

İKV DEĞERLENDİRME NOTU

KİŞİSEL VERİLERİN KORUNMASI: AVRUPA VE
TÜRKİYE

Ahmet CERAN
İKV Uzman Yardımcısı

İKTİSADİ KALKINMA VAKFI



KİŞİSEL VERİLERİN KORUNMASI: AVRUPA VE TÜRKİYE

Ahmet Ceran, İKV Uzman Yardımcısı

Günümüzde, artan bir hızla gelişen teknolojilerin ve küreselleşmenin etkilerinden, temel insan hakları da nasibini almış durumda. Temel hakların korunmasına ilişkin hukuki düzenlemelerle teknolojik gelişmelerin etkileşimi, hem iş çevrelerinde hem de akademik çevrelerde popüler bir tartışma konusu haline gelmekte. Bu çerçevede ilk olarak 1948 İnsan Hakları Evrensel Beyannamesi'nin 12'nci Maddesi'nde belirtilmiş olan "özel hayatın korunması", gelişen teknolojilerden ve küreselleşmeden en çok etkilenen temel haklar arasında yer alıyor¹. Bu noktada, özellikle kişisel verilerin korunması konusu özellikle, bazı AB ülkelerinde vatandaşlara ilişkin özel bilgilerin başka devletlerin istihbarat örgütlerinin eline geçmesi ve halka mal olmuş kişilerin özel hayatlarına dair verilerin internete sızması gibi sansasyonel olaylarla, gündemin merkezine oturuyor.

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 kullanılmakta. Bulut bilişim (*cloud computing*) ve benzeri, her gün gelişen teknolojilerle birlikte, "kişisel bir veri, internet aracılığı ile, Berlin'den işlenmek üzere Boston'a gönderilebilmekte ve Boston'da işlenen bu veri, depolanmak üzere Hindistan'ın silikon vadisi kabul edilen Bangalor'a çok kısa sürede ulaştırılabilmektedir"². Bu süreçler; bilgi teknolojilerindeki hızlı ilerleme ile beraber sınırların belirsizleşmesi, kişilik haklarının zarar görmesi, ulusal denetimin zorlaşması, mevcut hukuki düzenlemelerin yetersiz kalması gibi sorunların ortaya çıkmasına sebep olabilmektedir. 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 müzakere alanları ile doğrudan bağlantılı. Dolayısı ile Türkiye'nin, AB müktesebatına uyum noktasında, konuya ilişkin gelişmeleri önemle takip etmesi gerekmektedir. Bu çalışma kapsamında öncelikle konuya ilişkin temel kavramsal ve hukuki çerçeveye değinildikten sonra, AB'deki uygulamalar incelenmekte ve Türkiye'nin AB'deki uygulamalara uyumu değerlendirilmektedir.

Genel Tespitler

- ❖ Kişisel verilerin korunması konusunda, bireyinin güvenliğinin mi yoksa verilerin serbest dolaşımının mı önplana çıkarılacağı konusunda AB çapında genel bir kabule ulaşılamamıştır.
- ❖ Kişisel verilerin korunması, kişinin kendisine ilişkin verilere her şartta ulaşabilmesini ve verinin silinmesi talep edebilmesini de kapsamaktadır.
- ❖ Bu alanda AB çapında bir güvenlik/özgürlük dengesinin kurulabilmesi için her olayın kendi iç dinamiklerine göre değerlendirilmesi; yeni kararlarla gelişen bir içtihat hukukunun oluşması ve yasal mevzuatın modernize edilmesi gerekmektedir.
- ❖ 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 ötesinde önem taşımaktadır.
- ❖ Kişisel verilerin korunmasına yönelik AB içinde de tartışmaların bu dönemde Türk yetkili makamları tarafından atılacak adımlar, ilgili başlıklara ilişkin yükümlülüklerin yerine getirilmesi konusunda olumlu bir hava oluşmasına sebep olacaktır.

