Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 25, Sayı 2, Prof. Dr. Ferit Hakan Baykal Armağanı, Aralık 2019, ISSN 2146-0590, ss. 850-872 DOI: 10.33433/maruhad.665460

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması

Transborder Flows of Personal Data: An International Law and EU Law Perspective

Berna AKÇALI GÜR*

Öz

Bilgi iletişim ve veri işleme teknolojilerinde meydana gelen gelişmelere istinaden, kişisel verilerin yurt dışına aktarılmasına ilişkin uluslararası düzenlemelerin yeniden yorumlanmasına, güncellenmesine ve hatta konuya münhasır yeni düzenlemelerin yapılmasına ihtiyaç duyulmuştur. Küresel dijital ekonominin gelişimi açısından kişisel verilerin sınır ötesine aktarılmasının engellenmesi arzu edilmemektedir. Ancak, kişilik hakları ve ulusal güvenliğe etki eden yönleri sebebiyle, kişisel veri aktarımları üzerinde tesis edilen devlet kontrolleri de meşru kabul edilmektedir. Bu iki tezat hedef arasında hassas bir dengenin kurulmaya gayret edildiği bu süreçte, özellikle Birleşmiş Milletler ve bağlı kuruluşları, Avrupa Birliği, Dünya Ticaret Örgütü, Avrupa Konseyi ve Ekonomik İşbirliği ve Kalkınma Örgütü konuyu kendilerinin faaliyet alanlarına uygun açılardan ele alan çalışmalar yapmaktadırlar. İletişim teknolojilerinin ve dijital ekonominin uluslararası karakteri göz önüne alındığında devletlerin kişisel verilerin korunmasına ilişkin olarak tesis edeceği düzenin etkili olabilmesi için bu gelişmeler çerçevesinde ele alınması gerekmektedir.

Anahtar Kelimeler: Uluslararası Hukuk, AB Hukuku, Kişisel Verilerin Korunması, Kişisel veriler, kişisel verilerin yurt dışına aktarılması

Abstract

The developments in information communication and information processing technologies have not only led to revision and re-interpretation of existing international instruments relevant to the cross-border transfer of personal data but also necessitated new ones specifically targeting this area. The obstruction of trans-border flows of personal data may have an adverse effect on the growth of digital economy. On the other hand, state based controls are justified mainly due to its impact on individual rights and national security. In this current phase of pursuing a balance between the two conflicting goals, the United Nations and its agencies, European Union, World Trade Organization, Council of Europe and the Organization for Economic Co-operation and Development have all been involved. In order for any state law in this area to be effective it shall be structured by taking the relevant

* Dr. Öğr. Üyesi, Kadir Has Üniversitesi, Milletlerarası Hukuk Anabilim Dalı Öğretim Görevlisi, E-Mail: berna.gur@khas.edu.tr

Makale Gönderim Tarihi: 14.11.2018
Yayına Kabul Tarihi: 28.12.2018

international law instruments and negotiations in consideration given the international character of the communication technologies and the digital economy.

Keywords: International Law, EU Law, Protection of Personal Data, Personal Data, transborder flows of personal data

GİRİŞ

1990lı yıllardan bu yana bilgi iletişim ve veri işleme teknolojilerinde meydana gelen gelişmeler ve özellikle iletişim ağlarının yüksek hız ve kapasiteye ulaşması sonucu kişisel veriye dayalı ekonominin küresel ticari faaliyetlerde payı hızla arttı. Bu ekonomik hareketlilikten pay almayı arzu eden devletler, olumsuz buldukları etkilerini de yönetmek istemektedirler. Olumsuz etkiler arasında kişisel verilerin sınır ötesine kontrolsüz aktarılması ön plana çıkmıştır. Devletler konuya özellikle kişilik hakları ve ulusal güvenliğe ilişkin yönleri sebebi ile hassasiyet göstermekte ve denetim mekanizmaları tesis etmektedirler. Karakteri itibariyle uluslararası nitelik taşıyan veri ekonomisine ilişkin bu düzenlemeler ancak mevcut uluslararası taahhütler ve hali hazırda bu konuda devam eden küresel ve bölgesel müzakereler çerçevesinde şekillendirilirse etkili olabilecektir.

Uluslararası hukukun bu alana ilişkin çok çeşitli kaynakları bulunmaktadır. Birleşmiş Milletler (BM) ve bağlı kurumları, Dünya Ticaret Örgütü (DTÖ), Avrupa Konseyi (AK) gibi Türkiye'nin de üye bulunduğu uluslararası ve bölgesel örgütler mevcut uluslararası düzenlemeleri yeni gelişmeler ışığında tekrar yorumlamak, model kanunlar oluşturmak, kişisel verilerin korunması konusuna has ikili ve çok taraflı sözleşmeler hazırlamak gibi çeşitli girişimlerde bulunmuşlardır. Türkiye'nin üyelik müzakerelerinin devam ettiği Avrupa Birliği (AB)'de de konuya ilk zamanlardan başlayarak hassasiyetle eğilmiş ve kapsamlı düzenlemeler yapılmıştır. Türkiye ile yakın ilişkileri sebebi ile bu düzenlemeler de bu inceleme kapsamında değerlendirilmiştir. Düzenlemelerin ilk örnekleri, özel hayatın gizliliği ve kişilerin kendi verilerine ilişkin haklarını korumak odaklıdır. Daha sonra hazırlanan düzenlemelerde ise kişisel verilerin stratejik ve özellikle ekonomik değeri de ön plana çıkmaktadır. Son dönemde ise, öncelikleri göz önüne alındığında çoğunlukla birbirine tezat duran bu iki hedef hassas bir dengede ele alınmaya çalışılmaktadır.[1]

Bu makalede öncelikle uluslararası hukuk boyutuyla kişisel verilerin korunması konusu tarihsel gelişimi içerisinde ortaya konulacaktır. İkinci bölümde konu AB hukuku kapsamında değerlendirilmektedir. Daha sonra konu, mevcut gelişmeler ışığında uluslararası hukukun kaynakları ile ilişkili olarak incelenecektir.[2] Son bölümde Türkiye'de yeni gelişmeye başlayan

1 Verilerin Korunması ve Özel Hayatın Gizliliği Uluslararası Konferansı'nın, 14-16 Eylül 2005 tarihinde gerçekleşen 27. toplantısında Montrö Beyannamesi benimsenmiştir. Konferans üyeleri, mevcut haliyle, 76 farklı ülkenin kişisel verileri koruma alanında yetkili kurumlarıdır. Bu beyannmenin 10. maddesi bahse konu dengenin kurulmasının önemine ilişkindir. Beyanname metni için bakınız: Montreux Declaration (2005) – 'The protection of personal data and privacy in a globalized world: a universal right respecting diversities', Declaration of the 27th International Conference of Privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005.

2 Uluslararası hukukun iç hukuka etkisi yönünden bakınız: Olgun Akbulut, "Güncel Tartışmalar Işığında İnsan Hakları Sözleşmelerinin Türkiye Anayasal Sisteminde Normlar Hiyerarşisindeki Yeri", **Bahçeşehir Üniversitesi**

bu alanda, devletin mevcut uluslararası taahhütlerinin ve yeni gelişmelerin önem ve etkisine dikkat çekmek hedeflenmektedir. Burada özellikle uluslararası düzenlemelerde farklı ülkelerin düzenlemeleri arasında birlikte işlerliği (interoperability) sağlamanın[3] gerek ekonomik hedeflere yönelik gerekse kişilik haklarının etkin korunabilmesi ve ulusal güvenliğe ilişkin risklerin yönetilebilmesine ilişkin önemine işaret edilecektir.

I. ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİ KORUMA OLGUSUNUN TARİHSEL GELİŞİMİ[4]

Uluslararası hukukta kişisel veri hem korunması gerekli şahsi bir hakkın konusu hem de ekonomik bir değer olarak ele alınmıştır. Bu çerçevede uluslararası hukuki düzenlemeleri iki ayrı grupta düşünebiliriz. Birinci grup düzenleme temel bir hak olarak özel hayatın gizliliğine ilişkin maddeleri içeren uluslararası antlaşmalardır. Bu maddeler ilerleyen yıllarda kişisel bilgilerin korunması hakkını da kapsadığı şeklinde yorumlanmıştır. Diğerleri ise bilgi ve iletişim teknolojilerinin neden olduğu hızlı dönüşümün neden olduğu kişisel verilerin korunması konusuna has zorluklara cevap vermektedir. Bu düzenlemeler teknolojik gelişmelere ve ticari faaliyetlere engel oluşturmamak anlayışıyla kaleme alınmıştır.

Ancak, devletler, veri koruma standartları arasında ülkesel farklılıkları ve ulusal güvenliğe ilişkin riskleri öne sürerek korumacı yaklaşımlarında ısrarcı olabilmektedirler. Bu halde ulusal düzenlemeler arasındaki farklılaşmanın derinleşmesi ve uluslararası standartlar üzerinde çok taraflı bir uzlaşma sağlayarak ulusal düzenlemeler arasında birlikte işlerliğin sağlanamaması riski doğmaktadır. BM, küresel iletişim ağı internete erişimi hem küresel kalkınmaya ilişkin, hem de temel hak ve özgürlüklerin etkin kullanılmasına olanak sağlayan önemli bir hak olarak kabul etmiştir. [5] Bu hakkin kısıtlanmasının olumsuz etkileri yapılan çalışmalarda anlatılmıştır.[6]

Hukuk Fakültesi Dergisi, S: 9/115-116, Mart-Nisan 2014, sf: 7-45.
Işıl Özkan, "Uluslararası Hukuk – Özel Hukuk İlişkileri", **Yaşar Üniversitesi Elektronik Dergisi,** sf:8 (Prof. Dr. Aydın Zevkliler'e Armağan), 2014, sf. 2127 (Çevrimiçi) https://journal.yasar.edu.tr/wp-content/uploads/2014/01/1-I%C5%9F%C4%B1l-%C3%96ZKAN.pdf (Erişim Tarihi: 25 Kasım 2017).

3 Christopher Kuner, *Transborder Data Flow and Data Privacy Law*, Oxford, Oxford University Publishing, 2013, sf. 175-180.

4 Kişisel verilerin korunmasına münhasır mevzuatların ilk olarak İkinci Dünya Savaşı sonrasında Avrupa'da hazırlandığı bilinmektedir. Bu yıllarda kişisel verilerin korunması kişilik haklarına ilişkin bir iç hukuk meselesi olarak değerlendirilmektedir. 1990´larda İnternet kullanımının yaygınlaşması ve veri işleme teknolojilerindeki diğer gelişmeler sonucu, son dönemde uluslararası boyutu önem kazanan bir alandır. Bu konuda daha detaylı bilgi için bakınız: G. Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Switzerland, Springer International Publishing, sf. 65.
J. Lee Riccardi, "The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?", **Boston College International & Comparative Law Review**, S:6/1, 1983, sf. 243-272.

