YOLCU İSİM KAYITLARININ TERÖRLE MÜCADELE KAPSAMINDA YURT DIŞINA YASAL AKTARIMI: AVRUPA BİRLİĞİ UYGULAMALARI VE TÜRKİYE

LEGAL TRANSMISSION OF PASSENGER NAME RECORDS ABROAD FOR FIGHTING AGAINST TERRORISM: EUROPEAN UNION PRACTICES AND TURKEY

Gizem GÜLTEKİN VÁRKONYI*

Özet: Terörizmin son yıllarda daha uluslararası bir nitelik kazanmasıyla terörle mücadelede uluslararası iş birliğinin önemi artmıştır. Kişisel verilerin suç ve terörle mücadelede bir istihbarat değeri olduğu bilinmektedir. Bu kapsamda veriler bir güvenlik önlemi olarak toplanıp işlenebilmektedir. Ancak verilerin toplanması ve işlenmesi esnasında Kişisel Verilerin Korunması hakkı ihlal edilmeden yasal bir temele dayanmalıdır. Havacılık sektöründe Passenger Name Records (PNR) olarak bilinen Yolcu İsim/Rezervasyon Kayıtları farklı tür ve miktarda kişisel veri içermektedir. Bu veriler ilk kez Amerika Birleşik Devletleri güvenlik güçleri tarafından ABD'ye gelen ve ABD'den giden uçaklardaki yolcuların profil analizini yapmak üzere ek güvenlik önlemi olarak edinilmiş, ancak kısa zamanda Avrupa Birliği tarafından Kişisel Verilerin Korunması mevzuatını ihlal ettiği gerekçesiyle yasal bir temele dayandırılması gerektiği ortaya çıkmıştır. Terörle en aktif biçimde mücadele eden ülkemizde kişisel verilerin korunması ile ilgili mevzuatın yetersiz kalmasından dolayı ülkemiz böyle bir programdan yararlanamamaktadır. Türkiye, AB ve ABD arasındaki ikili iş birliği örneğinde olduğu gibi, programa dahil olabilmek için gerekli yasal düzenlemelerde bulunmalıdır.

Anahtar kelimeler: Kişisel Verilerin Korunması, Terörle Mücadele, Güvenlik, PNR

Abstract: Terrorism has became a more international issue which brought the fact that it can be solved with international cooperation. It is well known that personal data has an intelligence value in the frame of counter-terrorism. Personal data can be collected and processed in this way. However, this shall be done in a legitimate ground without interfering the fundamental rights of people. PNR program in the aviation security has been launched by the US authorities as an additional security measure but shortly it was recognized that it should be based on a cooperative bilateral agree-

* Szeged Üniversitesi Siyasal Bilimler ve Hukuk Fakültesi Doktora Öğrencisi, gizemgv@juris.u-szeged.hu

ment for a reason that it breaches the EU personal data legislation. Turkey, as one of the active fighting countries against terrorism, could not benefit from such collaboration due to the weak personal data legislation. Turkey should take necessary legal steps to benefit from such cooperation.

Keywords: Personal Data Protection, Counter-Terrorism, Security, PNR

Kişisel verilerin korunması ile ilgili ilk adımlar genelde özel hayatın gizliliği kapsamında atılmış, özel hayatın gizliliği ise fiziksel çevrenin korunması veya aile yaşamına saygı gibi temel haklar kapsamında kavramsallaştırılmıştır. Kişisel verilerin korunması hakkı bir temel hak olarak ulusal anlamda ilk kez Almanya, İsviçre, Portekiz gibi Avrupa ülkeleri mevzuatında, uluslararası anlamda ise ilk kez Avrupa Konseyi (AK) ve Avrupa Birliğinin (AB) mevzuatlarında görülmektedir. AK'nin 1981 yılında imzaya açtığı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 Sayılı Sözleşme)[1] konu ile ilgili ortaya konmuş ilk uluslararası belge olarak kabul edilebilir. Akabinde 1995 yılında AB mevzuatına katılan "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" (95 Direktifi)[2] yalnızca AB ülkeleri için değil, diğer ülkeler için de önemli bir model haline gelmiştir. Ayrıca, Kişisel Verilerin Korunması hakkının AB Temel Haklar Şartının 8. maddesinde başlı başlına bir hak olarak belirtilmesi ve 95 Direktifinin Kişisel Veri Koruma Yönergesi olarak değiştirilmesi, AB'nin konuyu yakından takip ettiğini göstermektedir.