¹ Madde 12, *Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi*, TBMM İnsan Haklarını İnceleme Komisyonu, <http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf>, Erişim Tarihi:20.11.2014

² 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

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BASİT KAVRAMSAL VE HUKUKİ ÇERÇEVE

En temel tanımı ile kişisel veri; kişinin özel, profesyonel veya kamusal yaşamıyla bağlantılı 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 girmektedir. Türk yetkili makamlar 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 tanımlanmaktadır³. 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 alınmıştır. Bununla birlikte, 1960'lardan itibaren bilgi teknolojilerinde artan 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*) oluşturulmuştur. 108 sayılı Sözleşme, bu alanda bağlayıcılığı olan ilk düzenlemedir. Sözleşme'ye, Avrupa Konseyi üyesi olmayan Uruguay ve Fas gibi ülkeler de taraf konumundadır. Sözleşme'nin hükümleri, taraf ülkelerdeki özel sektörün ve kamu sektörünün tamamını bağlamaktadır⁴. Türkiye ise 1988 yılında 108 sayılı Sözleşme'yi imzalamış olsa dahi, daha onaylamamış ve yürürlüğe koymamıştır.

İlgili uluslararası düzenlemeler kapsamında, kişisel verilerin yanı sıra; özel koruyucu önlemleri gerekli kılan üç adet veri türü bulunmaktadır. 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 verilerdir. Bu veriler otomatik yollarla işlenemez⁵; yani manuel olmayan yollarla "*toplanamaz, kayıt altına alınmaz, depolanamaz, değiştirilemez.*"⁶ **Anonim veri** (*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, istatistiksel 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 aittir⁷. Farklı türlerine rağmen, bütün kişisel verilerin

³ Kişisel Verilerin Korunması Kanun Tasarısı, Adalet Bakanlığı, <http://www.kgm.adalet.gov.tr/tasariyasamalari/basbakanlik/Kanuntas/kisiselveriler.pdf>, Erişim Tarihi: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>, Erişim 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.

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 almaktadır. OECD yönlendirici ilkeleri, *Tablo 1*'de görülmektedir⁸.

Tablo 1 Sınır Ötesi Veri Akışlarına İlişkin 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.

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 AB⁹, kendi içinde ve üçüncü ülkelerle veri akışının tam kontrolünü sağlamakta ciddi zorluklarla karşılaşmakta. İkinci Dönem Barroso Komisyonu'nun 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 ediyor¹⁰. Öyle ki, konu Avrupa liderlerinin kendi iç kamuoylarında eleştirilmelerine bile sebep olabilmekte. Örneğin, 2013 yılında Alman vatandaşlarının internet üzerindeki kişisel verilerinin, İngiltere ve ABD istihbarat örgütleri tarafından

⁸ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>, Erişim Tarihi: 21.11.2014.

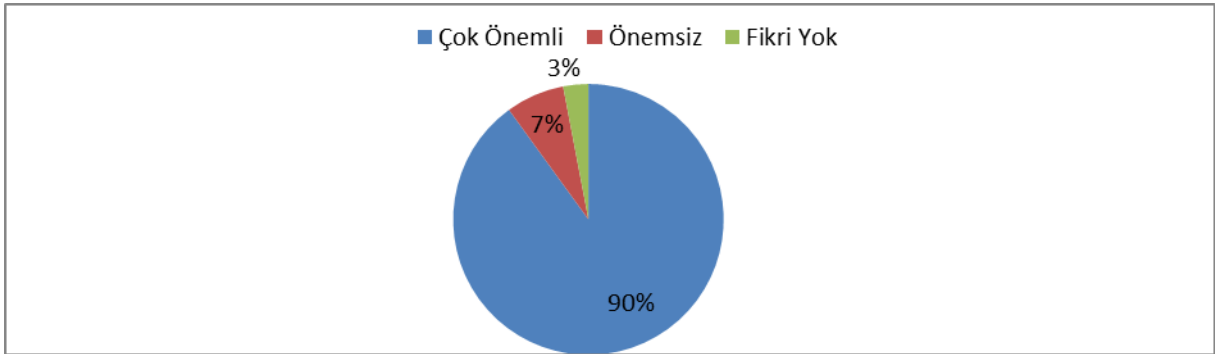
⁹ Avrupa Komisyonu, "How does the data protection reform strengthen citizens' rights?", *Data Protection Facts Sheet*, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf, Erişim Tarihi:22.11.2014.

¹⁰ Avrupa Komisyonu, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Press Release*, 25 Ocak 2012.

ele geçirilmesi ve kullanılması tartışmaları, seçim döneminde Almanya Şansölyesi Angela Merkel'in karşısına çıkan en zorlu muhalif propaganda hamleleri arasında yer aldı. Aynı şekilde ABD'nin, Merkel'i dinlediğine yönelik iddialar, dünyanın iki önemli gücü Almanya ve ABD arasında kısa süreli gerginliğe sebep oldu¹¹.