5 BM İnsan Hakları Komisyonu, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27, 16 May 2011.

6 BM İnsan Hakları Komisyonu, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/32/13, 18 Temmuz 2016.
ITU, *Achieving Universal and Affordable Internet in the Least Developed Countries: ICTs, LDCs and the SDGs, ICT and Telecommunications in Least Developed Countries*, 2018. (Çevrimiçi) http://handle.itu.int/11.1002/pub/810be2fb-en

Bu bağlamda, birlikte işlerliğin sağlanamaması ve diğer korumacı yaklaşımlar, devletlerin tesis edecekleri ağır kontrol mekanizmaları, interneti üzerinde ülkesel ya da bölgesel sınırlar tesis edilmiş parçalı bir hale (internet fragmentation) dönüştürebilecektir. Bu BM'in mevcut yaklaşımına göre arzu edilmeyen bir durumdur.[7]

BM tarafından 1976 tarihinde kişisel verilerin korunmasına ilişkin standartları belirlemek amacı ile 45/95 sayılı Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri hazırlanmıştır. Bu belgenin yayımlanması ise ancak 14 Aralık 1990 tarihinde gerçekleşmiştir. Bu metin, hazırlanması ve yayımlanması arasındaki süre içerisinde yayımlanan iki diğer düzenlemeye temel oluşturmuştur. Bunlar, Ekonomik İşbirliği ve Kalkınma Teşkilatı'nın (OECD) 1980 senesinde yayınladığı Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkelere ve AK üyeleri tarafından 1981 senesinde imzalanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Sözleşme)'dir. BM, son olarak, Uluslararası Hukuk Komisyonu (ILC) uzun dönemli çalışma programına "Sınır ötesi transferlerde kişisel verilerin korunması" başlığı ile bu konuyu dâhil etmiştir.[8]

Yayımlanmış ilk uluslararası belge olarak OECD tarafından hazırlanan rehber ilkelerin dikkat çekici bir yönü, yurt dışına aktarım konusuna özel olarak değinilmiş olmasıdır. OECD'nin konulara öncelikle ekonomik açıdan baktığı kabul edildiğinde, kişisel verilerin yurt dışına aktarılmasının uluslararası ekonomik bir değer olarak potansiyelinin ortaya çıkmış olduğu anlaşılacaktır. Rehber ilkelerin eklenmiş bulunduğu OECD Konseyi Tavsiye Kararı'nda kişisel verilerin sınır ötesine aktarılmasının sosyal ve ekonomik gelişmeye olumlu katkıları olacağı ve kişilerin özel hayatlarının gizliliğine ilişkin ulusal düzenlemelerin bu sınır ötesi akışları aksatabileceği ifade edilmiştir.[9]

Nitekim 3. Bölüm 16. maddede, OECD'ye üye ülkelerin arasında yapılacak aktarımlarda ve yine ülkesel yetki alanından geçiş yapılarak gerçekleşecek veri hareketlerinde kısıtlama yapılmaması öngörülmektedir. 17. maddede kısıtlamanın ancak aktarma yapılacak OECD üyesi ülkenin rehber ilkelere itaat etmiyor olması, aktarılan verinin özel düzenlemeye tabii belli bir sınıf veri olması ve aktarma yapılacak ülkede denk bir korumanın bulunmaması ya da üçüncü bir ülkeye yapılacak aktarmanın devletin ülkesel mevzuatından kaçınmak sonucunu doğurabileceği hallerde getirilmesi kabul edilmiştir.[10] 18. maddede kişisel özgürlükler ve özel hayatın korunmasına ilişkin düzenlemelerin sınır ötesi aktarmalara kısıtlama getirebileceği göz önüne alınarak uygulamanın orantılılık esasına göre yapılması gerektiğine dikkat çekilmiştir. 5. Bölümde ise kişisel verilere ilişkin konularda uluslararası işbirliğinin önemi vurgulanmıştır.

(Erişim Tarihi: 18 Ocak Kasım 2019).

7 William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter, *Internet Fragmentation: An Overview (White Paper),* Davos, World Economic Forum, Ocak 2016.

8 Bu konu Bölüm 4.'te daha detaylı ele alınmaktadır.

9 OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Preface, 23 September 1980.

10 Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler 4. maddesinde ulusal bağımsızlık, ulusal güvenlik, toplum düzeni gibi istisnalar ayrıca tanınmıştır.

Bu belge tavsiye niteliğindedir ve bağlayıcı özelliği bulunmamaktadır. Buna karşın, kişisel verilerin korunması konusunda yayınlanmış ve çok uluslu bir organizasyonda kabul edilen ilk belge olması nedeniyle Kişisel Verilerin Korunması hukuku alanında önemlidir. Pek çok ulusal düzenleme bu rehbere uygun olarak kaleme alınmıştır.[11] Etki alanı itibarıyla konuya ilişkin uluslararası hukuk kaynakları arasında, esnek hukuk kuralları kategorisinde etkili bir örnek teşkil etmektedir.[12] Kişisel verilerin sınır ötesine aktarılması konusu daha az detaylı olmakla beraber, bir başka esnek hukuk kuralı olarak 45/95 sayılı Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler'de benzer şekilde ele alınmıştır. Kişisel verilerin ve bilginin serbest aktarılması esas alınmış, kısıtlamalarda orantılılık esası aranmıştır.

Kişisel verilerin ve bilginin sınır ötesi aktarılmasının serbest bırakılması esası bu iki düzenlemenin hazırlanma dönemlerinin belirleyici politikalarının bir yansımasıdır. Bu dönemde bilgi ve iletişim teknolojilerinin gelişmesine engel oluşturabilecek her türlü yasal düzenlemeye mesafeli durulmuştur. İletişimi sınırlandıracak her türlü ulusal düzenleme gerek teknolojik ve ekonomik gelişmelere gerekse fikir ve ifade özgürlüğüne olumsuz etki edeceği fikri ağır basmaktadır. Genel olarak bilgi, bilim ve ekonomik özgürlüklerin karşısında bir duruş olarak algılanabilmektedir.[13]

Uluslararası hukukun kaynakları arasında bölgesel düzenlemeler incelendiğinde, AK'nin bünyesinde 1981 senesinde imzalanmış olan 108 sayılı Sözleşme ön plana çıkmaktadır. AK tarafından hazırlandığı için çoğunlukla AK üyesi ülkelerin taraf olduğu bu sözleşme, üye olmayan ülkelerin de imzasına açıktır. 2013'ten bu yana, Konsey üyesi olmayan altı ülke bu sözleşmeyi onaylamıştır.[14] Bu açıdan değerlendirildiğinde kişisel verilerin korunması konusunda özel olarak hazırlanmış ve bağlayıcı olduğu kabul edilen ilk ve hala tek uluslararası belge olması nedeniyle büyük bir önem taşımaktadır. AK da yaygınlaştırılması için büyük çaba harcamaktadır.

Esasında, 108 sayılı Sözleşme metni ilk imzaya açıldığı dönem için dahi yenilikçi hükümler içeren bir metin olarak kabul edilmemektedir. AK bünyesinde alınan kararlardan ve AK üyesi ülkelerin mevzuatlarında bulunan hükümlerden faydalanılarak hazırlanmıştır.[15] O dönemde büyük ticari işletmeler ve devlet kurumları bu gelişmeler sayesinde çok büyük veri bankaları kurulmuştur. Verimlilik ve üretkenlik açısından çok büyük avantajlar sağlansa da; kişilerin özel hayatının gizliliğinin ihlal edilebileceğine dair endişeler doğmuştur. AK'da da 1960'larda

11 Fred H. Cate, Peter Cullen, Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century*, Mart 2014, Oxford Internet Institute: Oxford University (Çevrimiçi) https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (Erişim Tarihi: 15 Mart 2018)

12 OECD Rehber İlkeleri 2013 senesinde güncellenmiştir. OECD faaliyetleri hakkında daha detaylı bilgi için bakınız: OECD, "OECD Privacy Guidelines", 2013 (Çevrimiçi) http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm, (Erişim Tarihi: 15 Mart 2018).

13 Stuart S. Malawer, "Global Governance of E-commerce and Internet Trade: Recent Developments", **Virginia Lawyer**, S:14, June/July 2001, sf. 14-19.

14 Bu makalenin yazıldığı tarih itibarı ile bu devletler Meksika, Uruguay, Senegal, Tunus, Yeşil Burun Adaları ve Mauritius'tur. Arjantin ve Fas başvuru sürecini tamamlamıştır. Japonya ve Güney Kore de gözlemci olarak katılmıştır.

15 L. Andrew Bygrave, *Data Privacy Law An International Perspective, An International Perspective,* New York: Oxford University Press, 2014, sf: 36.

verileri elektronik işlemeye imkân veren bilgi teknolojilerin gelişmesine cevaben bir dizi kararlar çıkarılmıştır. Kararların amacı üye ülkelerin iç mevzuatlarının gelişmesine ön ayak olarak bu endişeleri gidermektir. Sonradan, kararların yeterli olmadığı, bağlayıcı bir sözleşmenin daha verimli olacağı düşünülmüştür. 108 sayılı Sözleşme bu gelişmeler sonucunda kaleme alınmıştır. [16]

İlerleyen yıllarda iletişim teknolojilerindeki yeni gelişmeler, veri ekonomisi temelli iş modellerinin yaygınlaşması, verinin sınırlar ötesine rahatça aktarılıp, farklı ülkelerin yetki alanına giren bölgelerde muhafaza edilebilmesi ve işlenebilmesi 108 sayılı Sözleşmeye ek bir protokol hazırlanmasına sebebiyet vermiştir.[17]

108 sayılı Sözleşme'nin temel iki hedefi kişisel verilerin toplanması ve işlenmesi hallerinde oluşabilecek hak ihlallerine karşı gerçek kişileri korumak ve sözleşmeye taraf ülkeler arasındaki kişisel verilerin aktarılmasını düzenlemektir. Bu çerçevede, gerçek kişilere ilişkin, ırk, cinsel tercih, sabıka kaydı gibi hassas verilerin uygun önlemler alınmadan toplanmasını ve işlenmesini yasaklamaktadır.[18] Burada yer alan bir başka önemli hak ise ilgili kişilerin kendileri hakkında toplanan verileri öğrenebilmesi ve eksik ya da yanlış ise düzeltme yapabilmesine ilişkindir.[19] Bu hali ile OECD ve BM'in hazırlamış olduğu rehber ilkelere benzer şekilde asgari şartları düzenlemektedir.