Teknolojik gelişmelerin veri toplama ve işleme konusunu sistemler açısından çok daha kolay ve uygun hale gelmesi ile birlikte verilerin hem bir ülke sınırları içerisinde gezinebilmesi hem de sınır dışına kolayca aktarılabileceği gerçeğini ortaya çıkmıştır. Bu gerçek, verilerin elektronik sistemlerde güvenliğinin sağlanması gerektiğini, bunun ise

---

1 Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme, , 28.1.1981, CETS 108, Strasbourg.

2 OJ L 281 , 23/11/1995 P. 0031- 0050. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

ancak yasal adımlarla düzenlenebileceğini göstermiştir. Kişisel verilerin milli güvenlik çerçevesinde terörle mücadele ve ciddi suç teşkil eden durumlar kapsamında istihbarat oluşturma adına yurt dışına aktarımı ise başlı başına yasal düzenleme gerektiren bir konu olarak zamanla ortaya çıkmıştır. Konu zaman zaman ikili ülkeler arasında siyasi krizlere yol açsa da hukukun gücü bu konuya da çare olmuştur. Yolcu İsim Kayıtları (YİK)[3] kişilerin veri koruma hakkına ve gizliliğine zarar verebilecek şekilde böyle bir kategoride değerlendirilebilecek bir örnek olarak verilebilir.

YİK Programı terörle mücadele kapsamında ABD'ye gelen ve ABD'den başka ülkelere hava yolu ile yolculuk yapacak yolcuların ön güvenlik kontrollerinin yapılabilmesi amacıyla 19 Kasım 2001'de yürürlüğe giren Havacılık ve Taşımacılık Güvenliği Yasası[4] ile gündeme gelmiştir. Bu program bilhassa 9/11 terör saldırısı üzerine ve dünyada ve ABD'de artan terör olaylarına karşılık ek bir güvenlik önlemi olarak geliştirilmiştir. ABD'li güvenlik güçlerinin (ABD İç Güvenlik Bakanlığı başta olmak üzere) YİK bilgilerini paylaşmayan havayolu şirketlerine para cezası verme veya inişe izin vermeme gibi yaptırımları birçok havayolu şirketini YİK bilgilerini paylaşmaya zorlamıştır. İç Güvenlik Bakanlığı adına YİK bilgilerini toplayan ABD Gümrük ve Sınır Koruma idaresi, bu bilgileri bir yolcunun milli güvenliğe zarar verip vermeyeceği ile ilgili karar vermek için kullanmaktadır. Artan terör olaylarına önlem almak amacıyla bu denli geniş ve detaylı kişisel bilgilerin sağlanması, işlenmesi ve saklanması güvenlik güçleri ve havayolu şirketlerine çeşitli sorumluluklar getirmiştir. Kişisel verilerin aktarımı konusunda her ülkede yeterli yasal düzenlemenin bulunmaması, toplanan verilerin korunması ve güvenliğinin sağlanması ile ilgili sorumluluğun yerine getirilememesi durumunu ortaya çıkarmıştır.

YİK bilgileri emniyet teşkilatı, gümrük birimleri ve göç bürolarının vereceği kritik kararları etkileyen ve içerik açısından oldukça önemli

---

3 Yazar İngilizcesi "Passenger Name Record" olan ve Türkçe'de "Rezervasyon Kaydı" olarak kullanılan terimin, isimle başlayıp çok sayıda önemli kişisel verileri içeren bir kod olarak, ticari anlamda kullanılan birleşik rakamlardan daha fazlası olduğuna dikkat çekmek için birebir çeviriyi tercih etmiştir.