AB hukuku çerçevesinde, kişisel verilerin korunmasına ilişkin, AİHS ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin ötesinde de, birtakım adımlar atılmıştır. İlk olarak, 1995 yılında kabul edilen 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında Yönerge ile, Birlik dâhilinde verinin korunması alanında yüksek bir standart oluşturmaya çalışıldı. Verilerin Korunması Yönergesi, yüksek seviyede veri güvenliği sağlanmadığı takdirde, AB iç pazarında malların; kişilerin ve hizmetlerin etkin serbest dolaşımının mümkün olamayacağı ana fikri üzerine inşa edilmiştir. Bu doğrultuda Yönerge, 108 sayılı Avrupa Konseyi Sözleşmesi'ne ek olarak, AB ülkelerinde bağımsız denetim organları kurulmasını öngörmektedir. Öte yandan, gelişen teknolojilerin ve küreselleşmenin etkileriyle birlikte mevcut düzenlemelerin güncelliğini yitirmesi ve Birlik içerisinde veri güvenliğinin ideal ölçüde sağlanamaması, reform tartışmalarını gündeme taşımıştır. Avrupa Komisyonu'nun resmi istatistik kurumu olan Eurostat tarafından, AB kamuoylarının belli konulardaki görüşlerini ortaya koyan düzenli *Eurobarometer* anket çalışmasının sonuçlarına göre, Avrupalılar'ın yüzde 90'ı, kişisel verilere ilişkin Avrupa çapında eşit koruma talep etmektedir¹².

Grafik 1 Kişisel verilerin toplandığı ve işlendiği ülke farketmezsiniz 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'na ve AB Konseyi'ne, 1995 tarihli Verilerin Korunması Yönergesi'nin modernize edilmesine ve internet çağına ayak uydurulmasına yönelik bir teklif sunmuştur. Teklifin öne sürdüğü; bütün AB' sınırları içerisinde geçerli tek Verinin Korunması Tüzüğü'nün oluşturulmasıyla birlikte, önemli mali tasarruflar ve kolaylıklar

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.

sağlanması; ihlal hallerinde veri sahibinin anında uyarılması ve veri öznesinin talebi üzerine verinin silinebilmesi gibi önemli adımlar atılması hedefleniyor. Tek Verinin Korunması sistemi ile idari prosedürlerin azaltılması, böylelikle AB dâhilindeki 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 Dolayısı ile 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/özgürlük kısılacında devam eden bu tartışmaların yakın gelecekte kolay bir çözüme ulaşacağı tahmin edilmiyor.

ABAD KARARI: AVRUPALILAR UNUTULMAK İSTİYOR

Kişisel verilerin korunmasına ilişkin her konuda geniş çaplı uzlaşya varılamasa dahi, 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 hallerde mümkün. Ayrıca, verinin paylaşımına sebep olan amaç gerçekleştiğinde, OECD ilkeleri gereği kişisel veri başka bir amaç doğrultusunda kullanılamaz. Öte yandan, kişisel verilerin korunması, kişinin kendisine dair kişisel veriye her şartta ulaşabilmesini ve kendisine ilişkin verinin silinmesini talep edebilmesini de kapsıyor.

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 başvurdu. 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 (Bkz. *Tablo 2*)¹⁵.

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

Tablo 2 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 ulaşılabilen kişisel verilerinin silinmesini talep etme (right to be forgotten) hakkı var mıdır?

Bilginin; hatalı, eksik, ilgisiz ve aşırı olduğu durumlarda, kişilerin arama motorlarından veya diğer veri depolayıcılarından, verilerinin silinmesini talep etme hakkı (right to be forgotten) bulunmaktadır.

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

AB'DEN ÜÇÜNCÜ ÜLKELERE VERİ AKIŞI

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

108 sayılı Sözleşme'nin Ek Protokolü'ne göre verinin üçüncü ülkelere transferi, belli bir verinin; yabancı yargı sistemlerinin yetkisi altındaki kişilere ulaşması anlamına

gelmektedir.¹⁶ Başka bir deyişle, sadece sınır ötesindeki belli bir kişiye yöneltilmiş belirli veriler, sınır ötesi veri akışına uygun kabul edilmektedir. 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 şekillenmektedir. 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 düzenlemeleri öngören kararları da bulunmaktadır. Örneğin, AB ile belirli bir takım üçüncü ülkeler arasında kurulan hava ulaşım hatlarında yolcu isim kayıtlarının karşılıklı paylaşımına yönelik anlaşmalara varılmıştır.¹⁷

KİŞİSEL VERİLERİN KORUNMASI VE TÜRKİYE

Daha önce ifade edildiği üzere, kişisel verilerin korunmasına ilişkin AB müktesebatı, üye ülkelerin iç hukuk mevzuatı el verdiği ölçüde üçüncü ülkelerle karşılıklı veri akışını mümkün kılmaktadır. Bu noktada, Avrupa Konseyi kurucu üyesi sayılan ve AB ile üyelik müzakerelerini sürdüren Türkiye'nin statüsü, 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 ötesinde önem taşımaktadır.