2001 yılında, AK, 108 sayılı Sözleşme'ye ek 181 sayılı Protokolü (Ek Protokol) imzaya açmıştır. Bu protokolle iki hedef yerine getirilmiştir. Öncelikle taraf ülkelere kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici makam kurmaları şartı getirilmiştir.[20] Buna göre, kontrol makamları araştırma ve müdahale etme yetkisine sahip olacaklar ve aynı zamanda hukuki süreçte aktif rol alabileceklerdir. Yine bu tip kurumlarda alışılageldiği üzere ilgili kişilerin yaptıkları şikâyetleri inceleme yetkisine sahip olmaları beklenmektedir. İkincisi ise 108 sayılı Sözleşme'de taraf olmayan ülkelere yapılacak kişisel veri aktarılmasına ilişkin hüküm bulunmazken bu protokolün 2. maddesi ile söz konusu eksiklik giderilmiştir. Buna göre taraf ülkeler taraf olamayan ülkelere kişisel veri aktarılmasına ancak ilgili devletin ya da organizasyonun denk bir koruma sağlayacağına emin olduktan sonra izin verebileceklerdir. [21]

2018 senesinde, yedi yıl süren, 108 sayılı Sözleşme'yi modernleştirme çalışmaları tamamlanmıştır. Yeni metin 223 sayılı Protokol ile 18 Mayıs 2018 tarihinde kabul edilmiştir.[22] Değişiklikler

16 Avrupa Konseyi, "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg", 28 Ocak 1981.
Avrupa Konseyi, "Background", www.coe.int *(Çevrimiçi)* https://www.coe.int/en/web/dataprotection/convention108/background *(*Erişim Tarihi: Ocak 2018)

17 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol (Ek Protokol).

18 108 sayılı Sözleşme, 6. madde

19 108 sayılı Sözleşme, 8. madde

20 181 sayılı Protokol, 1. madde

21 181 sayılı Protokol, 2(b) madde

22 25 Haziran 2018 tarihinde tarafların imzasına açılmıştır. Bu makalenin yazım tarihi itibarı ile 25 ülke imzalamıştır. Konu ile ilgili bilgi ve dökümanlar için bakınız: Avrupa Konseyi, "223 sayılı Sözleşmenin Detayları", (Çevrimiçi)

yapılırken, sözleşmenin temel prensiplere odaklı ve teknoloji-nötr karakteri korunmuştur. Diğer taraftan öngörülen koruma standartları yükseltilmiş ve sözleşmenin kapsamı genişletilmiştir.[23] Bu şekilde AB'nin kişisel verileri koruma mevzuatında meydana gelen değişiklikler ile paralellik sağlanmıştır.[24] Bir başka önemli gelişme de sözleşmeye uygunluğun denetlenmesine ilişkin yapıyı güçlendirilmesidir.[25] Sözleşme Komitesi'nin yetkileri genişletilmiş ve başka yetkilerin yanında, ulusal mevzuatlarda tanımlanan koruma standartlarının yeterliliğini Sözleşme hükümleri kapsamında değerlendirme hakkı tanınmıştır. Taraf devletlerin uygulamalarının sözleşme hükümlerine uygun olup olmadığının daha etkin bir şekilde denetlenebilmesinin sözleşmenin uluslararası itibarının arttıracağı öngörülmektedir. Son olarak, Avrupa Birliği'ne ve uluslararası organizasyonlara sözleşmeye taraf olma hakkı tanınmıştır.[26] Türkiye henüz yeni metni onaylamamıştır.

A. ULUSLARARASI HUKUK'TA ÖZEL HAYATIN GİZLİLİĞİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI İLE İLİŞKİSİ

Kişisel Verilerin Korunması konusunun ortaya çıkmasından evvel hazırlanmış olan temel hak ve hürriyetlere ilişkin uluslararası antlaşmalarda özel hayatın gizliliğine ilişkin maddeler bulunmaktadır. Bu maddelerin "kişisel verilerin korunması" konusunu da kapsaması gerektiği kabul görmektedir. Bu bağlamda özel hayatın korunmasına ilişkin uluslararası belgelere bu makale konusu kapsamında değinmek konunun bütünlüğü açısından önem arz etmektedir.[27]

BM İnsan Hakları Evrensel Bildirisi'nde, özel hayatın gizliliğine ilişkin 12. maddenin bu hakkı kapsadığı kabul edilmiştir.[28] Madde içeriği şu şeklidedir:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 (Erişim Tarihi: 16 Ocak 2019)

23 Avrupa Komisyonu, *Proposal for a Council Decision authorizing Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, COM (2018) 451 final, 5 Haziran 2018.

24 Greenleaf, Graham, "*Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives*", **Privacy Laws & Business International Report**, S:142, 3 Ağustos 2016, sf. 14-17.

25 Konu ile ilgili bilgi ve dökümanlar için bakınız: Avrupa Konseyi, "Modernisation of the Data Protection Convention 108", (Çevrimiçi) https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true (Erişim Tarihi: 10 Mart 2018)

26 223 sayılı Protokol, 27(173) madde.

27 Bu iki kavramın karşılaştırmalı incelemesi derin ve karmaşık bir konudur. Bu makalede konu, kısaca iki kavramın arasında kesişen alanlar ve farklar olduğunu belirtmek ve bu bağlamda özel hayatın gizliliğine ilişkin ulularası düzenlemelerin de dikkate alınması gerektiğini belirtmek hedefi ile ele alınmıştır. Bu konuda daha ayrıntılı bir değerlendirme için bakınız.: Juliane Kokott, Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", **International Data Privacy Law,** S:3/4, 1 Kasım 2013, sf. 222–228.
Orla Lynskey, *The Foundations of EU Data Protection Law,* sf. 131-173.

28 Christopher Kuner, "International Organizations and the EU General Data Protection Regulation", University of Cambridge Faculty of Law Research Paper Series, S:20/2018, Şubat 2018, sf:4.

> "Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır."

Yine Türkiye'nin taraf olduğu ve bağlayıcılığı olan Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin mahremiyet hakkına ilişkin 17. maddesinin de bu hakkı kapsadığı kabul edilmektedir. Bu sözleşmede, devlete özel hayatın gizliliğine saygı göstermek, keyfi ya da hukuka aykırı şekilde bu hakkı ihlal etmemek gibi olumsuz yükümlülükler getirildiği gibi ve bu hakkı korumak için önlemler almak gibi olumlu yükümlülükler de getirilmiştir.[29]

Avrupa İnsan Hakları Mahkemesi de (AİHM) kişisel bilgilerin işlenmesi ve muhafaza edilmesine ilişkin uyuşmazlıkları, Avrupa İnsan Hakları Beyannamesi'nin özel hayatın gizliliğine ilişkin 8. madde kapsamında değerlendirmiştir. Dolayısıyla bu konuda içtihat oluşmuştur.[30] Mevzu bahis kararlar hiç şüphesiz ki yerel mahkemelerin kararları üzerinde etkili olmaktadır. Bu bağlamda devletlerin bu temel hakkı ihlal edecek tasarruflarda bulunmaması öngörülmüştür. Aynı zamanda devletlerin bu korumayı sağlamakta pozitif bir yükümlülüğü olduğu da kabul edilmiştir. Kısacası AİHM, Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin yorumuyla benzer bir yaklaşım sergilenmiştir.

Özel hayatın gizliliği hakkı ile kişisel verilerin korunması hakkının örtüşmeyen kısımları da bulunmaktadır.[31] Kişisel veri, veri sahibinin özel hayatına ilişkin olmak zorunda değildir. Bu sebeple korunmaya tabii kişisel veri, bireyin özel hayatına ilişkin olmasa dahi ilgili her türlü bilgiyi kapsar. Buna karşın özel hayatın gizliliği kişinin özel, aile ve ev hayatına, fiziksel ve ahlaki bütünlüğüne, onuruna ve şöhretine, kendisi hakkında yanıltıcı bir imajın oluşmasını engellemeye, ilgisiz ve utandırıcı gerçeklerin açıklanmamasına, özel fotoğrafların izinsiz yayınlanmamasına ve gizli kalacağına güvenilerek verilen veya alınan bilginin açıklanmasının engellenmesine ilişkin olabilmektedir.[32] Bu farklılıklar sebebi ile kişisel verilerin korunması ayrı bir hak olarak düzenlenmektedir.

II. AB HUKUKU'NDA KİŞİSEL VERİLERİN KORUNMASI

Avrupa Komisyonu, AB üyelerinin ulusal mevzuatlarının öngördüğü kişisel verileri koruma standartları arasındaki farklılıkların AB iç pazarında kişisel veri aktarılmasının önünde bir engel teşkil ettiğini fark etmiştir. Bu sebeple, 1990 senesinde bu mevzuatların uyumlu hale getirilmesinin önemine işaret etmiş ve bu konuda bir direktif hazırlanmasını teklif etmiştir. Direktifin

29 BM İnsan Hakları Komitesi, *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*", CCPR General Comment No:16, 8 Nisan 1988.

30 AİHM, "*Fact Sheet-Personal Data Protection*", September 2018.

31 L. Andrew Bygrave, *Data Privacy Law, An International Perspective*, sf:82-98.
Orla Lynskey, *The Foundations of EU Data Protection Law,* sf: 173.

32 AK Parlamenterler Meclisi, *Declaration on Mass Communication Media and Human Rights*, Resolution No: 428, 1970, Paragraf C.

hazırlanıp kabul edilmesi beş yıl sürmüş ve nihayet 24 Aralık 1995'te Kişisel verilerin işlenmesi ve serbest dolaşımına ilişkin olarak kişilerin korunmasına ilişkin 95/46/EC sayılı Direktif (AB KVK Direktifi) kabul edilmiştir. Bu direktif de zamanla ihtiyaçlara cevap veremez hale gelmiştir. Bilgi iletişim teknolojilerinin sunduğu yenilikler ve kişisel verilerin giderek genişleyen bu küresel ağın merkezine oturması konunun tekrar ele alınmasını gerektirmiştir. Nitekim hazırlanan Genel Veri Koruma Tüzüğü (GDPR) 2016'da kabul edilmiş ve 25 Mayıs 2018'de yürürlüğe girmiştir. Bu bölümde her iki düzenlemeye de sınır ötesi veri aktarılması açısından değinilmektedir.

