistan gibi bir takım üye ülkelerde yeterli ölçüde sınır güvenliği, işbirliği ve kolluk kapasitesi bulunmamasından dolayı bu ülkeler halen daha Schengen Sistemi'nin bir parçası değil. Başka bir deyişle, kişilerin AB'ye vizesiz seyahat ve AB'de serbest dolaşım hakkı, kaynak ülkelerdeki güvenlik ve işbirliği altyapısının yeterliliğine dayanıyor.

Temel bir hak olan kişilerin serbest dolaşımı, Türkiye-AB Katılım Müzakereleri'nin de kilit bir alanını oluşturuyor. 1963 yılında taraflar arasında Ankara Anlaşması'nın imzalanmasıyla malların karşılıklı serbest dolaşımı yolunda önemli adımlar atılırken kişilerin serbest dolaşımı da bu kapsamda tartışmaya açılmış ve belli bir süre sonrasında kişilerin de AB'ye serbest dolaşımının

sağlanması öngörülmüşt. Güncel konjönktürde ise hizmetlerin serbest dolaşımı, Gümrük Birliği'nin güncellenmesi, AB'nin karşı karşıya kaldığı mülteci krizi tartışmalarının vazgeçilmez parçası haline geldi.

Fakat güncel durumda, Türkiye ile AB arasında vize serbestliğine ilişkin müzakereler hem katılım müzakerelerinden hem de Gümrük Birliği'nden bağımsız olarak, Türkiye-AB Vize Serbestliği Diyaloğu çerçevesinde gerçekleşiyor. Bu bağlamda, Türkiye'nin, Avrupa Komisyonu tarafından ortaya koyulan ve 2013 yılında taraflarca kabul edilen Vize Serbestliği Yol Haritası'nın 5 bloğunda yer alan 72 kriteri gerçekleştirmesi gerekiyor. Ayrıca Aralık 2013 yılında imzalanan Türkiye-AB Geri Kabul Anlaşması'nın etkin bir şekilde işletilmesi de önemli kıstaslardan bir tanesi. Daha önce de belirtildiği üzere, temel felsefe olarak, AB ülkelerine serbestçe girebilmek ve AB ülkelerinde serbestçe dolaşabilmek için, kaynak ülkelerin; AB ülkelerini, Avrupa standartlarında bir güvenlik anlayışına ve altyapısına sahip olduklarına inandırması gerekiyor. Bu anlayış, Türkiye-AB Vize Serbestliği Yol Haritası'na da büyük ölçüde yansıyor. Öyle ki, vizesiz seyahat için AB'nin Türkiye'den en temel beklentilerinden biri, Türkiye'nin veri güvenliği alanında Avrupa standartlarına ulaşabilmesi. Vize Serbestliği Yol Haritası'nda en az 10 kriter bu konu ile bağlantılı. Başka bir deyişle, Türk vatandaşlarının vizesiz Avrupa hayalinin gerçekleşebilmesi için Türkiye'de, AB standartlarında bir veri güvenliği sistemi oluşturulması gerekiyor.

7.1.Türkiye - AB Vize Serbestliği Diyaloğu'nda Kişisel Veriler Nasıl Değerlendiriliyor?

Avrupa Komisyonu'nun Türkiye'nin vize serbestliği diyaloğuna ilişkin performansını değerlendirdiği 20 Ekim 2014 tarihli ilk raporda, Türkiye'nin hangi alanlarda veri güvenliğine ilişkin ileri adımlar atması gerektiğinin altı çiziliyor. Yol haritasının belge güvenliğine ilişkin 1'inci bloğunda ortaya koyulan kriterlere göre, Türkiye'nin AB standartlarında pasaportlara geçiş yapması gerekiyor. Bunun için ise, Komisyon'un öne sürdüğü üzere Türk pasaportlarında, pasaport sahibinin dijital fotoğrafının yanı sıra, parmak izi gibi biyometrik verilerinin de pasaportun içerisinde yer alması gerekiyor.

Biyometrik verilerin etkin kontrolü ve muhafazası, özellikle etkin veri güvenliği altyapısına sahip olmayan gelişmekte olan ülkelerde büyük zorluklara sebep oluyor. Bununla birlikte, biyometrik verilerin etkin kontrolü ve kullanımı, temel sosyal ihtiyaçlara ulaşım, gıda güvenliği, sağlık, seçim sistemleri, kimlik kaydı, ulusal güvenlik ve göç yönetimi gibi çok çeşitli alanlarda kapsayıcı ve sürdürülebilir kalkınmanın önünü açıyor. Dolayısıyla hassas veri niteliğindeki biyometrik verilerin, gelişmekte olan ülkelerde kalkınmaya ve iyi yönetişime olumlu etkisi, bu ülkelerde kişisel verilerin korunmasına yönelik etkin sistemlerin oluşturulması ile doğrudan orantılı.