4 Aviation and Transportation Security Act, 49 U.S. Code § 114, Nov. 19,2001. https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf

bilgilerdir. Terörle mücadelede uluslararası iş birliklerinin öneminin kavranması üzerine YİK bilgilerinin toplanması ve işlenmesi yalnızca ABD'de değil başka ülkelerde de gündeme gelmiştir. Ancak bu denli geniş ve ayrıntılı kişisel verilerin korunması konusunda özellikle ABD düzenlemelerinin AB standartları ve 95 Direktifiyle çelişmesi AB otoritelerinin dikkatini çekmiştir. AB ve ABD arasında uzun süren politik tartışma ve görüşmeler sonucunda 2004 yılında, YİK bilgilerinin ABD'ye yasal bir biçimde aktarımını öngören ilk anlaşma imzalanmıştır. Ancak bu anlaşma Avrupa Adalet Divanı (AAD) tarafından iptal edilmiştir.[5] AAD bu kararı, ABD ve AB'nin gizlilik konusuna tamamen farklı pencerelerden yaklaştığı gerçeğine dayanarak almıştır. Buna göre ABD, aldığı YİK verilerini yeterli düzeyde koruyacak yasal altyapısı olmadığı sebebiyle 95 Direktifini ihlal etmiştir. Kararın gerekçeleri ise şöyledir:

- Verilerin elektronik sistemlerden "çekme"[6] yoluyla sağlanması veri aktarımı için adil ve uygun bir metot değildir,
- Aktarılacak verilerin sayısı ihtiyaç duyulandan fazladır,
- Verilerin sağlanma amacı net bir biçimde ifade edilmemiştir,
- Verilerin ABD tarafından gereğinden fazla bir zaman dilimi içerisinde saklayabileceği fark edilmiştir.

Anlaşmanın bahsedilen sorunlar çerçevesinde 8 yıl içerisinde birkaç kez düzeltilmesine rağmen, taraflar iş birliklerini yasal bir temelde devam etme kararı alarak 2012'de yılında "AB-ABD YİK Verilerinin ABD İç Güvenlik Bakanlığı tarafından Kullanımı ve Transferi Anlaşmasını[7]" imzalamıştır. Günümüzde hala geçerliliğini koruyan anlaşmanın süresi 2019 yılında sona erecektir.

---

5 Judgement of the Court (Grand Chamber), 30 May 2006, ECLI:EU:C:2006:346 http://curia.europa.eu/juris/showPdf.jsftext=&docid=57549&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=440984

6 Veriyi talep eden elektronik sistem, istediği zaman istediği veriyi karşı sistem very tabanından çekebilmektedir.

7 OJ L 215, 11.8.2012, p. 5–14. Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security. Anlaşmanın 26. maddesine göre anlaşma 7 yıl geçerlidir. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416915581157&uri=CELEX:22012A0811(01)

AB, bahsi geçen anlaşma ilk olmak üzere 2006'dan beri Kanada, 2013'den beri Avusturalya olmak üzere iş birliğini genişletmiştir. Meksika ile 2015'ten beri süren görüşmeler AB'nin konu ile ilgili çalışmalarının devam ettiğini göstermektedir. AB'nin üye devletler arasında da konuyu standartlaştırmaya ve yasal bir arka plana dayandırmaya çalıştığı bilinmektedir. Ancak özellikle kendisine üye olmayan ülkelerle olası iş birliğini standart bir yasal arka plana dayandırmak isteyen AB, 2010 yılında yayınladığı "AB'ye üye olmayan ülkelerle AB arasında YİK veri transferi genel kriterleri" veya kısaca Küresel Yaklaşım olarak adlandırabileceğimiz bildirimi ile aslında standart bir çerçeveyi kendi açısından çizmiştir.

Türkiye 40 yılı aşkın bir süredir terörle en aktif biçimde mücadele eden bir ülkedir ancak, özellikle 2015-2017 yılları arasındaki saldırılar adeta 90'lardaki kanlı ve vahşi saldırıları hatırlatmaktadır. Çok farklı terör örgütleri tarafından aynı amaçla yapılan yaklaşık 40 terör saldırısı ve darbe girişimi adı altındaki 15 Temmuz 2016 terör saldırısı, yüzlerce vatandaşımızın hayatını kaybetmesine ve yine yüzlercesinin de yaralanmasına veya sakat kalmasına sebep olmuştur. Rus Büyükelçisinin Aralık 2016'da Ankara'da katledilmesi ile birlikte artık açıkça belli olmuştur ki, Türkiye bugün farklı gruplara mensup ve farklı alanlarda aynı amaca hizmet eden bir terörist profili ile karşı karşıyadır. Bazen istihbarat,[8] bazen de yılların tecrübesine[9] dayanan tek bir fark ediş, birçok vatandaşımızın hayatını kurtaran ve ülke güvenliğine katkıda bulunan önemli unsurlardır. En ufak bir bilgi veya verinin teröristlerin hain planlarını bozmak için ne denli önemli olduğundan aşağıda bahsedeceğiz. Bu yüzden bu çalışmamızda Türkiye'nin de terörle mücadele konusunda önemli sayılan