Diğer bir önemli gelişme de, aynı süre zarfında kişisel verilen korunmasının anayasal bir hak olarak tanınmasıdır. AB Temel Haklar Şartı'nın 8. maddesinde yer alan bu hak, 2009'da Lizbon Antlaşması'nın yürürlüğe girmesiyle anayasal bir hak statüsüne kavuşmuştur. Ayrıca AB'nin İşleyişine İlişkin Antlaşma'nın 16. maddesi de AB Parlamentosu'na ve AB Konseyi'ne kişisel verilerin işlenmesine ilişkin kuralların belirlenmesine ilişkin bir yükümlülük getirmiştir. Kişisel Verilerin Korunmasının özel hayatın korunmasından ayrı bir anayasal bir hak olarak tanınması AB'ne özgü bir yaklaşım olarak ortaya çıkmıştır. AB uyum sürecinde bulunan Türkiye'de de bu yaklaşım benimsenerek kişisel verilerin korunması ayrı bir anayasal hak olarak yer almıştır.[33]

AB iç pazarının işleyişinin malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımı temeline dayanmaktadır. AB KVK Direktifi, bu "dört özgürlüğün" sağlanabilmesi için verilerin de serbestçe akabilmesi fakat aynı anda kişilerin temel haklarının da korunması gerektiği anlayışı üzerine kaleme alınmıştır.[34] Bu iki hedef ancak AB üyelerinin mevzuatlarının uyumlu hale getirilmesi ile sağlanabilecektir. Bu uyumun sağlanabilmesi için de AB düzeyinde bir düzenlemeye ihtiyaç duyulduğu özellikle belirtilmiştir. AB Hukukunda direktifler doğrudan iç mevzuatın yerini almamaktadır. Üye ülkeler mevzuatlarını uyumlu hale getirmektedirler. Üyeler arasında mevzuat farklılıkları sadece direktif ile düzenlenmeyen hususlarda ya da direktif ile farklılıkların tanındığı alanlarda olabilmektedir. AB KVK Direktifi de aynı şekilde, temel hususları düzenleyerek üye devletlere farklılaşma alanı bırakmıştır. AB üyelerinin hali hazırda 108 sayılı Sözleşme'ye taraf olduğu da direktif metninde göz ardı edilmemiş, direktifin bu sözleşme ile sağlanan korumayı güçlendireceği ve arttıracağı belirtilmiştir.[35]

AB KVK Direktifinde, AB sınırları dışına aktarılacak verilerin durumu IV. Bölüm'de düzenlenmiştir. Burada kişisel verilerin ancak "uygunluk denetimini" geçmiş ülkelere aktarılmasına izin verileceği belirtilmiştir. Dolayısı ile ulusal düzenlemeleri ve/veya uluslararası taahhütleri göz önüne alındığında yeterli korumanın sağlanacağına Avrupa Komisyonu tarafından karar verilmiş olma şartı aranmaktadır. Kural bu olmakla beraber, uygunluk denetiminin yaygınlaşmasının zorluğu, kişisel tercihler ve ekonomik hayatın gerekleri göz önünde bulundurularak istisnalar da getirilmesi gerekli görülmüştür.

Bu istisnalar çerçevesinde; yeterli korumanın bulunmaması durumunda dahi,

33 TC Anayasası, 20(3) madde

34 AB KVK Direktifi, Giriş Bölümü, 3. paragraf

35 AB KVK Direktifi, Giriş Bölümü, 11. paragraf

i. ilgili kişinin açık rızası olması,

ii. veri aktarılmasının ilgili olduğu kişinin taraf olduğu bir sözleşmenin ifası ya da bir sözleşmeden kaynaklanan sair yükümlülüklerini yerine getirmesi için gerekli olması,

iii. aktarılmanın yapılmasında toplumsal fayda ya da kanuni mecburiyet bulunması,

iv. kanuni hakların ispat edilmesi korunması, savunması için gerekli ya da mecburi olması,

v. ilgili kişinin menfaatlerinin korunması için gerekli olması

gibi durumlarda üçüncü ülkelere veri aktarılması uygun görülmektedir.[36] Yine aynı maddenin 2. ve 4. paragrafına göre veri sorumlusunun sözleşme ile kişilerin özel hayatının korunması ve ilgili temel hak ve hürriyetlerinin korunacağını taahhüt etmesi halinde AB üyeleri bu veri sorumlularına veri aktarılmasına izin verebileceklerdir. Burada kastedilen kimi uluslararası şirketlerin merkezinin olduğu ülkenin yeterli koruma sağladığına dair bir uygunluk kararı olmasa dahi kişisel verileri koruma standartlarına ilişkin taahhüdün kurumun kendisi tarafından yapılabileceğidir. Bu iki şekilde olabilmektedir: Bağlayıcı şirket kuralları ya da model sözleşmeler.[37] Bu şekilde onaylanan veri aktarılmasından AB üyeleri, Avrupa Komisyonu'nu ve diğer AB üyelerini haberdar etmek zorundadırlar.

Bu gibi yöntemlere ek olarak ikili uluslararası antlaşmalar da kullanım alanı bulmuştur. Örneğin ABD Ticaret Bakanlığı AB ve İsviçre makamlarına danışarak AB Adalet Divanı'nın 2015 senesinde iptal etmiş olduğu Güvenli Liman Özel Hayatın Gizliliği Çerçeve Prensipleri[38] ve onun yerini alan Özel Hayatın Gizliğine İlişkin Çerçeve Prensiplerini hazırlamıştır. Avrupa Komisyonu tarafından uygunluk denetimi onayı verilen her iki belge, bu çerçeve prensipleri onaylayan ABD merkezli şirketlere AB'den yapılacak aktarmalara izin verilmesi hedefiyle hazırlanmıştır.

Katılımı tamamen şirketlerin kendi takdirine bırakılmış olan bu program kapsamına ABD Federal Ticaret Komisyonu'nun veya Ulaştırma Bakanlığı'nın yetki alanına giren ticari işletmeler dâhil olabilmektedir. Başvuran şirketlere, bağlı bulundukları bakanlıklar tarafından uygun görülmesi halinde sertifika verilmektedir. Bu şirketler bu şekilde, ABD devletleri kanunlarından doğan yükümlülükleri saklı kalmak kaydıyla belgede yer alan prensiplere uygun faaliyet göstereceklerini taahhüt etmektedirler. Böylece ABD'nin kişisel verilerin korunması hukukuna yaklaşımının AB'den çok farklı olmasına rağmen ABD merkezli Facebook, Microsoft, Google gibi küresel faaliyetleri bulunan şirketlerin AB'deki faaliyetlerine devam edebilmeleri ve AB'den toplayacakları verilere AB'ne denk bir koruma sağlamaları sağlanması hedeflenmiştir.

36 AB KVK Direktifi 26(1)(a) madde.

37 Bağlayıcı şirket kuralları ile çok uluslu şirketlerin yetkili organları tarafından alınan ve bu grup şirketlerinin tüm çalışan ve yöneticiler için bağlayıcı nitelik taşıyan kurallar kastedilmektedir. Bu şekilde benimsenen kişisel verileri koruma standartlar AB tarafından onaylanmak sureti ile sınır ötesi ancak şirket içi veri aktarılması mevzuata uygun şekilde gerçekleşebilmektedir. Bu uygulamanın dayanağı AB KVK Direktifi'nin 26(2) maddesidir. Yine aynı maddeye göre standart sözleşme maddeleri kullanmak sureti ile uygunluk denetimini geçmemiş ülkelere veri tarnsferi yapmak mümkün olabilmektedir. Bu iki uygulama GDPR'da 46(2)b ve 46(2)c maddelerinde düzenlenmiştir.

38 Bu taahhütnamenin 26 Temmuz 2000 tarihli 520 nolu Avrupa Komisonu Uygunluk Denetimine ilişkin rapor metni için bkz: Official Journal of the European Communities, 25 Ağustos 2000.

İlk belgenin iptali ve ikincisinin hazırlanması basit bir mevzuat yeniliği sebebiyle ortaya çıkmamıştır. Bu değişiklik kişisel verilerin sınır ötesine aktarılmasına ilişkin en çok ses getiren dava kabul edilebilecek *Schrems Davası* sonucunda gerçekleşmiştir.[39] 6 Ekim 2015 tarihli kararında AB Adalet Divanı ABD devlet kurumlarının elektronik iletişimlere genel erişim hakkına ilişkin mevzuatın güvenli liman taahhüdüne göre üstün olması, ABD devlet kurumlarının AB'den elde edilen verilere de istisnai ve belirli hallerde değil, genel bir hak olarak erişebileceği sonucunu doğurmaktadır. Bu özel hayatın korunması hakkının en temelden riske atılması olarak değerlendirmiştir.[40]

AB Komisyonu tarafından uygunluk onayı verilen ve ABD tarafından hazırlanan ikinci belge bu mahkeme kararının sonucunda kaleme alınmıştır. Buna göre şirketlerin taahhütlerinin kapsamı genişletilmiş ve ABD Ticaret Bakanlığı ve Federal Ticaret Komisyonu'nun inceleme ve yaptırım gücü arttırılmıştır. AB üyelerinin kişisel verileri koruma kurumları ile işbirliği arttırılmıştır. En önemlisi belirlenmiş şartlar, sınırlar ve denetim olmadan ABD devlet kurumlarının kişisel verilere genel erişimi olamayacağı taahhüt edilmiştir. Yine AB'den gelecek soru ve şikâyetleri ile ilgilenecek bir yetkili atanması da yenilikler kapsamındadır.[41] Bu uygunluk onayının da ABAD tarafından iptal edilmesi riskine karşı pek çok şirketin AB'de veri merkezlerine yatırım yaptığı da bilinmektedir.[42]

1995 senesinden beri geçerli olan AB KVK Direktifi 25 Mayıs 2018 tarihinde yürürlükten kalkmış ve yerini GDPR almıştır. GDPR, mevcut uluslarüstü (supranational) ve uluslararası belgelere bakıldığında kişisel verilere ilişkin hazırlanmış en kapsamlı mevzuattır. Kişisel verilerle ilgili işlem yapan tüm kamu kurumlarına ve özel kuruluşlara ağır sorumluluklar getirmektedir. Bu sebeple GDPR hükümlerine uyum sağlayabilmeleri için AB üyelerine 2 yıl geçiş süresi tanınmıştır.

GDPR'ın hazırlanmasında iki temel hedef üzerinde durulmuştur. Birincisi, ilgili kişilerin veri koruma haklarının geliştirilmesi, ikincisi ise kamu kurumlarının ve ticari işletmelerin faaliyetleri kapsamında gerçekleştirilen veri aktarımını, AB üyeleri arasındaki mevzuat farklılıklarını ortadan kaldırarak kolaylaştırmaktır.[43] Bu kapsamda sadece AB üyeleri arasındaki kişisel veri akışı değil, AB sınırları ötesine yapılacak veri aktarılmasının da bağlı olduğu şartlar düzenlenmektedir.

AB sınırları dışına ve uluslararası organizasyonlara aktarılacak verilere ilişkin hükümler temelde tüzüğün 5. bölümünde ele alınmıştır. Bu bölümde, veri aktarılmasına ilişkin olarak Direktif ile getirilen genel kısıtlamalara büyük değişiklik yapılmamıştır.[44] Ancak uygunluk denetimi sürecine

39 Graham Greenleaf, "International data privacy agreements after the GDPR and Schrems", **Privacy Laws & Business International Report,** S:139, 30 Ocak 2016, sf. 12-15.

40 *Schrems v Data Protection Commissioner (Facebook)* (C-362/14).

41 Avrupa Komisyonu, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, Press Release, 2 Şubat 2016.

42 Amir Misroch**,** "U.S. Tech Firms Look to Data Centers on European Soil", **The Wall Street Journal**, 6 Ekim 2015.

43 Avrupa Birliği Konseyi, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Preparation of a general approach*, S: 9565/15, 11 Haziran 2015.

44 GDPR 44. madde

ve veri aktarımlarının yapılmasına ilişkin alternatif yöntemlere ilişkin yenilikler ve değişiklikler göze çarpmaktadır. 45. maddede uygunluk denetiminde aranacak şartlar daha geniş detaylı olarak tanımlanmıştır.[45] Yine uygunluk denetiminin her 4 senede bir tekrarlanacağı ve şartların değişmesi halinde uygunluk kararının iptal edilebileceği eklenmiştir.