Geçtiğimiz dönemlerde "parmak izi" en çok bilinen biyometrik veri niteliğindeyken, günümüzde DNA'lar, retina taramaları ve insan seslerine kadar çok çeşitli biyometrik veriler, yukarıda belirtilen amaçlar doğrultusunda kullanılıyor. Biyometrik verilerin güvenliği ve etkin kullanımı ise, bu verilerin işlenme süreci ve muhafaza sürecinin sorunsuz ve yeterli olmasını gerekli kılıyor. Verilerin işlenme ve muhafaza sürecinin sorunsuz gerçekleşmesini sağlayacak hukuki ve teknik altyapının olmadığı bölgelerde, temel hak ihlalleri gerçekleşebiliyor. Örneğin, yetersiz teknik alt yapının bulunduğu bir sınır bölgesinde, sığınma talebinde bulunan bir kişinin parmak izi, veri tabanındaki parmak izleriyle karşılaştırıldığında, bu kişinin parmak izinin başka bir sığınmacının parmak iziyle eşleşmesi halinde, ilgili kişinin sığınma talebinin reddedilmesi ve böylelikle temel bir hakkının ihlal edilmesi söz konusu olabilir. Özellikle sınır kontrolünde, mültecileri ve göçmenleri kayıt altına almak için kullanılan biyometrik verilerin saklandığı veri tabanlarının, belirtilen amacın dışında kullanımı ve merkezi bir sistem üzerinde tutulması halinde yanlış ellere geçmesi, hukuki açıdan en temel sakıncaları oluşturuyor[62].

Dolayısıyla Türkiye'nin bu kriteri karşılayabilmesi için, hassas kişisel verilerin korunması konusuna eğilen hukuki düzenlemeler ve teknik altyapı oluşturulması gerekiyor. Komisyon, benzer standartların, kimlik belgeleri için de geçerli olması gerektiğini öne sürüyor. Komisyon özellikle Türk yetkili makamlarını, eski fotoğraflı kimlik belgelerini geçersiz kılmaya veya kimlik belgelerine geçerlilik süresi getirmeye çağırıyor.

Türkiye-AB Vize Serbestliği Yol Haritası'nın Göç Yönetimi başlıklı 2'nci bloğunda da veri güvenliği konusu üzerinde duruluyor. AB'nin, hem Türkiye-AB Katılım

Müzakereleri'nin 24 numaralı faslı (Adalet, Özgürlük ve Güvenlik) hem de vize serbestliği diyaloğu kapsamında en temel beklentilerinden birini, entegre sınır yönetimi stratejisi çerçevesinde, sınır güvenliğinden sorumlu bütün birimlerin etkin işbirliği içerisinde hareket etmesi oluşturuyor. Daha ileri vadede ise, sınır yönetiminden sorumlu bütün birimlerin birleştirilerek, yeni, sınır kontrolünden sorumlu bir birimin oluşturulması öngörülüyor. Bu işbirliğinin ve uzun vadede entegrasyonun sağlanabilmesi için ise öncelikli olarak, bütün sınır kontrol birimlerinin, gerekli hallerde diğer birimlerin veri tabanlarına ulaşabilmesi ve kişisel verilerin korunmasına ilişkin hukuk kurallarıyla uyumlu, karşılıklı etkin veri akışını sağlaması gerekiyor. Öte yandan, sınır kontrol birimlerinde ve diplomatik temsilciliklerdeki sorumlu personele veri/belge güvenliği alanında eğitim sağlanması da önemli bir gereklilik.

Veri güvenliği meselesi, vize serbestliği diyaloğu çerçevesinde üçüncü olarak, Türkiye ile AB arasındaki adli işbirliğinin geliştirilmesiyle bağlantılı olarak ele alınıyor. AB, hem vize serbestliği yol haritası kapsamında hem de katılım müzakerelerinin 24 numaralı faslının bir parçası olarak, Türkiye'nin Eurojust ve Europol ile etkin işbirliği kurması gerektiğini öne sürüyor. Bu işbirliğinin önemli bir boyutunu, adli, cezai ve güvenlikle ilgili meselelerde tarafların karşılıklı anlık veri paylaşımı gerçekleştirebilmesi oluşturuyor. Fakat güncel konjönktürde, Türkiye'de geçerli bir kişisel verilerin korunması kanunun bulunmaması sebebiyle bu işbirliğinin önü kesiliyor. Bilindiği üzere, AB kurumlarının herhangi bir üçüncü ülke birimiyle veri paylaşımı gerçekleştirebilmesi için, ilgili üçüncü ülkede AB standartlarında bir veri güvenliği mevzuatı bulunması gerekiyor. Dolayısıyla Eurojust ve Europol halihazırda Türkiye ile karşılıklı kişisel ve gizli veri akışı gerçekleştiremiyor.

7.2.Europol'ün Veri Güvenliği Politikası

1998 yılında kurulan ve merkezi Hollanda'nın Lahey şehrinde bulunan Europol, o tarihten bu yana AB'nin resmi kolluk birimi olarak görev yapıyor. Europol'ün temel görev ve sorumluluklarını, organize suçla, terörle ve diğer ciddi suçlarla mücadeleye AB çapında destek vermek oluşturuyor. Bu görev ve sorumluluklar çerçevesinde, Europol Bilgi Sistemi adlı bir yapı aracılığıyla Europol ile ulusal Europol birimleri ve ulusal kolluk birimleri arasında veri paylaşımı gerçekleştiriliyor. Europol Bilgi Sistemi üzerinden, Europol'ün ve

ulusal Europol birimlerinin yukarıda belirtilen nitelikteki suçların şüphelilerine, zanlılarına veya suç işleyeceği yönünde şüphe oluşan kişilere ilişkin verilere ulaşabilmesi mümkün.

Europol'ün Kuruluşuna ilişkin Avrupa Konseyi Kararı (*Europol Decision*)'nın 27'nci maddesinde belirtildiği üzere Europol, suçla mücadeleye yönelik verileri işlerken ve üye ülkelerle Europol Bilgi Sistemi üzerinden karşılıklı veri paylaşımı gerçekleştirirken, bütün süreçlerin ilgili AB müktesebatına ve 108 sayılı Avrupa Konseyi Sözleşmesi'ne uyumlu olması gerekiyor. Başka bir deyişle, kişisel verilerin her daim koruma altında olması gerekiyor. Bunun sağlanması için ise bağımsız bir Europol Ortak Denetim Kurulu görev yapıyor[63].