8 Türkiye'deki terör saldırıları geçmişte belki de daha çok ülke sınırları içerisindeki bir grup terörist tarafından planlanıp icra ediliyordu. Ancak Türkiye'ye karşı her türlü terör olaylarının dışarıdan da açık biçimde desteklenmesi, komşu ülkelerde ortaya çıkan IŞİD gibi agresif terör örgütleri ve bu örgütlerin her yerde aktif eylemlerde bulunmaya başlaması ülkemizi etkilemektedir. Hatta teröristler Türkiye'yi Avrupa'ya açılan bir kapı olarak görmekte, komşu ülkelerden Avrupa'ya veya Avrupa'dan komşu ülkelere yolculuk eden teröristler Türkiye'den mutlaka geçmektedir.

9 5 Ocak 2017'de İzmir Adalet Sarayına saldırı planıyla gelen ancak kahraman Fethi Sekin'in canı pahasına durdurduğu teröristlerden bahsetmekteyiz. Teröristlerin arabasından 2 kalaşnikof, 8 el bombası, 8 roketatar ve çeşitli silahların çıkması planın büyüklüğünü göstermektedir.

YİK verilerinin aktarımı konusunda AB ile bir iş birliği anlaşmasına varmasının önemini vurgulayacağız.

Türkiye'de veri koruma yasalarının yetersizliği ve konu ile ilgili çalışmalarda oldukça geç kalınmış olması, kişisel verilerin korunması konusunda global bir lider konumunda olan AB ile iş birliği konusunda sorunlar çıkmasına sebep olmuştur. Bir Avrupa ülkesi olarak Türkiye, Kişisel Verilerin Koruma Kanununu kabul etme konusunda çok geç kalmıştır. Türkiye yukarıda bahsi geçen 108 Sayılı Sözleşmeyi imzalamış, ancak anlaşmanın Türkiye Büyük Millet Meclisi'nde onaylanması için 2016'ya kadar beklenmiştir. 2014 yılında yapılan Anayasa Referandumu ile birlikte 1982 Anayasamıza giren Kişisel Verilerin Korunması hakkı, 2016'da kanunlaşmış olmasına rağmen gerek güncel siyasi gelişmeler gerekse darbe girişimi sonrasındaki gergin atmosferden dolayı ön planda tutulamamıştır. Bu durum, çalışmamızın da temelini hazırlayan bazı soruları akıllara getirmektedir:

1. Kişisel Verilerin Korunması Kanunu özellikle Avrupa Birliği ülkeleri ile YİK verileri paylaşımı konusunda yeterli midir?
2. Türkiye'den yurt dışına YİK veri aktarımı yapılmakta mıdır? Konunun yasal arka planı nedir? Pratikte durum ne şekildedir?
3. Uluslararası YİK Programından Türkiye nasıl faydalanabilir?

Bu çalışmada kişisel verilerin korunması ile ilgili genel bir değerlendirme, ardından terörle mücadele amaçlı YİK paylaşımı kapsamında AB ile ABD müzakerelerini inceleyerek daha dar kapsamda bir tartışma sunacağız. Daha sonra YİK verilerinin yurt dışına aktarılması ile ilgili Türkiye'nin mevcut yasal temelini, AB'nin PNR Verisi Transferlerine Küresel Yaklaşımı[10] belgesine göre inceleyeceğiz. Ayrıca, Türkiye'den YİK verilerinin yurt dışına aktarılması konusunda pratikte nasıl bir yol izlendiğini göstermeye çalışacağız. Sonuç kısmında ise Türkiye ile AB arasında olası bir YİK veri aktarımı anlaşması için Türkiye tarafında atılması gereken olası adımları tartışacağız.