İki mevzuat arasındaki önemli farklardan birisi, Direktif'te yer almamasına karşın uygulamada yaygın olarak kullanılan koruma tedbiri 'bağlayıcı şirket kuralları'nın GDPR ile tanınması ve detaylı olarak düzenlenmesidir.[46] Bunun yanı sıra, model sözleşme hükümleri GDPR'da da koruma tedbiri olarak kalmış, ancak ayrıca denetleme kurumu tarafından onay alınması şartı kaldırılmıştır. GDPR'da amaca yönelik sözleşmeler de Direktifte olduğu gibi koruyucu tedbir olarak tanınmış ancak bu yöntemin bağımsız denetleyici ve düzenleyici kurumların "uyum mekanizması"[47] sürecinden geçmesi şartı getirilmiştir.[48]

GDPR'da kişisel verileri koruma kurumlarının oluşturacakları sözleşme hükümlerinin de sınır ötesi veri aktarımına temel olabileceği kabul edilmiştir. Diğer yeni yöntemler arasında iş etiği kuralları[49], sertifikasyon[50], idari düzenlemeler[51] ve üçüncü ülke yargı organlarının kararları[52] bulunmaktadır Bu farklı koruyucu tedbir alternatiflerinin düzenlenmesi ile, uygulamada dikkate değer bir rahatlama sağlayacağı düşünülmektedir. Nitekim direktifte yer alan istisnalar da GDPR'da daha detaylı tanımlanmak suretiyle tanınmış, aynı zamanda veri sorumlusunun

45 GDPR ile insan haklarına ve temel hak ve hürrüyetlere ilişkin korumanın bulunması, kamu otoritelerinin aktarılmış veriye erişimine ilişkin şartlar, bağımsız denetleyici ve düzenleyici bir kurumun varlığı ve faaliyetlerinin etkili olması, uluslararası taahhütler ve diğer uluslararası yükümlülükler uygunluk denetiminde aranacak şartlar arasına girmiştir.

46 GDPR 47. madde

47 GDPR ile AB üyesi ülkelerin kişisel verilerin korunması ile görevli bağımsız denetleyici ve düzenleyici kurumları arasında işbirliği mecburiyeti getirilmiştir. Bu çerçevede birden fazla ülkeyi ilgilendiren meselelerde de Avrupa Veri Koruma Kuruluna danışılabilecektir. Bu uygulamanın amacı AB'de faaliyet gösteren organizasyonların uyması gereken kurallar arasında tutarlılığın sağlanmasıdır. Tutarlılığın sağlanmasına ilişkin hükümler GDPR 7. Bölüm, 2. Kısımda ele alınmıştır.

48 AB KVK Direktifi, Giriş Bölümü, 3. Paragraf

49 GDPR üçüncü ülkelere yapılacak veri aktarımlarında koruyucu tedbir olarak iş etiği kullarını da tanımıştır. İş etiği kuralları bir AB üyesi ülkenin bağımsız denetleyici ve düzenleyici kurumu tarafından onaylanmış işletmelerin daha sonra bu kurallara dayanarak yapacakları kişisel veri aktarımları için ayrıca izin almaları gerekmemektedir. İş Etiği kuralları GDPR 4. bölüm, 5. kısımda, iş etiği kurallarının üçüncü ülkelere yapılacak veri aktarımları ile ilgili atıf ise 46(2)(e) madde'de düzenlenmiştir.

50 GDPR 46(2)(f) maddesinde ise sertifikasyon prosedürü ile üçüncü ülkelere veri aktarımı yapılabileceği konusu düzenlenmiştir. Burada sertifikasyon ile beraber veriyi ithal edecek veri sorumlusunun ve işleyenin de kişinin haklarını koruyan, bağlayıcı ve yaptırımı olan taahütlerinin bulunması şartı aranmaktadır. Sertifikasyona ilişkin hükümler de GDPR 4. Bölüm, 5. Kısımda yer almaktadır.

51 GDPR 46(3)(b) maddesine göre kamu kurumları arasında uzlaşma sağlanan idari düzenlemeler de, eğer ilgili kişilerin hakları için yeterli koruma sağlıyorsa veri aktarımı için kabul edilen yöntemlerden biri olabilecektir. Bu düzenlemelere dayanarak yapılcak veri aktarımları bağımsız denetleyici ve düzenleyici kurumların onayı sonrası gerçekleşebilecektir.

52 Üçüncü ülke mahkemelerinin ya da idari makamlarının kararları eğer veri aktarımını gerektiriyorsa, bu ancak aktarımın uygun bir uluslararası sözleşme çerçevesinde yapılması halinde hukuka uygun kabul edilecektir. Bu kapsamda bir sözleşmenin bulunmaması halinde diğer koruma tedbirleri çerçevesinde aktarım yapılabilecektir. Bu konu GDPR 48. maddede düzenlenmiştir.

zorlayıcı meşru menfaatleri[53] de bu istisnalara eklenmiştir.[54]

GDPR'da AB dışına aktarılacak belli kategorilerdeki verilerin toplumsal menfaatlere ilişkin nedenler üye ülkeler tarafından kısıtlanabileceğini 49. maddenin 5. fıkrası ile düzenlenmiştir. Bu uygulamanın birlik içindeki uyumu tehdit edebileceği ve ticari hayat üzerinde olumsuz etki yaratabileceğine dikkat çekilmiştir. Ancak genel olarak GDPR'ın AB'nin iç pazarına ve AB'nin dış ilişkilerine nasıl yansıyacağını daha katiyetle değerlendirmek uygulamada örneklerin ortaya çıkması ile mümkün olacaktır.

A. AB ve AK İŞ BİRLİĞİ

AB ve AK kişisel verileri koruma hukukunun gelişiminde gerek uluslararası örgütlere gerekse Avrupa bölgesi dışındaki ülkelere öncü örnek teşkil etmektedir.[55] Bilgi ve iletişim teknolojilerinde öncü kabul edilebilecek ABD'de konu bir bütün olarak düzenlenmemiştir.[56] Özel hayatın gizliliği hakkının anayasal bir hak olduğuna ilişkin Yüksek Mahkeme kararına[57] karşın, bu kararın sağladığı kapsam, incelediğimiz mevzuatlara mukayese ile çok sınırlı kalmaktadır. Kişisel verilerin korunmasına ilişkin sağlık, finans, sigorta gibi sektörlere has federal düzenlemeler bulunmaktadır. Buna ek olarak eyaletler arasında da yaklaşım farklılıkları bulunmaktadır. Bu parçalı ve karmaşık yapı sonucunda, uygulanacak mevzuat, ilgili işlemin ilişkili olduğu sektöre ve işlemlerin bağlantılı olduğu eyaletlere göre farklılık göstermektedir.[58] Her ne kadar sektörlere has farklı uygulamalar AB'de de bulunsa da mevzuat genel olarak bütünlük arz etmektedir. Bağımsız denetleyici ve düzenleyici kurumlarının varlığı güven sağlamaktadır. Dolayısıyla uluslararası hukuk belgelerinin benzer yapısını dikkate aldığımızda yeni mevzuat hazırlayan ülkelerde Avrupa bölgesinin yaklaşımının daha çok tercih edilmesi[59] şaşırtıcı değildir.

53 GDPR 49. maddede, üçüncü ülkelere yapılacak veri aktarımları için diğer hukuki zeminlerin uygulanamaması halinde, aktarımın tekrarlanmadığı, sınırlı sayıda ilgili kişiyi kapsadığı ve veri sorumlusunun zorlayıcı meşru menfaatlerinin bulunduğu durumlar için bir istisna tanımıştır. Burada veri sorumlusunun menfaatinin ilgili kişisinin menfaatlerine göre ağır basmaması ve veri sorumlusunun koruyucu tedbirler uygulamış olması şartı da bulunmaktadır. Veri sorumlusunun, durumdan gerek bağımsız denetletleyici ve düzenleyici kurumu gerekse ilgili kişileri haberdar etme yükümlülüğü bulunmaktadır.

54 Direktif'in 26(1)(a) maddesinde yer alan ilgili kişinin onayı şartı GDPR 49(1)(a) maddesinde açık onay olarak değiştirilmiştir.

55 Graham Greenleaf, "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108", **International Data Privacy Law**, S:2/2, 1 Mayıs 2012, sf: 68–92.
L. Andrew Bygrave, Data Privacy Law, An International Perspective, sf:208.
A.L. Newman, *Protectors of Privacy: Regulating Data in the Global Economy,* New York: Cornell University Press, 2008.

56 Robert Gellman, Pam Dixon, "Failures of Privacy Self-Regulation in the United States", in Wright D., De Hert P. (eds) *Enforcing Privacy*, Switzerland: Springer International Publishing, 2016, sf: 53-77.

57 *Griswold v. Connecticut*, 381 U.S. 479 (1965)

58 Graham Greenleaf, "Data protection in a Globalized World" in *Research Hanbook on the Governance of the Internet*, Ed. by Ian Brown, Cheltenham, UK: Edward Elgar Publishing Limited, 2013, sf:228, 229.

59 Graham Greenleaf, "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108", **International Data Privacy Law,** S:2:2, 2012, sf. 68–92.

108 sayılı Sözleşme'ye taraf olmak da hali hazırda AB Uygunluk Denetiminde etkili bir faktör olarak göz önüne alınmaktadır. GDPR'da bu durum özellikle belirtilmiştir. Uygunluk denetiminin şartlarını düzenleyen GDPR 45(2)c maddesinde de verinin aktarılacağı üçüncü ülkenin koruma standartlarının uygunluğunun tespit edilmesinde, özellikle kişisel verilerin korunmasına ilişkin uluslararası taahhütleri ve yükümlülüklerine dikkat edileceği belirtilmiştir. AB'nin 108 sayılı Sözleşme'ye verdiği önem AB ile kişisel veri paylaşımında bulunmak isteyen diğer ülkelere bu Sözleşme'ye taraf olmak için önemli bir inisiyatif teşkil etmektedir. Sözleşmenin GDPR'a mukayeseli olarak daha az detaylı ve genel hükümler içeren yapısını koruması kişisel verilerin korunması hukukuna Avrupa modelinin küresel yayılma hedeflerini gerçekleştirebilmesi açısından önemlidir.

III. ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI: GÜNCEL GELİŞMELER

BM Uluslararası Hukuk Komisyonu (ILC) 'bilginin sınır ötesi aktarılmasında kişisel verinin korunması' konusunu uzun vadeli çalışma programına dâhil etmiştir.[60] Bilindiği üzere ILC'nin hedefi uluslararası hukuk boyutunda henüz düzenleme yapılmamış alanları antlaşma taslakları hazırlamak suretiyle geliştirilmesi ve yazılı kurallara dönüştürülmesidir. Dolayısı ile ILC tarafından kişisel verilerin korunması alanında bir uluslararası antlaşma hazırlanması ihtimali bulunmaktadır. Hatta kişisel verilerin korunması konusunun ulusal sınırları aşan bir olguya dönüştüğü göz önünde bulundurularak, BM bünyesinde kurulacak bir organizasyon tarafından yönetilmesi konusu akademik çevrelerde tartışılmaktadır.[61]

2015 yılında BM bünyesinde toplanan dünya liderleri 2030 yılına yönelik sürdürülebilir kalkınma için 17 adet küresel hedef belirlemiştir. Bu hedeflere ulaşılabilmesi için bilgi iletişim teknolojilerinin sunduğu imkânlardan en iyi şekilde faydalanılması gerektiği, bu amaçla ileri dönük politikaların belirlenmesinin önemine de işaret edilmiştir.[62][63] BM Ticaret ve Kalkınma Örgütü (UNCTAD) bugünün dijital ekonomisinde kişisel verilerin akışının ana kaynak konumuna geldiğini, güvenlik ve bu verilerin gizliliği ve ulusal mevzuatların uyumsuzluğu gibi konuların çözülmemesi halinde bu ticari aktivitelerin olumsuz etkileneceğine işaret etmiştir. Bu amaçla kişisel verilerin korunması ve yurt dışına veri akışına ilişkin düzenlemeler ve bu düzenlemelerin ticaret ve kalkınmaya etkilerini inceleyen çok kapsamlı bir çalışma hazırlamıştır. Bunun yanı sıra üye ülkelere ve bölgesel organizasyonlara mevzuat aralarında kişisel verilerin korunması

60 BM Uluslararası Hukuk Komisyonu, *Programme of Work,* 2017.

61 Paul de Hert, Vagelis Papakonstantinou, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?", **Journal of Law and Policy for the Information Society,** S: 9/3, Yaz 2013, sf. 271-324.

62 BM Genel Kurulu, *Transforming our world: the 2030 Agenda for Sustainable Development* A/RES/70/1, 25 Eylül 2015.

63 UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, Switzerland: UN Publications, 2016, sf. Preface, iii.

ve özel hayatın gizliliği konusunun da yer aldığı[64] elektronik ticaret ile ilgili hususlarda destek sağlamaktadır.

Meselelere daha çok ticaret ve kalkınma perspektifinden bakan UNCTAD'ın yanı sıra BM bünyesinde bir başka kurum olan Uluslararası Telekomünikasyon Birliği (ITU) de konuya daha geniş bir perspektiften yaklaşmaktadır. Bu kurum öncülüğünde ve BM Genel Sekreterliğinin himayesinde iki aşamalı Dünya Bilgi Toplumu Zirvesi (WSIS) düzenlenmiştir. Zirve üye devlet temsilcileri, uluslararası kuruluşlar, BM kuruluşları, BM ihtisas kuruluşları, sivil toplum örgütleri ve konu ile ilgili özel şirketlerin katılımıyla gerçekleşmiştir. Bilgi iletişim teknolojilerinin yönetimi konusu çok geniş bir yelpazede ele alınmıştır.

2003 yılında Cenevre'de gerçekleşen ilk zirvede[65] her ne kadar internet yönetiminin geleceği hakkında kararlar alınamamışsa da Cenevre İlkeleri Beyannamesi[66] benimsenmiştir. Bu beyannamede geleceğin Bilgi Toplumunun temelini oluşturacak ilkeler belirlenmiştir. Bu belgenin 35. maddesinde bilgi iletişim teknolojilerine erişim ve ticaret için kullanılmasını geliştirirken güvenliğinin, kişisel verilerin korunmasının ve özel hayatın gizliliğinin sağlanması gerektiği belirtilmiştir.

2005 yılında Tunus'ta gerçekleşen 2. Zirvede Tunus Taahhütnamesi ve Tunus Takvimi benimsenmiş, aralarında kişisel verilerin korunması ve sınır ötesine akışı konularının da bulunduğu tüm internetle ilgili konuları tartışmak ve raporlar hazırlamak üzere her sene toplanması öngörülen Internet Yönetimi Forumu (IGF) kurulmuştur. Bu foruma internet kullanımına ilişkin menfaat sahibi her grubun katılabilmesi öngörülmüştür. Tunus'ta benimsenen belgelerde kişisel verileri ve özel hayatın gizliliği konularına verilen önem tekrar edilmiş, bu konularda sadece uluslararası işbirliği değil tüm menfaat sahiplerinin işbirliğinin önemli olduğu vurgulanmıştır.[67] Bu toplantıda alınan kararlara bağlı olarak, UNCTAD bünyesinde 2016-2018 senelerinde çalışarak İnternet ve kamu politikaları ile ilgili konularda bir rapor hazırlamak üzere bir çalışma grubu oluşturmuştur.

BM İnsan Hakları Yüksek Komiserliği (OHCHR) bünyesinde hazırlanan "Dijital Çağda Özel Hayatın Gizliliği Hakkı" başlıklı rapor 2018 yılı Ağustos ayında BM Genel Kurulu'na sunulmuştur.[68] Rapor özel hayatın korunması konusunu kişisel verilerin korunması ile bütünlük içinde ele almaktadır. Raporun amacı konuya ilişkin temel ilkeleri, standartları ve en iyi uygulamaları belirlemektedir. İçerik sadece devletlerin değil, özel işletmelerin de konuya ilişkin sorumluluklarını da kapsamaktadır. Bu raporu takiben, BM Genel Kurulu'nda son gelişmeleri de değerlendirme kapsamına alan bir karar alınmıştır.[69] Kararda, pek çok diğer hususun yanı

64 Cecile Barayre, "Data Protection Regulations and International Data Flows: Implications for Trade and Development" [Power Point Sunum] MIKTA Workshop on Electronic Commerce, WTO Headquarters, Geneva, 5 Temmuz 2016.

65 BM, *Geneva Plan of Action*, WSIS-03/GENEVA/DOC/0005, 10-12 December 2003.

66 BM, *Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/0004-E, 10-12 December 2003.

67 BM, *Tunis Commitment*, WSIS-05/TUNIS/DOC/7, 16-18 Kasım 2005, Tunus, m. 39 ve 46.

68 OHCHR, *The Right to Privacy in the Digital Age,* A/HRC/39/29, 3 Ağustos 2018.

69 BM Genel Kurulu, *The Right to Privacy in the Digital Age,* A/C.3/73/L.49/Rev.1, 14 Kasım 2018.

sıra, konuya ilişkin uluslararası düzenlemelere işaret edilmiş ve devletlerin ulusal mevzuatlarının bu düzenlemelere uyumlu olmasının önemi hatırlatılmıştır. Kısacası BM ve bağlı kurumları İnternetle ilgili politikaların oluşturulmasında aktif rol almaya gayret etmektedir. Mevcut çalışmalara bakıldığında kişisel verilerin korunması konusuna hem kişilik hakları boyutu hem de kalkınmanın itici gücü olan ticari boyutuyla bakmaktadır.

DTÖ kuruluş amacına uygun olarak İnternet'in özellikle elektronik ticaret boyutuyla ilgili meselelerinde konuya müdahil olmuştur. İnternet kullanılarak gerçekleştirilen mal ve/veya hizmet ticaretinin DTÖ kurucu antlaşmaları çerçevesinde nasıl değerlendirilmesi gerektiğine dair incelemeler yapmaya karar vermiştir.[70] Son zamanlarda e-ticaretle ilgili konularda bağlayıcı kararlar alınması da gündeme gelmiştir.[71] DTÖ Uyuşmazlık Mahkemesinin e-ticaret ile ilgili içtihatları[72] bulunmaktadır. Ancak kişisel verilerin yurt dışına aktarılmasına ilişin bir kararı bulunmamaktadır. Son dönemde, DTÖ'nün özel hayatın gizliliği, kişisel verilerin korunması gibi konuları uluslararası ticari faaliyetleri kısıtlayıcı bir engel gibi gördüğü ve üye ülkelere bu görüşü yönünde baskı yaptığı kanaati oluşmuştur. DTÖ kendi internet sitesinde bu iddiaların asılsız olduğunu, üye ülkelere baskı yapma yetkisi olmadığını belirtmiştir. Ayrıca DTÖ kurucu antlaşmalarından Hizmet Ticareti Genel Antlaşması'nın (GATS) XIV maddesinde devletlerin, kişilerin kişisel verilerinin işlenmesi ve paylaşılması ve kişisel kayıt ve hesapların gizliliğinin korunması ile ilgili olarak özel hayatın gizliliğinin korunmasına ilişkin tedbirler alabileceğini hakkının tanındığını belirtmiştir.[73] [74]

DTÖ örneğinde de görüldüğü üzere uluslararası antlaşmalarda yer alan, devletlerin ülkesel yetkileri ve uluslararası taahhütleri arasındaki dengenin gözetilmesinde büyük önem taşıyan toplumsal ahlaka, ulusal güvenliğe vs. ilişkin istisnaların yorumlanmasında uluslararası örgütler ve mahkemeler önemli rol oynayacaktır. Bahse konu istisnalara kişisel verilerin korunmasının dâhil kabul edilmesi gerektiği hâlihazırda hâkim görünen görüştür. Gerek uluslararası örgütler gerekse uluslararası mahkemeler genel istisnalar çerçevesinde ileri sürülen itirazların meşru bir zemine dayanıp dayanmadığını değerlendirebilecek tecrübeye sahiptir. İçtihatlar arttıkça uluslararası mahkemelerin rolünü daha sağlıklı değerlendirmek mümkün olacaktır.

70 DTÖ, *Work programme on electronic commerce,* 25 Eylül 1998, WT/L/274.

71 DTÖ, *Programme of Side Events, 11. DTÖ Bakanlar Konferansı*, 10-13 Aralık 2017.

72 DTÖ Temyiz Organı'nın *US-Gambling* ve *China-Audiovisuals* kararları örnek olarak verilebilir. 1. Appellate Body Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/AB/R, adopted 20 April 2005, DSR 2005: XII, p. 5663.
2. Appellate Body Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, WT/DS363/AB/R, 19 Ocak 2010, sf.3.

73 DTÖ, *WTO and Internet Privacy,* (Çevrimiçi) https://www.WTO.org/english/tratop_e/serv_e/ gats_factfiction10_e.htm (Erişim Tarihi: 10 Ocak 2018)

74 Maria Veronica, Perez Asinari**,** "Is There Any Room for Privacy and Data Protection within the WTO Rules", **Electronic Communication Law Review**, S:9, 2002, sf. 249.

IV. TÜRKİYE'DE KİŞİSEL VERİLER HUKUKUNUN GELİŞİMİ

Türkiye, 2016 Nisan tarihinde Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVK) ile ilk kez kişisel verilerin korunmasına özel hazırlanmış bir mevzuat ile tanıştı. Aynı kanunun 11. maddesinde Kişisel Verileri Koruma Kurumunun (KVKK) kurulmasına karar verildi. Kurul 17 Ocak 2017'de yemin ederek görevine başladı.