7.3.Eurojust ve Kişisel Verilerin Korunması

Eurojust, en az iki üye ülkeyi ilgilendiren ciddi suçların kovuşturma ve soruşturma aşamalarına katkı sağlamak ve adli işbirliğini artırmak amacıyla 2002 yılında göreve başladı. Bu çerçevede Eurojust, yetki alanındaki cezai süreçlerde, suçlulara, suçun mağdurlarına ve tanıklarına ilişkin kişisel verileri, sadece gerekli olduğu hallerde ve gerektiği kadarıyla sınırlı olmak üzere işleyebiliyor.

İstisnai hallerde, devam etmekte olan bir soruşturma için acilen gerektiğinde, kısa süreyle daha detaylı kişisel verileri işleme olanağına sahip. Bu amaç doğrultusunda Eurojust'un, diğer AB kurumları ile, üye ülkelerle ve AB standartlarında veri güvenliği mevzuatına sahip üçüncü ülkelerle ve uluslararası kuruluşlarla işbirliğine gitme ve karşılıklı kişisel veri paylaşımı gerçekleştirme yetkisi bulunuyor. Europol'e benzer şekilde, Eurojust'un kişisel verilerin korunmasına ilişkin tutumunu takip eden bağımsız bir ortak denetim birimi bulunuyor. Dolayısıyla Eurojust'un da bütün eylemlerinde, ilgili AB müktesebatına, Eurojust Veri Güvenliği Kurallarına ve Eurojust'u Kuran Konsey Kararı'na uyması gerekiyor[64].

7.4.Türkiye'de Bu Alanda Teknik Mevzuata ve Altyapıya Artan İhtiyaç

İç güvenlik ve adli işbirliğinin, Schengen sisteminin önemli bir boyutunu oluşturduğu ve AB projesinin bir standartlar bütünü olduğu düşünüldüğünde,

Türkiye'nin, ilgili AB kurumlarının ötesinde, üye ülkelerle işbirliğini artırabilmesi için de AB standartlarında veri güvenliği düzenlemeleri oluşturması ve yürürlüğe koyması gerekli.

Öte yandan, vize serbestliği yol haritası, etkin bir yasal mevzuatın oluşturulmasını bu alandaki kriterlerin karşılanması için yeterli görmemekle birlikte, Türk adli makamlar ve kolluk birimleri arasında veri ve istihbarat paylaşımını daha ileri aşamaya taşıyacak mekanizmalar kurulmasının gerekliliğini de vurguluyor. Bu doğrultuda kurulan UYAP (Ulusal Yargı Ağı Projesi) sistemi, Avrupa Komisyonu'nun Türkiye'ye ilişkin değerlendirmelerinde olumlu karşılanan konular arasında yer alıyor. Fakat Avrupa Komisyonu, Türkiye'nin ulusal mevzuatın yüklenilmesinin ötesinde, uluslararası yükümlülüklerinin de altını çiziyor. Bu kapsamda Türkiye, 108 sayılı Avrupa Konseyi Sözleşmesi ile 181 sayılı Ek Protokolü ve kişisel verilerin korunmasına ilişkin diğer uluslararası belgelerin imzalamaya ve Türkiye ile AB arasında imzalanan Geri Kabul Anlaşması'nın veri güvenliğiyle ilgili hükümlerini uygulamaya çağırılıyor. Bilindiği üzere, Kopenhag Kriterleri'ne uyum amacıyla daha da güçlendirilen Anayasa'nın 90'ıncı maddesi, uluslararası antlaşmaların kanun hükmünde olduğunu belirtiyor. Ayrıca vize serbestliği yol haritasının değerlendirildiği ilk Komisyon raporunda (Ekim 2014), gerçekleştirilmesi öngörülen bütün bu reformların gözetiminden sorumlu bağımsız bir denetim mekanizmasının öneminin de özellikle altı çiziliyor.

Sonuç olarak, Türk vatandaşlarının vizesiz Avrupa idealini gerçekleşebilmesi için, AB standartlarında bir kişisel verilerin korunması mevzuatının acil şekilde oluşturulması gerektiğini önemle hatırlatmak gerekiyor. Bununla birlikte, vize serbestliği yol haritasının ilgili kriterlerinin yerine getirilebilmesi için, özellikle üç blokta Türk yetkili makamların veri güvenliği ile bağlantılı reformları hızlı bir şekilde yerine getirmesi gerekiyor;

- Belge Güvenliği Bloğu
- Göç Yönetimi Bloğu
- Kamu Düzeni ve Güvenliği Bloğu.

7.5.AB'nin Cezai Meselelerde ve Sınır Yönetiminde Veri Güvenliği Kapasitesi

Henüz Birlik çapında bir Kişisel Verilerin Korunması Tüzüğü üzerinde uzlaşmaya varamayan ve yakın tarihte ABD ile veri paylaşımı üzerine anlaşmalarının ABAD gündemine alındığı AB'nin de; özellikle adli, cezai, güvelik ve göç yönetimiyle ilişkili konularda veri güvenliği konusunda kapsayıcı ve eksiksiz bir yaklaşım benimseyemediği ortada. Bu durum özellikle AİHM ve ABAD kararlarında büyük ölçüde yankı buldu.