---

10 Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries COM/2010/0492 final. Belge, AB ile AB olmayan ülkeler arasında YİK veri aktarımının gerçekleşmesini sağlayacak ikili anlaşmalar için genel yasal kriterleri belirlemektedir. Yazar bu dokümanın başlığını Küresel Yaklaşım dokümanı olarak çevirmiştir

1. Temel Bir Hak Olarak Kişisel Verilerin Korunması

Ünlü Gartner Inc.'in Başkan Vekili Peter Sondergaard, büyük verinin 21.yüzyılın petrolü olduğunu söyleyerek[11] verinin, bilginin ve bilmenin gücüne işaret eder. Bilgi temelde bir grup verinin anlamlı biçimde belli bir amaçla bir araya gelmesi ile oluşan bir kavramdır. Bu çerçevede bilginin ham veriye göre anlaşılması ve yorumlanmasının da daha kolay olduğunu söylemek yanlış olmayacaktır. Verilerin anlamlı bütünler haline getirilebilmesi şüphesiz bir miktar zaman ve emek gerektirir. İkinci Dünya Savaşı sonrası yaşanan bilgi patlaması ve bilme merakındaki artış, aslında daha çok bilenin daha da güçlü olabileceği önermesinin temelini oluşturur. Zaten, Sondergaard'ın yorumunun temeli olarak düşündüğümüz bilginin güç olduğu gerçeği de buradan gelmektedir. Teknolojinin ve elektronik sistemlerin gelişimi ile bu gelişmelerin kişilerin günlük hayatına girişi, veri ve bilgiye erişme, bunların aktarılması ve saklanması işlemlerini çok daha kolay hale gelmiştir. Bu gelişmeler aynı zamanda kişilerin kendi ile ilgili bilgileri kontrolsüz biçimde Internet ortamında paylaşmasına sebep olmuş, bu paylaşım gizlilik ile ilgili endişeleri gündeme getirmiş ve sonuçta gizlilik ile kişisel verilerin korunması arasında bir ilişki olduğu fark edilmiştir. Bu ilişki ise şöyle açıklanmaktadır;[12] "Veri koruma hakkı, gizlilik hakkından hem daha geniş hem de daha dardır. Daha geniştir, çünkü veri koruma hakkı ifade özgürlüğü, din ve vicdan hürriyeti, bilgi edinme özgürlüğü, ayrımcılık yapmama ilkesi gibi kişisel hakların yanı sıra diğer temel hakları da korumaktadır. Ancak daha dardır, çünkü verilerin korunması hakkı yalnızca kişisel veriler işlendiği zaman geçerlidir".

Kişisel verilerin korunması hakkı günümüzde birçok devletin anayasası tarafından temel haklar çerçevesinde yasal garantiye alınması gereken bir haktır. 1990'lı yıllardan önce yasalarda ve hukuk literatüründe bu konu genelde gizlilik hakkı ile bağdaştırılıp yorumlan-

---

11 Peter Sondergaad, "Big Data Fades to the Algorithm Economy", Forbes/Tech, 14 August 2015. https://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/#2f3b5c1a51a3

12 Serge Gutwirth, Yves Poullet ve Paul de Hert, "Data Protection in a Profiled World" Dordrecht ; New York : Springer, 2010, s.37.