AB'ndeki gelişmelerle mukayese edildiğinde KVK'nın çok yeni olması, onu uygulamakla görevli kurumun yakın bir tarihte görevine başlamış olması kişisel verilere ilişkin olarak daha evvel bir koruma sağlanamamış olduğu izlenimi yaratabilir. Bu noktada Anayasa'da[75], Ceza Kanunu'nda[76],Borçlar Kanunu'nda, sağlık, elektronik haberleşme, bankacılıkla ilgili yönetmeliklerde konuya ilişkin hükümlerin bulunduğunu belirtmek gerekir.

2010 yılında 5982 sayılı Kanun'la yapılan Anayasa değişikliği ile Anayasa'nın 20. maddesine eklenen ilave fıkra fıkra şu şekilde kaleme alınmıştır:

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

Türkiye'ye göre daha etkin koruma sağladığı kabul edilen pek çok ülkede kişisel verilerin korunması Anayasal bir hak olarak görülse de ayrıca ve özel olarak düzenlenmiş bir hak değildir. Daha çok özel hayatın korunması, ifade özgürlüğü gibi diğer anayasal haklar ile bağdaştırılmak suretiyle anayasal bir hak olarak yorumlanmaktadır.[77]

Bu yasal düzenlemeler ve uygulamalar küresel bir mukayese içerisinde değerlendirildiğinde, Türkiye'nin, en az korumanın sağlandığı ülkelere göre daha iyi konumda, limitli korumanın sağlandığı ülkeler arasında yer aldığı görülecektir.[78] Genel olarak, mevzuatları liberal demokrasilere öncü örnek teşkil eden AB'nin ve üyesi ülkelerin ve ABD'nin uyguladığı koruma standartları Türkiye'ye göre daha yüksek değerlendirilmektedir.[79] Uluslararası ortak standartların varlığı ve bunların daha çok ülke tarafından benimsenmesi, kişisel verilerin yurt dışına aktarılmasının kaçınılmaz olduğu bu dönemde çok önem kazanmıştır.

75 Elif Küzeci, "Anayasal Bir Hak: Kişisel Verilerin Korunması", **Bilişim Dergisi**, S: 38/128, Şubat 2011, sf. 142-149.

76 Rezzan İtişgen, "*Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı olarak Verme veya Ele Geçirme Suçu*", **Türkiye Adalet Akademisi Dergisi**, S:6/23, Ekim 2015, sf.178-202.

77 Fruzsina Molnar-Gabor, "Data Protection*", Max Planck Encyclopedia of Comparative Constitutional Law*, Oxford: Oxford University Press, Eylül 2016, (Çevrimiçi) http://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e95?prd=MPECCOL (Erişim Tarihi: 18 Ocak 2019).

78 DLA Piper, Data Protection Laws of the World, (Çevrimiçi) https://www.dlapiperdataprotection.com (Erişim Tarihi: Ocak 2018)

79 A.e.

A. KVK'NIN ULUSLARARASI KAYNAKLARI

KVK da Türkiye'nin uluslararası antlaşmalardan doğan taahhüt ve yükümlülükleri gözetilerek hazırlanmıştır. Türkiye'nin, kişisel verilerin korunmasına ilişkin etkin hukuki düzenlemelerin hayata geçirilmesi ve bağımsız denetleyici ve düzenleyici bir kurumun kurulması taahhüdü hem AK bünyesinde hazırlanan 108 sayılı Sözleşme'ye Ek Protokol'de, hem de AB müktesebatına uyum programının bir şartı olarak da yer almaktadır. Bu bağlamda o dönemde yürürlükte olan AB Direktifine uygun düzenlemeler yapılması öngörülmektedir. 2005'de başlayan üyelik müzakerelerine bağlı olarak sunulan program kapsamında Bilgi Toplumu ve Medya başlığı altında da bu taahhütler yer almaktadır. 2015'te Avrupa Komisyonu'nun yayınladığı raporda kişisel verilerin korunmasına ilişkin düzenlemelerin yapılmamasının yarattığı problemlere işaret edilip, düzenlemelerin geciktirilmemesi tavsiye edilmiştir.[80] Bu bağlamda Türkiye'deki gelişmeleri her iki taahhüt kapsamında incelemek yerinde olacaktır.

Türkiye, AK bünyesinde hazırlanan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Sözleşme'ye ilk imza atan ülkeler arasında yer almıştır. Ancak taahhüt edilmiş olan özel kanun tam 35 yıl sonra 2016'da yürürlüğe girmiştir. 108 sayılı Sözleşme de, aynı sene, bu kanunun yayımlanmasından hemen önce 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazetede yayınlanarak iç hukuka dâhil etmiştir.[81] Öncesinde, Türkiye haricinde bu sözleşmeyi imzalamış olmasına rağmen, onay işlemlerini tamamlamayıp yürürlüğe koymayan başkaca ülke bulunmamaktaydı. 108 sayılı Sözleşme ve Ek Protokol temel hak ve özgürlüklere ilişkin uluslararası bir antlaşmadır. Anayasa 90. madde kapsamında değerlendirildiğinde, ulusal mevzuat ile aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda bu antlaşmanın hükümleri esas alınacaktır.[82]

Bu halde KVK'nun, 108 sayılı Sözleşme ve AB KVK Direktifi model alınarak hazırlanması bir tesadüf değildir. Bu haliyle AB mevzuatına uyum sağlanmış, 108 sayılı Sözleşme ve Ek Protokolü taahhütlerine de uygun bir adım atılmıştır. Ancak KVK'ya temel oluşturan AB KVK Direktifi 25 Mayıs 2018 tarihi itibariyle yerini GDPR'a bırakmaktadır. Dolayısı ile uyum süreci ve AB ile yakın ticari ilişkiler de dikkate alınırsa, ikincil mevzuatın GDPR dikkate alınarak kaleme alınacağı düşünülmektedir.

Mevcut hali ile Türkiye'deki yasal çerçeve ve uygulama AB Uygunluk Denetimini geçmek için yeterli değildir. Bunun sebepleri Avrupa Komisyonu'nun 2018 tarihli Türkiye Raporu'nda raporunda açıklanmıştır. Kişisel verileri koruma mevzuatına ilişkin en önemli sebep KVK Kurumu'nun denetleme görevini yerine getirirken tamamen bağımsız hareket edeceğine dair güvence verilememesi ve kişisel verileri koruma hakkının ifade özgürlüğü ve bilgi edinme hakkı

80 Avrupa Komisyonu 2015 tarihli Türkiye Raporu'nda bu eksikliğin giderilmesini talep etmiştir. Bakınız: Avrupa Komisyonu, *Commission Staff Working Document Turkey 2015 Report*, SWD(2015) 216 final, 10 Kasım 2015.

81 Ek Protokol de 5 Mayıs 2016 tarihinde yayımlanarak iç hukuka dâhil edilmiştir.

82 Anayasa 90. maddenin yorum ve uygulamasına ilişkin olarak: Olgun Akbulut, "Güncel Tartışmalar Işığında İnsan Hakları Sözleşmelerinin Türkiye Anayasal Sisteminde Normlar Hiyerarşisindeki Yeri", **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, S: 9/115-116 , Mart-Nisan 2014, sf: 7-45.

ile dengelenememiş olmasıdır.[83] Buna ek olarak kolluk kuvvetlerinin ve yargı organlarının faaliyetlerinin kişisel verileri korumaya ilişkin yasalar tarafından tam kapsanmıyor olması da belirtilmiştir.[84] Mevzuatın uyumlu hale getirilmemiş olması ticari, idari ve güvenliğe ilişkin güven veri paylaşımının sağlanmasına engel oluşturmaktadır. Nitekim AB Polis Teşkilatı (EUROPOL)[85] ve AB Adli İşbirliği Teşkilatı (EUROJUST) [86] ile kişisel veri paylaşımına dayanan uluslararası antlaşmalara ilişkin müzakereler mevzuattaki yetersizlikler sebebi ile açılamamaktadır.

Türkiye'nin AB uygunluk denetimini geçecek standartlara ulaşmayı hedeflediği kabul edilirse, kolluk kuvvetleri ve yargı organlarının faaliyetlerinin de kişisel verileri koruma yasalarına tabi olmasını ve KVK Kurumu'nun denetleme görevini yerine getirirken tam bağımsız bir şekilde hareket etmesini sağlaması gerekmektedir. Kurumun tam bağımsızlıkla hareket eden bir kurum olması şartı 181 sayılı Ek Protokol'ün 3. maddesinde de yer almaktadır. Bu bağlamda uluslararası antlaşmadan kaynaklanan bir taahhüttün bulunduğu göz önünde bulundurmak gerekmektedir. Bu şartlar ilgili kişiyi merkezine alan gerek idari makamlara, gerek yargı mercilerine, gerekse özel kuruluşlara karşı ilgili kişilerin temel hak ve hürriyetlerine öncelik veren etkili bir denetim sistemi kurulmasıyla ilişkilidir.

B. KİŞİSEL VERİLERİN TÜRKİYE'DEN YURT DIŞINA AKTARILMASI

KVK Kanunu'na göre kişisel verinin aktarılacağı ülke ile Türkiye arasında uluslararası bir antlaşma bulunması ya da ilgili kişinin açık rızası olması hallerinde kişisel veriler yurt dışına aktarılabilmektedir. Bu iki şartın da bulunmaması halinde kişisel verilerin işlenmesine ilişkin şartların ek tedbirleri ile beraber uygulanmadığı farklı bir uygunluk denetimi devreye girmektedir. Bun göre kişisel verinin işlenmesine ilişkin KVK Kanunu'nun 5(2)[87] ve 6(3)[88] maddelerinde

83 Avrupa Komisyonu, *Commission Staff Working Document Turkey 2018 Report*, SWD 366 final, 17 Nisan 2018.

84 Avrupa Komisyonu, *Commission Staff Working Document Turkey 2016 Report*, SWD 366 final, 9 Kasım 2016.

85 EUROPOL AB'nin suçlara ilişkin istihbarat faaliyetlerini yürüten kurumudur. Bakınız: About EUROPOL, (Çevrimiçi) https://www.europol.europa.eu/about-europol (Erişim Tarihi: 18 Ocak 2019)

86 EUROJUST AB'nin sınırötesi suçlar ve organize suçlarla mücadelede adli organlar arasında işbirliğini sağlamakla görevli kurumudur. Bakınız: EUROJUST, *EUROJUST Core Business,* (Çevrimiçi) http://www.eurojust.europa.eu/about/background/Pages/eurojust-core-business.aspx (Erişim Tarihi 20 Mart 2017)

87 KVK Kanunu 5(2) madde metni şu şekilde kaleme alınmıştır: "(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:
a) Kanunlarda açıkça öngörülmesi.
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel
verilerin işlenmesinin gerekli olması.
ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

88 KVK Kanunu 6. maddesi şu şekilde kaleme alınmıştır: "(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı,

belirtilen şartların yerine gelmesi halinde, yurt dışına aktarılmanın uygun olup olmadığı, KVK Kanunu 9. maddede KVK Kurulu'nun (Kurul) yeterli korumanın bulunduğunu kabul ettiği ülkeler ve diğerleri için ayrı ayrı düzenlenmiştir.