Örneğin; *S. ve Marper v Birleşik Krallık* AİHM Davası'nda, suçlanan fakat henüz hüküm giymemiş olan kişilerin parmak izlerinin, DNA'larının, hücre örneklerinin kolluk birimleri tarafından tutulması ve depolanması üzerine, ilgili kişiler, haklarının ihlal edildiği yönündeki şikayetlerini AİHM'e kadar taşıdı. AİHM, hassas nitelikteki biyometrik verilerin sınırlı sürelerle tutulabileceğine ve veri sahibinin gizlilik hakkının dikkate alınması gerektiğine, dolayısıyla AİHS'in 8'inci maddesinin ihlal edildiğine hükmetti. Bu konu, özellikle sınır ve göç yönetimi gibi ulusal güvenlikle bağlantılı alanlarda ele alındığında, özgürlük ve güvenlik dengesi açısından oldukça hassas durumlar yaratıyor[65].

Az önce ifade edildiği üzere, dış sınırların ötesinden ve iç sınırlarından AB ülkelerine seyahat, AB projesinin temel unsurları arasında yer alıyor. Schengen Sistemi de bu amacın gerçekleştirilmesine ve sınırların etkin şekilde yönetilmesine yönelik adımları içeriyor. Dolayısıyla sınır yönetiminde gelişen teknolojilerin önemi her geçen gün artıyor. Göçmen krizinin etkisiyle AB sınırlarından giriş yapmaya çalışan üçüncü ülke vatandaşlarının sayısında her geçen gün yaşanan büyük artış, kişilerin tespiti, kayıt altına alınması ve bu kişilere ilişkilerin verilerin depolanmasına ilişkin teknik altyapının önemini de her geçen gün artırıyor[66].

Bu sebepten ötürü AB de, gelişen teknolojiler ve güncel popüler fenomenlerin etkisiyle, teknoloji odaklı veri güvenliği sistemlerini, sınır kontrol politikalarının merkezine yerleştirdi.

Adli, cezai meselelerle sınır yönetiminin, AB Veri Güvenliği Yönergesi'nin kapsamı dışında kalması sebebiyle, 27 Kasım 2008 tarihinde Konsey, Cezai Meselelerde Kolluk ve Adli İşbirliği Çerçevesinde İşlenen Kişisel Verilerin Korunmasına ilişkin 2008/977/JHA sayılı Kararı kebul etti. 2008 tarihinden itibaren AB'de sınır ötesi işbirliğinin gerekli olduğu hallerde bu Çerçeve Karar geçerli olurken, ulusal güvenliğin söz konusu olduğu ve sınır ötesine taşmayan durumlar, Çerçeve Karar'ın yargı yetkisi dışında kaldı[67].

Çerçeve Karar da, kişisel verilerin korunması'na ilişkin benzer nitelikteki AB mevzuatında olduğu gibi, kişisel verilerin sadece yetkili makamlar tarafından ve önceden belirtilen belirli amaçlar doğrultusunda işlenmesini mümkün kılan hükümler içeriyor. Öte yandan kişisel verilerin, sınır ötesi iş birliği kapsamında kaynak üye ülkeden üçüncü tarafa transferi de diğer benzer nitelikteki hukuki belgelerde belirtildiği üzere, AB üyesi kaynak ülkenin rızası dahilinde mümkün olabiliyor. Çerçeve Karar'dan daha ileri işbirliğini ortaya koyan hukuki yapılar da bulunuyor. *Prüm Kararı* olarak da adlandırılan, 2008/615/JHA sayılı Konsey kararı bu örnekler arasında. *Prüm Kararı,* imzacı AB üyesi ülkeler arasında, özellikle terörle ve ciddi suçlarla mücadelede işbirliğine yönelik etkin veri paylaşımının çerçevesini çiziyor. *Prüm Kararı*; imzacı ülkelerdeki DNA profillerine, parmak izi veri tabanlarına ve ulusal araç kayıt bilgilerine otomatik erişim; sınır ötesi büyük ölçekli vak'alara ilişkin verilerin sağlanması; terör suçunun önlenmesine yönelik veri paylaşımı ve sınır ötesi kolluk işbirliğini artıracak diğer alanlarda hükümler içeriyor. Dolayısıyla imzacı üye ülkeleri, Prüm Sistemi ile uyumlu ulusal mevzuat ve teknik altyapı oluşturmaları gerekiyor. Fakat uluslararası sivil toplum temsilcileri, bütün devletlerin eşit standartlarda düzenlemeler gerçekleştiremediği ve imzacı ülkelerin büyük bölümünün yeterli teknik altyapıya sahip olmadığı yönünde eleştirilerde bulunuyor. Teknik altyapı yetersizliği de yanlış biyometrik verilerin eşleşmesi gibi bir takım büyük sorunlara sebep olabiliyor. Dolayısıyla, hukuki çerçevenin yanı sıra, AB çapında etkin sınır yönetiminin önemli bir parçasını oluşturan ortak bilgi sistemlerinin niteliği ve işlerliği de büyük önem taşıyor[68].

Europol ve Eurojust gibi Avrupalı kurumların oluşturulması ve ilgili yasal mevzuatın oluşturulmasının yanı sıra; AB tarafından sınır ve göç yönetiminde iş birliğine yönelik önlemler arasında, bir takım veri paylaşım platformları

oluşturulması yer alıyor. Bu platformlar arasında en ön planda olanları ve Türkiye-AB Vize Serbestliği Diyaloğu ile İlerleme Raporlarına da yansıyanları; Schengen Bilgi Sistemi (*Schengen Information System II*) ile Vize Bilgi Sistemi (*Visa Information System*).