maktaydı. Gizliliğin korunması hakkı İkinci Dünya savaşı sonrasında kişisel verilerin saklandığı veri tabanlarının ırkçılık, soykırım ve azınlıkları hedef alan uygulamalarda kullanılması sebebiyle kamunun özel yaşama müdahalesinin ne denli tehlikeli olduğunun açıkça anlaşılması[13] ile tekrar düzenlenmiştir. Gizliliğin korunması bir temel hak olarak İnsan Hakları Evrensel Beyannamesi'nde[14] veya Avrupa İnsan Hakları Sözleşmesi[15] gibi uluslararası mevzuatta yerini almıştır. Ancak bilgisayar, akıllı telefon, tablet gibi teknoloji ürünleri ile çevirim içi hizmetler gibi insan hayatını kolaylaştıran yazılım ürünleri günlük hayatta artan şekilde yer almaya başladıkça salt gizliliğin korunması hakkı yasal anlamda yetersiz görülmeye başlandı. Bir yandan, bu ürünleri kullanmak istemeyenlerin bile belli hizmetleri daha masraflı olarak edinmemek için kullanmaya alışması, diğer yandan yasal eksiklikler sebebiyle teknolojik nimetlerin insanların temel haklarına zarar verdiği gerçeğinin fark edilmesi çok uzun sürmedi. Böylelikle gizlilik terimi tek başına gelişmeleri karşılayamayıp bilgi gizliliği, manevi (karar) gizlilik ve fiziksel gizlilik (özel yaşamın veya aile yaşamının gizliliği) gibi çeşitli konseptlere genişledi.[16] Bilgi gizliliği genelde kişisel veri koruma konusunu da kapsarken, halk arasında gözetim konusunda artan algı ve anlayış[17] sayesinde bilgi gizliliğinden öteye gidilmesi gerektiği fark edildi. Örneğin, İnternet daha önceleri gizliliğin korunmasına katkı sağlayan bir araç iken, pazarlama ile ilgili yöntemlerin internetle birlikte değişimi ve gelişimi sebebiyle artık kimin hangi internet sitelerinden ne tür ürünler satın aldığı ve hatta demografik bilgileri kolayca edinilebilir hale gelmiştir.[18] İsimler, adresler, banka kartı bilgileri ve bunun gibi birçok değerli bilgi yeterli güvenlik önlemleri alınmadıysa

13 Neil Robinson, Hans Graux, Maarten Botterman ve Lorenzo Valeri, "Review of the European Data Protection Directive", The Rand Corporation, 2009, s.6.

14 Birleşmiş Milletler Genel Kurulu," İnsan Hakları Evrensel Beyannamesi", 10 Aralık 1948, 217 A(III).

15 Avrupa Konseyi, "Avrupa İnsan Hakları Sözleşmesi", 4 Kasım 1950, ETS 5

16 Alina Savoiu, Catalin Capatina Basarabescu, "The Right to Privacy", Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series, 1, 89-96, 2013

17 David Wright ve Charles Raab, "Privacy Principles, Risks and Harms." International Review of Law, Computers & Technology 28, no. 3 , 2014, s.278.

18 Chen-Hung Chang, "New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory", National Taiwan University Law Review 10, no. 1, 2015, s.130.

kolayca elde edilebilir, yeterli yasal önlemler alınmadıysa da kötü niyetli kişilerin eline kolayca geçebilir hale gelmiştir.

2. Hava Taşımacılığı Alanında Kullanılan Yolcu İsim Kayıtları

Uluslararası Sivil Havacılık Örgütünün (USHÖ) 2010 yılında yayımladığı YİK Verileri Kılavuzuna[19] göre YİK, hava taşımacılığı sektöründe[20] yolcunun kendi yaptığı veya yolcu adına yapılan her bir rezervasyon kaydının havayolu şirketi veya yetkili acentalar tarafından ürettiği eşsiz kayıt numarasıdır. Zamanla, yolcuların kendi rezervasyonlarını rahatça yapabilmeleri için *online rezervasyon* sistemleri de geliştirilmiştir. Avrupa Konseyine göre YİK verilerinin kullanım amacı, hava taşımacılığı hizmetlerinin geliştirilebilmesi adına ticari amaçlıdır. Bir YİK verisini oluşturan veri parçacıklarının listesi oldukça uzun ve detaylıdır. Avrupa Konseyinin YİK ile ilgili tespit ettiği veri alanları en güncel olmakla birlikte yolcunun tam adından varsa yolcu üyelik bilgilerine, bagaj bilgisinden YİK rezervasyon tarihçesine kadar toplamda 22 adet veri alanından oluşmaktadır.

YİK verileri "terörizm ve suçla mücadelede önemli bir silah"[21] olarak da tanımlanmaktadır, ancak aynı zamanda bu verilerin toplanması, saklanması ve işlenmesi sonucunda masum insanların da suçlu gibi muamele görmesi ihtimalini beraberinde getirmektedir. Konuya ilişkin sorunlar özellikle ihtiyaç duyulandan daha fazla bilgi toplanması ve terörizmle mücadele kapsamı dışındaki otoritelerle paylaşılması veya kullanılması ihtimali üzerine ortaya çıkmaktadır.