Kurul yeterli korumanın bulunduğunu değerlendirdiği ülkeleri açıkça ilan edecektir. Değerlendirmesine, yani bir ülkenin kişisel veri aktarımı açısından güvenli olup olmadığına madde 9(4) çerçevesinde karar verir. Buna göre; Türkiye'nin taraf olduğu uluslararası antlaşmaları, aktarımın yapılacağı ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, her somut aktarımda kişisel verinin niteliği ile işlenme amaç ve süresini, kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını ve kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri dikkate alacaktır. Aynı maddede Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabileceği de belirtilmiştir. Bu onay mekanizmasının tek istisnası olarak Türkiye'nin taraf olduğu uluslararası antlaşmaların kapsamına giren durumlar belirtilmiştir.[89]

Kurul tarafından yeterli korumanın bulunduğuna karar verilememiş, yani oluşturulacak güvenli ülke listesinde bulunmayan ülkelere yapılacak kişisel veri aktarımları da kanunun 9(2)b maddesinde düzenlenmiştir. Bu maddede Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumanın sağlanacağını yazılı olarak taahhüt etmeleri ve kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına verilerinin aktarılabileceği düzenlenmiştir.[90]

Bahsedildiği üzere bu alan GDPR 2. Bölüm'de detaylı olarak düzenlenmiştir. AB ile yakın ilişkiler göz önüne alındığında Kurul'un ikincil mevzuatının GDPR'da yer alan hükümlere paralel olarak hazırlanması ihtimali yüksektir. Ekonomik sebeplerin yanısıra EUROPOL ve EUROJUST ile yapılacak işbirliği antlaşmalarında ve AB Vize Muafiyeti Yol Haritası'nda[91] kişisel verileri koruma mevzuatının AB standartlarına uygun seviyede olması beklenmektedir. [92]

ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.
(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.
(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.
(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

89 Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Yurt Dışına Aktarılması" (Çevrimiçi) http://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20AKTARILMASI.pdf (Erişim Tarihi: 17 Ocak 2018)

90 İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında bir Değerlendirme", **Türkiye Barolar Birliği Dergisi,** S:124, 2016, sf. 81-152.

91 AB Komisyonu, *Turkey's Progress on the Visa Liberalisation Roadmap*, 4 Mayıs 2016, 56. madde.

92 AB Komisyonu, *Exchanging and Protecting Personal Data in a Globalised World*, 10 Ocak 2017, sf. 14.
Nurullah Tekin, "*An Assessment of the Turkish Draft Law On Protection of Personal Data in Light of the EU Data Protection Directive*", **Human Rights Review**, S:4/1, Haziran 2014, sf. 21-89

Kurul'un kişisel verilerin yurt dışı aktarımına uygulayacağı denetim aynı zamanda 181 sayılı Ek Protokol çerçevesinde yapmış olduğu taahhütler kapsamında da yer almaktadır. Bu protokolün 2. maddesine göre 108 sayılı Sözleşme'ye taraf olmayan bir uluslararası örgüte ya da ülkeye gönderilebilmesi için, o örgütün veya ülkenin 108 sayılı Sözleşme'ye uygun veri koruma standartlarına sahip olması gerekmektedir.

SONUÇ

Her devletin ülkesel sınırları dâhilinde bulunan gerçek kişilerin verilerinin kendi belirleyeceği standartlar çerçevesinde işlenmesini arzu etmesi olağandır. Aynı şekilde bu verilerin aktarılacağı diğer devletlerin uyguladığı koruma standartlarının uygunluk denetiminin de kendi kurmuş olduğu bir düzenleyici ve denetleyici kurum tarafından gerçekleştirilmesini de ulusal menfaatleri açısından en uygun seçenek olarak görebilir. Kişisel verileri koruma mevzuatı olan ve konuya münhasır düzenleyici ve denetleyici bir kurumu bulunan pek çok ülkenin konuya yaklaşımı bu şekildedir.

Bu çerçevede kişisel verilerin yurt dışına aktarılması gibi başka devletlerin ülkesel yetki alanıyla kesişmesinin arzu edilmeyen bir durum olarak algılanması şaşırtıcı değildir. Nitekim yurt dışına aktarıldığında kişisel veri devletin ülkesel yetki alanı dışında kalabilmektedir. Bu nedenle arzu edilen kontrol ve denetim güç ve hatta çoğu zaman imkânsız kalabilmektedir. Buna karşın sınır ötesi ticari faaliyetlerin ekonomik faydalarından mahrum kalmak istemeyen ve hali hazırda bölgesel ve uluslararası hukuk çerçevesinde belli taahhütleri bulunan devletlerin sınır ötesi kişisel veri aktarılmasını tamamen engelleyici değil, kişiyi verinin sahibi olarak merkezine alan düzenleyici ve denetleyici yaklaşımların benimsediği görülmektedir. Ancak işlemlerin sınır-ötesi karakteri, ulusal sınırlarla limitli denetleme ve düzenleme faaliyetlerinin uluslararası standartlarla desteklenmesini gerektirmektedir. Mevcut uluslararası düzenlemeler yeni gelişmeler karşısında yer yer yetersiz yer yer de atıl kalabilmektedir. Bu sebeple hali hazırda bu düzenlemelerde değişiklikler yapılmakta ve yeni çok taraflı antlaşmalar üzerinde müzakereler devam etmektedir.

Türkiye'de de, kişisel verilerin yurt dışına aktarılmasının hukuka uygunluğu daha çok kişisel verilerin gönderileceği ülke ile kişisel verinin elde edildiği ülkenin sağladığı koruma ve denetleme standartlarında uygunluk olmasına bağlanmıştır. Bu bağlamda gerek tabiiyetinde bulunan gerçek kişilerin temel bir hakkını korumak gerekse güvenliğe ilişkin ve ekonomik menfaatlerini gözetmek hedefi ile ulusal mevzuatın ortak standartların öngörüldüğü uluslararası antlaşmalara uygun hazırlanması ve etkin olarak uygulanmasına özen göstermek önem arz etmektedir. KVK 20. maddede de kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek Kurumun görevleri arasında zikredilmiştir. Nitekim Anayasa'nın 90. madde temel hak ve özgürlüklere ilişkin uluslararası antlaşmalara, ulusal mevzuat ile uyumsuz olması halinde üstünlük atfetmektedir. Bahsi geçen sebepler ile ve özellikle doğası itibari ile uluslararası nitelik taşıyan kişisel verilerin yurt dışına aktarılmasına ilişkin hususların uluslararası hukuk boyutuyla da ele alınması gerek teorik çalışmalarda gerekse uygulamada bütünlük sağlayacaktır.

KAYNAKÇA

Akbulut, O. (2014), *"Güncel Tartışmalar Işığında İnsan Hakları Sözleşmelerinin Türkiye Anayasal Sisteminde Normlar Hiyerarşisindeki Yeri"*, Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi, S: 9/115-116, Mart-Nisan 2014, sf: 7-45.

Barayre, C. (2016), "*Data Protection Regulations and International Data Flows: Implications for Trade and Development*" [Power Point Sunum] MIKTA Workshop on Electronic Commerce, WTO Headquarters, Geneva.

Bygrave, L.A. (2014), *Data Privacy Law An International Perspective*, New York: Oxford University Press.

Cate, F.H., Cullen, P., Mayer-Schönberger, V. (2014) *Data Protection Principles for the 21st Century*, Oxford Internet Institute: Oxford University.

De Hert, P., Papakonstantinou, V. (2013) "*Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*", Journal of Law and Policy for the Information Society, S: 9/3, Yaz 2013, sf. 271-324.

Drake, W.J., Cerf, V.G., Kleinwächter, W. (2016) *Internet Fragmentation: An Overview (White Paper)*, World Economic Forum: Davos.

Fuster, G. G. (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer International Publishing, Switzerland, 2014.

Gellman R., Dixon P. (2016) Failures of Privacy Self-Regulation in the United States. In: Wright D., De Hert P. (eds) Enforcing Privacy, Springer International Publishing, Switzerland, 2016, sf: 53-77.

Greenleaf, G. (2012), "*The influence of European data privacy standards outside Europe: implications for globalization of Convention 108*", International Data Privacy Law, S:2/2, sf: 68–92.

Greenleaf, G. (2013), "*Data protection in a Globalized World*", Research Hanbook on the Governance of the Internet, Ed. by Ian Brown, Cheltenham, UK: Edward Elgar Publishing Limited.

Greenleaf, G. (2016), "Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives", Privacy Laws & Business International Report, S:142, sf. 14-17.

Greenleaf, G. (2016) "*International Data Privacy Agreements After the GDPR and Schrems*", Privacy Laws & Business International Report, S:139, sf. 12-15.

İtişgen, R. (2015), "*Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı olarak Verme veya Ele Geçirme Suçu*", Türkiye Adalet Akademisi Dergisi, Ekim 2015, S:6/23, sf.178-202.

Kuner, C. (2013), *Transborder Data Flow and Data Privacy Law*, Oxford, Oxford University Publishing, 2013.

Kuner, C. (2018), *"International Organizations and the EU General Data Protection Regulation*" (2018). University of Cambridge Faculty of Law Research Paper Series, No. 20/2018, sf:4.

Lynskey, O. (2015) *The Foundations of EU Data Protection Law*, 2015, Oxford: Oxford University Press.

Malawer, S., (2001), "*Global Governance of E-commerce and Internet Trade: Recent Developments*", Virginia Lawyer, S:14, sf. 14-19.

Misroch, A. (2015), "*U.S. Tech Firms Look To Data Centers on European Soil*", The Wall Street Journal.

Molnar-Gabor, F. (2016) "*Data Protection*", Max Planck Encyclopedia of Comparative Constitutional Law, Oxford: Oxford University Press.

Kokott J., Sobotta C., "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", International Data Privacy Law, S:3/4, 1 Kasım 2013, sf. 222–228.

Korkmaz, İ. (2016), "*Kişisel Verilerin Korunması Kanunu Hakkında bir Değerlendirme*", Türkiye Barolar Birliği Dergisi, S:124, sf. 81-152.

Küzeci, E. (2011), "*Anayasal Bir Hak: Kişisel Verilerin Korunması*", Bilişim Dergisi, S: 38/128, Şubat 2011, sf. 142-149.

Newman, A.L., (2008), *Protectors of Privacy: Regulating Data in the Global Economy,* New York: Cornell University Press.

Özkan, I. (2014), "*Uluslararası Hukuk – Özel Hukuk İlişkileri*", Yaşar Üniversitesi Elektronik Dergisi, S:8 (Prof. Dr. Aydın Zevkliler'e Armağan), sf. 2127.

Riccardi, J.L., "*The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?"*, Boston College International & Comparative Law Review S:6/1, 1983, sf. 243-272.

Tekin, N. (2014), "*An Assessment of the Turkish Draft Law On Protection of Personal Data in Light of the EU Data Protection Directive*", Human Rights Review, S:4/1, sf. 21-89

Veronica, M., Asinari, P. (2002), "*Is There Any Room for Privacy and Data Protection within the WTO Rules*", Electronic Communication Law Review, S:9, sf.249.