7.6.Schengen Bilgi Sistemi

En son haline 9 Nisan 2013 tarihinde getirilen Schengen Bilgi Sistemi (SIS II), bütün AB üye ülkeler ile, Norveç, İsviçre, Lihtenştayn ve Europol ile Eurojust'a erişim sağlıyor. Her üye ülkede bulunan ulusal sistemler (N-SIS) ve merkezi bir sistemden (C-SIS) oluşan Schengen Bilgi Sistemi, üye devletlerin, kişilere ilişkin girdiği verileri içeriyor. Bu veriler ise, Schengen bölgesi içerisinde yer alan ulusal sınır kontrol, kolluk, gümrük ve vize birimleri tarafından kullanılıyor. Bilgileri sorgulanan kişinin Schengen alanına girme hakkının bulunmadığı; kolluk birimleri tarafından aranmakta olduğu; kayıp olarak addedildiği hallerde veya kayıtlarla karşılaştırılan eşyaların çalıntı çıktığı hallerde Schengen Bilgi Sistemi uyarıda bulunuyor. Uyarının ardından ise ulusal sistemler (N-SIS) gerekli önlemleri alıyor.

Schengen Bilgi Sistemi'nin ve bu kapsamda alınan önlemlerin de benzer nitelikteki AB unsurları gibi, 108 sayılı Avrupa Konseyi Sözleşmesi ve diğer bağlantılı mevzuat ile uyumlu olması gerekiyor. Her üye ülkedeki Veri Güvenliği Kurullarının, o ülkenin ulusal bilgi sistemine girilen verilerin doğru ve uygun olduğunu gözlemleme sorumluluğu bulunuyor. Merkezi sistemin (C-SIS) gözetiminden sorumlu kurum ise Avrupa Veri Güvenliği Gözetmeni (EDPS).

7.7.Vize Bilgi Sistemi

Vize Bilgi Sistemi (VIS), AB'nin ortak vize politikasının uygulanabilmesini desteklemek amacıyla oluşturuldu. VIS aracılığıyla Schengen ülkelerinin üçüncü ülkelerde bulunan diplomatik temsilcilikleri ile Schengen ülkelerinin dış sınır geçiş noktaları arasında vizelere ilişkin karşılıklı veri paylaşımını sağlıyor. Kısa süreli vize başvurularına ilişkin verilerin işlendiği VIS, sınır kontrolünden sorumlu birimlere, vizeyi sunan kişinin doğru kişi olup olmadığını ve sunulan belgenin sahte olup olmadığını tespit etme olanağı sağlıyor.

VIS'e veri girişi, bu veriler üzerinde değişiklik yapma veya verileri silme yetkisi, ilgili üye ülkede vize politikalarından sorumlu ilgili birimler tarafından üstleniliyor. Öte yandan gerekli hallerde, gerektiği kadarıyla bu verilere ulaşım hakkı; dış sınırlarda kontrolden sorumlu birimlerle, göç ve sığınma taleplerine ilişkin kontrolü sağlayan birimlere de tanınıyor. Bununla birlikte terörün ve ciddi suçların tespiti ve önlenmesi için gerektiği takdirde, yetkili ulusal kolluk birimleri ve Europol de, VIS üzerinde tutulan verilere erişim talebinde bulunabiliyor. Ayrıca Eurosur (*European Border Surveillance System*) da, bu sistemleri desteklemek amacıyla, Schengen dış sınırlarının kontrolü, hukuk dışı göç ve sınır ötesi suçla mücadeleye yönelik veri paylaşımına olanak sağlıyor.

SONUÇ YERİNE: YAKIN GELECEKTE KÜRESEL YÖNETİŞİMİN ODAĞINDA KİŞİSEL VERİLER

Bu çalışma, kişisel verilerin korunması konusunun hem ulusal, hem bölgesel hem de küresel iyi yönetişim tartışmalarının merkezindeki yerinin her geçen gün artmakta olduğu bir tarihte hazırlandı. AB'ye bakıldığında, uluslararası hava yolcularına ilişkin verilerin sistematik şekilde toplanmasına ve muhafazasına ilişkin Birlik çapında geçerli bir PNR Yönergesi'nin oluşturulması üzerinde AB kurumları arasında anlaşmaya her zamankinden yakın olunduğu görülüyor. Bununla birlikte AB kurumları, sınır yönetiminde otomatik ve hızlı veri depolamaya ve paylaşımına dayalı "akıllı sınırlar" üzerine çalışmalarını her zamankinden daha da yoğunlaştırdı. Hatta AB Kişisel Verilerin Korunması Tüzüğü'nün hazırlıklarının önümüzdeki dönemde hem temel haklar hem dijital ekonomi kapsamında, AB'nin öncelikli konu başlıkları arasında yer aldığı muhakkak. Çalışma boyunca gerçeştirilen değerlendirmeler kapsamında görülüyor ki AB, kişisel verilerin korunması alanında bütüncül ve korumacı yaklaşımını önümüzdeki dönemde de sürdürecek.

Avrupa Komisyonu'nun ve bir takım AB ülkelerinin üyesi olduğu, küresel yönetişimin bir diğer odağı G20 çerçevesinde de veri güvenliği konusu, gündemin bir parçası. 2015 yılında, Türkiye dönem başkanlığında hazırlanan G20 Sonuç Bildirisi'ne bakıldığında, konunun hem bilgi teknolojileri hem de siber güvenlik ile bağlantılı olarak liderlerin gündemine alındığı görülüyor. Öte yandan Türkiye dönem başkanlığındaki G20'nin sivil toplumu ve iş dünyasını temsil eden resmi açılım grupları C20 ve B20 çerçevesinde de konu çeşitli defa gündeme taşındı.