Bugün Türkiye'nin kişisel verilerin korunması doğrultusundaki yolculuğu, ilk bağlayıcı antlaşma olan; 108 sayılı Avrupa Konseyi Sözleşmesi'ni 1988 yılında imzalamasıyla başlamıştır. Sözleşme, taraf devletler arasındaki veri akışını serbest kılmakta ve verinin kontrolünü sağlamaktadır. 1988 yılında imzaladığı bu Sözleşme'yi henüz onaylamamış ve yürürlüğe koymamış olan Türkiye, imzacı Avrupa Konseyi Üye Devletleri arasında Sözleşme'yi onaylamayan tek ülkedir.¹⁸ Türkiye'nin Sözleşme'yi onaylamamasının temel nedeni olarak, Sözleşme'nin 4'üncü maddesi gerekçe gösterilmektedir. Sözleşme'nin ilgili hükmüne göre taraf devletin, en geç Sözleşme'nin yürürlüğe girdiği tarihe kadar ilgili iç hukuk önlemlerini alması gerekmektedir.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.*"

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.

ibaresinin eklenmesiyle hız kazanmıştır.²⁰ Devam eden süreçte, 2013 Demokratikleşme Paketi kapsamında Kişisel Verilerin Korunması Yasa Tasarısı'nın oluşturulması ve kabul edilmesi öngörülmüştür.

Avrupa Komisyonu, 2014 Türkiye İlerleme Raporu'nda ve Vize Serbestliği Yol Haritasına İlişkin Birinci Değerlendirme Raporu'nun Kamu Düzeni ve Güvenlik Bloğu kapsamında, Türkiye'ye kişisel verilerin korunmasına ilişkin bir takım eleştirilerde bulunmuştur. Mesele, Türkiye AB müzakerelerinin 23ve 24'üncü fasılları ve Vize Serbestliği Diyaloğu açısından önemli bir tartışma konusu haline gelmiştir. Her iki raporda da, Kişisel Verilerin Korunması Yasa Tasarısı'nın, AB normlarına uygun bir şekilde yürürlüğü girmesinin ve 108 sayılı Sözleşme'nin imzalanmasının zorunlu olduğu vurgulanmaktadır. Bu zorunluluk doğrultusunda, 23 ve 24'üncü fasıllarda uyum düzeyinin karşılanması ve tam üyeliğin gerçekleştirilmesi için ilgili Yasa Tasarısı'nın, 95/46/EC sayılı Yönerge'yle uyumlu hale getirilmesi gerekmektedir. 95/46/EC sayılı Yönerge'yle uyum kapsamında atılması gereken ilk adım; kişisel verilerin korunmasını denetleyici; bağımsız ve tarafsız bir kurumun tesis edilmesi olmalıdır. Öte yandan Avrupa Komisyonu İlerleme Raporları'na göre, Türkiye ile AB kolluk kuvvetlerinin, sınır kontrol birimlerinin ve istihbarat teşkilatlarının arasında veri paylaşımını, veri transferini sağlayacak altyapı oluşturulmalıdır. Öte yandan bu alandaki reformlar, vize serbestliğinin sağlanması ve Geri Kabul Anlaşması'nın hükümlerinin yerine getirilmesi için de temel zorunluluklar arasında yer almaktadır. Dolayısıyla 1 Aralık 2014 tarihinde açıklanan AB'ye Katılım için Ulusal Eylem Planı'nın II. Aşaması kapsamında kişisel verilerin korunmasına yönelik adımlar yer almaktadır. Eylem Planı'nın koyduğu hedef doğrultusunda, 2016 yılının birinci dönemine kadar, 108 sayılı Sözleşme'nin ve 181 sayılı Ek Protokol'ün onaylanması planlanmaktadır.²¹

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

²⁰ Melih Özsoz 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](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>