Anlaşılacağı üzere, Türkiye'nin, küresel yönetişim tartışmalarının parçası olabilmesi; parçası olduğu entegrasyon projelerindeki konumunu sağlamlaştırması ve sorumluluklarını yerine getirebilmesi için etkin bir kişisel verilerin korunması mevzuatı şart. Fakat çalışma boyunca ortaya koyulan görüş ve değerlendirmeler ışığında belirtilmelidir ki, bir kişisel verilerin korunması kanunun oluşturulması, Türkiye'de bu alanda temel hak ve özgürlüklerin garanti altına alınabilmesi için yeterli değil. Hazırlanması öngörülen bu kanunun, temel hak ve özgürlükleri eksiksiz şekilde koruduğunun garanti altına alınması,

bununla birlikte AB ülkeleri ile ilgili AB kurumları ve birimlerindekiyle benzer nitelikte bir denetim mekanizmasının oluşturulması gerekiyor. Bu reformların gerçekleşmesiyle, Türkiye-AB müzakereleriyle eş zamanlı olarak Türkiye-AB Vize Serbestliği Diyaloğu ve gümrük birliğinin güncellenmesi çalışmalarının büyük ölçüde, olumlu ivme kazanacağını öngörmek mümkün.

Çalışmanın hazırlık ve yazım aşamasında görüldüğü üzere, Avrupa çapında, politika üretim çalışmalarının odaklandığı bu alanda, Türkçe çalışmalar yeterli sayıda değil. Dolayısıyla bu çalışma, temel kavramsal ve hukuki çerçeveyle birlikte, AB standartlarını, Türkiye ve AB'deki temel tartışmalar ile Türkiye'nin uyumunu ele alırken konuya ilişkin bir takım temel sorunları ve tartışmalı alanları ortaya koyuyor. Şüphesiz ki Türkiye ile birlikte uluslararası literatürde de tartışılan konuyla bağlantılı pek çok sorun, sivil toplum-akademi-işdünyası ve kamu işbirliğine dayanan ileri aşama kolektif çabayı gerektiriyor. İlgili paydaşların bu alandaki etkin işbirliği, Türkiye'de Avrupa standartlarında insan hakları kültürünün oluşması ve refahın gelişmesi açısından da elzem.

Kişisel verilerin korunması tartışmalarının odağındaki sorunların başında şüphesiz ki **kişisel verilerin korunması ile bağlantılı hakların ilişkisi ve sınırları** meselesi geliyor. Avrupa Komisyonu'nun hazırladığı 2015 Türkiye İlerleme Raporu'nda göze çarpan temel bulgulardan biri, Komisyon'un, temel hak ve özgürlüklere ilişkin olarak en fazla, kişisel verilerin korunması konusu ile birlikte, bilgiye erişim hakkı ve ifade özgürlüğünü gündeme taşımasıydı. Aynı şekilde, bu çalışmada da değinildiği üzere, sivil toplumun katılımı, karar alma süreçlerinde verilere erişim ve şeffaflık noktasında yetkili kamu kurumları tarafından sınırlandırmaya gidilirken öne sürülen öncelikli savlardan biri, kişisel verilerin korunması, ulusal güvenlik ve veri güvenliği oluyor. Dolayısıyla, önümüzdeki dönemde, hangi hallerde kişisel verilerin karşılıklı dolaşımının ve bilgiye erişimin sınırlanabileceğine yönelik ileri aşama tartışmaların sürmesi gerekiyor.

Kişisel verilerin hangi hallerde koruma altında olduğu, öte yandan hangi hallerde yetkili kamu kurumları tarafından erişilebileceği meselesinin ilgili kanun tasarısında nasıl ele alındığı da temel hak ve özgürlüklere ilişkin önümüzdeki dönemde daha fazla tartışılan konuların başında gelmeli. Bu noktada kamu güvenliği garanti altına alınırken, temel hak ve özgürlüklerin zedelenmemesinin

sağlanması gerekiyor. Kişisel verilerin korunması alanında atılacak her olumlu adımın, eş zamanlı olarak hem Türkiye-AB katılım müzakerelerinde hem vize serbestliği diyaloğunda hem de ticari ilişkilerde olum hava oluşturacağı; paralel olarak temel hakların güvence altına alınmasına da katkı sağlayacağı göz önüne alındığında, bu alandaki reform çabalarında hız kaybedilmemesi büyük önem taşıyor. Böylelikle küresel yönetişimin odağındaki öncelikli bir konuda, küresel konjönktürün gerisinde kalınmamış olacaktır.

SON NOTLAR

1. Avrupa Komisyonu, "Commission proposes a comprehensive reform of data protection rules to increase users› control of their data and to cut costs for businesses", Press Release, 25 Ocak 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm, Erişim Tarihi:20.11.2014
2. Steve Peers, "Basic data protection principles in the proposed Data Protection Regulation: back to the future?", Statewatch Analysis, p.1.
3. Adalet Bakanlığı, Kişisel Verilerin Korunması Kanun Tasarısı, http://www.kgm.adalet.gov.tr/tasariasamalari/basbakanlik/Kanuntas/kisiselveriler.pdf, ErişimTarihi:20.11.2014
4. European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, p.17.
5. Songül Atak, "Avrupa Konseyi'nin Kişisel Verileri Açısından Sağladığı Temel Güvenceler", TBB Dergisi, Sayı 87, 2010.
6. Article 2, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/html/108.htm , Erşim Tarihi:04.12.2014
7. Leyla Keser vd., Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, TEPAV, 2014, ss.62-63.
8. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, Erişim Tarihi: 21.11.2014.
9. Avrupa Komisyonu, "How does the data protection reform strengthen citizens' rights?", Data Protection Facts Sheet, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf, Erişim Tarihi:22.11.2014.
10. Avrupa Komisyonu, "Commission proposes a comprehensive reform ofdata protection rules to increase users› control of their data and to cut costs for businesses", Press Release, 25 Ocak 2012.
11. "Angela Merkel calls for EU-wide agreement on data protection", Financial Times, 2013, http://www.ft.com/intl/cms/s/7a4b26d8-eca6-11e2-a0a4, Erişim Tarihi: 22.11.2014

12. Avrupa Komisyonu, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, p.2, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, Erişim Tarihi 23.11.2014.
13. Avrupa Komisyonu, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, p.182, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, Erişim Tarihi 23.11.2014.
14. Avrupa Komisyonu, "Commission proposes a comprehensive reform of data protection rules to increase users› control of their data and to cut costs for businesses", Press Release, 25 Ocak 2012.
15. Avrupa Komisyonu, Factsheet on the "Right to be forgotten" ruling, C-131/12, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Erişim Tarihi: 23.11.2014
16. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 2001, http://conventions.coe.int/Treaty/en/Treaties/html/181.htm, Erişim Tarihi:26.11.2014.
17. European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, pp.130-131.
18. Sözleşmeyi imzalayan devletlere buradan ulaşılabilir: http://conventions.coe.int/Treaty/Commun/cherchesig.asp?nt=108&cl=eng, Erişim Tarihi:27.11.2014
19. Atak, a.g.e., s.94.
20. Melih Özsöz ve Özgür Bozçağa,"Anayasa Değişikliği Paketinin Türkiye'nin AB Müktesebatına Uyumuna Etkisi", İKV Değerlendirme Notu, 2010, http://ikv.org.tr/images/upload/data/files/anayasa_degisikligi_degerlendirme_notu(1).pdf, Erişim Tarihi: 27.11.2014.
21. AB Bakanlığı, "Avrupa Birliğine Katılım için Ulusal Eylem Planı II. Aşama", s.144,http://www.abgs.gov.tr/files/uepii.pdf
22. Songül Atak, Avrupa Koniseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, TBB Dergisi, No.87, 2010, ss.92-93.
23. Věra Jourová: "We will be strict with the US on Safe Harbour", EurActiv, http://www.euractiv.com/sections/infosociety/vera-jourova-we-will-be-strict-us-safe-harbour-312856. Erişim tarihi:28.03.2015.
24. Commissioner Jourová›s statement at the Justice and Home Affairs Council (press conference) 13 March 2015, http://ec.europa.eu/commis-

sion/2014-2019/jourova/announcements/commissioner-jourovas-statement-justice-and-home-affairs-council-press-conference-13-march-2015_en Erişim Tarihi: 28 Mart 2015.
25. Peers, a.g.e., p.4. Basic data protection principles in the proposed Data Protection Regulation: back to the future?, Statewatch Analysis, p.4.
26. European Commission, "How will the EU's data protection reform benefit European businesses?", http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf.
27. Council of the European Union, Data protection: Council agrees on general principles and the «one stop shop» mechanism, http://www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/.
28. EU Seeks to Tighten Data Privacy Laws, The Wall Street Journal, http://blogs.wsj.com/digits/2015/03/10/eu-seeks-to-tighten-data-privacy-laws/.
29. Dilek Aydın, "İnternet, Transatlantik İlişkiler ve Avrupa Birliği", TUSİAD Avrupa Birliği Temsilciliği, Mart 2014, http://www.gundem.be/file/download/140325121547_0_1_889878
30. Kişisel Verilerin Korunması Kanun Tasarısı Hakkında TÜSİAD Görüşü, 19 Ocak 2015, ss. 17-18.
31. Jeremy Fleming,"TTIP: Data is the elephant in the room", Euractiv, 24.08.2013, http://www.euractiv.com/specialreport-eu-us-trade-talks/ttip-data-elephant-room-news-530654, Erişim Tarihi: 20.09.2015.
32. European Commission, "Data Protection Factsheet", Eurobarometer, 24.06.2015, http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.
33. European Commission, "Data Protection Factsheet", Eurobarometer, 24.06.2015, http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.
34. Paul Hofheinz ve Michael Mandel, "Uncovering the Hidden Value of Digital Trade", the Lisbon Council –Progressive Policy Institute, 02.07.2015, http://www.progressivepolicy.org/issues/economy/uncovering-the-hidden-value-of-digital-trade/, Erişim Tarihi: 21.09.2015.
35. Margot Kaminski, "Why trade is not the place for the EU to negotiate privacy", Internet Policy Review, 23.01.2015, http://policyreview.info/articles/news/why-trade-not-place-eu-negotiate-privacy/354, Erişim Tarihi: 18.09.2015.
36. Privacy International, "Privacy is not a commodity to be traded", 21.07.2013,

https://www.privacyinternational.org/node/246, Erişim Tarihi: 15.09.2015.
37. European Commission, "Services in TTIP", http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152999.2%20Services.pdf, Erişim Tarihi. 19.09.2015.
38. European Parliament, "TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEPs", European Parliament News, 31.03.2015, http://www.europarl.europa.eu/news/en/news-room/content/20150330IPR39308/html/TTIP-Trade-agreements-must-not-undermine-EU-data-protection-laws-say-MEPs, Erişim Tarihi: 01.10.2015.
39. Hofheinz ve Mandel, a.g.e.
40. Paul Van den Bulck ve William J. Cook, "United States: Safe Harbor, Standard Contractual Clauses, Binding Corporate Rules", Mondaq, 27.02.2014, http://www.mondaq.com/unitedstates/x/295710/Trade+Regulation+Practices/Safe+Harbor+Standard+Contractual+Clauses+Binding+Corporate+Rules, Erişim Tarihi: 22.09.2015.
41. Marlon Graf, ACTA Revisited? TTIP and Data Privacy, The RAND Blog, RAND Corporation, 25.11.2014, http://www.rand.org/blog/2014/11/acta-revisited-ttip-and-data-privacy.html, Erişim Tarihi: 10.09.2015.
42. Advocate General's Opinion in Case C-362/14 Maximillian Schrems v Data Protection Commissioner, Court of Justice of the European Union Press Release, No 106/15, 23.09.2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf
43. Leo Kelion, "Facebook privacy campaign advances after EU court opinion", BBC News, 23.09.2015, http://www.bbc.com/news/technology-34336111?ocid=socialflow_twitter, Erişim Tarihi: 26.09.2015.
44. Ombudsman commends Commission for progress on transparency in TTIP negotiations, European Ombudsman Press Release, 23.03.2015, http://www.ombudsman.europa.eu/en/press/release.faces/en/59353/html.bookmark, Erişim Tarihi:04.10.2015
45. European Ombudsman, "Ombudsman commends Commission for progress on transparency in TTIP negotiations", 23.03.2015, http://www.ombudsman.europa.eu/en/press/release.faces/en/59353/html.bookmark , Erişim Tarihi: 06.11.2015.
46. European Ombudsman, "Further steps to increase TTIP transparency necessary", 07.01.2015, http://www.ombudsman.europa.eu/en/press/release.faces/en/58669/html.bookmark (Erişim Tarihi: 8.11.2015)

47. C20 Türkiye Yolsuzlukla Mücadele Politika Belgesi, http://c20turkey.org/uploads/C20-AntiCorruption%20WGTR.pdf
48. Fiona Smith vd., "Supporting sustainable development with open data, Open Data Institute", 2015, pp. 3-4.
49. Michael Chui, Open data: Unlocking innovation and performance with liquid information, McKinsey Global Institute, 2013, http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information. Erişim Tarihi:15.10.2015.
50. Open Data Barometer 2nd Edition, 2015, http://barometer.opendataresearch.org/report/analysis/rankings.html.
51. European Commission, "Open data: An engine for innovation, growth and transparent governance", Communication, 2011, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011DC0882. Erişim Tarihi: 16.10.2015.
52. European Commission, "Delivering savings for Europe: moving to full e-procurement for all public purchases by 2016", Press Release, http://europa.eu/rapid/press-release_IP-12-389_en.htm.
53. European Commission, Open Data Portals, http://ec.europa.eu/digital-agenda/en/open-data-portals. Erişim Tarihi: 18.10.2015.
54. European Commission, "New EU website to provide easy and transparent access to aid data", Press Release, 2014, http://europa.eu/rapid/press-release_IP-14-434_en.htm.
55. Transparency Register, Who is expected to register?, http://ec.europa.eu/transparencyregister/public/staticPage/displayStaticPage.do?locale=en&reference=WHOS_IS_EXPECTED_TO_REGISTER.
56. Transparency InternationalEUOffice, Lobby meetings with EU policy-makers dominated by corporate interests, http://www.transparency.org/news/pressrelease/lobby_meetings_with_eu_policy_makers_dominated_by_corporate_interests.
57. Mark Perera vd., The European Union Integrity System, Transparency International EU Office, 2014, http://www.transparencyinternational.eu/wp-content/uploads/2014/04/EU_Integrity_System_Report.pdf.
58. Katleen Janssen ve Sara Hugelier, "Open data as the standard for Europe? A critical analysis of the European Commission›s proposal to amend the PSI Directive", European Journal of Law and Technology, vol.4, no.3, 2013, http://ejlt.org/article/view/238/411.

59. European Commission, EU implementation of the G8 Open Data Charter, 2013, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3489.
60. European Commission, EU implementation of the G8 Open Data Charter, 2013, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3489.
61. C20 Turkey Communiqué, 2015, http://c20turkey.org/uploads/C20%20Turkey%20Communique_FINAL_16.09.15.pdf.
62. Diana Dimitrova, Biometrics Please! Automated Border Controls & Data Protection Obligations, LSE Media Policy Project, 2014, http://www.printfriendly.com/print?url=http%3A%2F%2Fblogs.lse.ac.uk%2Fmediapolicyproject%2F2014%2F07%2F21%2Fbiometrics-please-automated-border-controls-data-protection-obligations%2F. Erişim Tarihi:21.11.2015
63. European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, pp.153-156.
64. European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, pp.153-156.
65. Case of S. And Marper v The United Kingdom, ECHR, 2008, https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf. Erişim Tarihi: 28.11.2015
66. Deloitte, Next Generation Smart Border Security, 2013, p.4.
67. European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, p.144.
68. Chris Jones, "Complex, technologically fraught and expensive - the problematic implementation of the Prüm Decision", Statewatch, http://www.statewatch.org/analyses/no-197-prum-implementation.pdf. Erişim Tarihi: 28.11.2015.

İKTİSADİ KALKINMA VAKFI

Esentepe Mahallesi Harman Sokak TOBB Plaza No:10 Kat:7-8
34394 Levent, Şişli/İstanbul/Türkiye
Tel: +90 212 270 93 00 Faks: +90 212 270 30 22
E-posta: ikv@ikv.org.tr

Avenue Franklin Roosevelt 148/A 1000 Brüksel/Belçika
Tel: + 32 2 646 40 40 Faks: + 32 2 646 95 38
E-posta: ikvnet@skynet.be

www.ikv.org.tr