Yolcuların uçak bileti rezervasyonu esnasında verdikleri bütün bilgiler Küresel Dağıtım Sistemi olarak da bilinen Bilgisayarlı Rezervasyon Sisteminde (BRS)[22] ve havayolu taşıyıcılarının kendi rezer-

---

19 International Civil Aviation Organization (ICAO), "Guidelines on Passenger Name Record (PNR) Data", ICAO, 2010. https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf

20 Türkiye'de bazı otobüs firmaları, web üzerinden rezervasyon yapan yolcularına YİK kodu sağlamaktadır. Kodlar genelde isim ve soyisim, yolculuk tarihi ve saati bilgisinden oluşmakta T.C. Kimlik Numarası da bazen istenmektedir.

21 Georgios Nouskalis, "Biometrics, E-Identity and the Balance between Security and Privacy: A Case Study of Passenger Name Record (PNR) System Comment", *The Scientific World Journal*, 11, 2010, s.474.

22 Uluslararası alanda Global Distribution Systems (GDS) ve Computerized Reser-

vasyon sistemlerinde tutulmaktadır.[23] İsim-soy isim, doğum tarihi, telefon numarası gibi bilgilerin yanı sıra yolcuların milliyeti, pasaport numarası, cinsiyeti ve yemek tercihi gibi daha özel ve hassas bilgileri de bu sistemlerde tutulur. Rezervasyonlar iptal olsa bile bu bilgiler sistemde tutulur. Oluşturduğu kişisel seyahat bloğunu yasal bir bilgilendirme platformuna çeviren Hasbrouck, BRS'lerin düzenli yolculuk yapan yolcuların geçmiş rezervasyon işlemlerinden yola çıkarak tüm veri tabanlarından elde ettiği bilgileri bütünleştirip bir profil oluşturduğuna dikkat çekmektedir. Bu profil biletleme veya pazarlama amaçlı değildir; örneğin göçmen büroları bu profili kişiyle ilgili bilgi edinmek için kullanılabilir. Aslında sistemlerde tutulan yolcu verileri yalnızca YİK verileri ile sınırlı değildir. İleri Seviye Yolcu Bilgileri (İSYB) olarak bilinen ve kişilerin daha çok pasaport ve vize bilgileri gibi bilgilerini içeren bir veri paketi daha bulunmaktadır. YİK ve İSYB verileri arasındaki farkı şöyle açıklayabiliriz: YİK verileri öncelikle hava yolları şirketlerinin ticari amaçlarla oluşturduğu verilerdir. Bu verilerin güvenlik kontrolü için kullanılmaya başlanması ilk defa ABD tarafından gerçekleşmiştir. İSYB Sistemleri ise ilgili yolculuğun gerçekleşeceği sınır ve güvenlik kontrol birimlerinin uçak harekete geçmeden önce yolcu bilgilerinin aktarıldığı sistemlerdir. Eğer birimler bu bilgileri uçak kalkmadan önce alamazsa, indikten sonra kontrolleri gerçekleştirmeye başlayacak bu da çeşitli güvenlik sorunları ile zaman kaybına yol açacaktır.[24] YİK verileri standart olarak bilinmekte ve bu şekilde aktarılmakta iken, İSYB verilerinin her ülkeye göre değiştiği bilinmektedir. Hem YİK hem de İSYB verileri, sınır kontrolü görevlilerinin yolcuların uçağa biniş izinlerinin verilip verilmemesiyle ilgili karar verme aşamasında kullanılan yardımcı verilerdir. Örneğin, ABD başta olmak üzere birçok ülke bu verileri milli güvenlik açısından riskli olarak tanımlanmış yolcuların listesini oluşturmak amacıyla kullanmaktadır.

---

vation Systems (CRS) olarak bilinmektedir.

23 Richard D. Rasmussen, "Is International Travel Per Se Suspicion of Terrorism - The Dispute between the United States and European Union over Passenger Name Record Data Transfers Notes and Comments", *Wisconsin International Law Journal*, 26, 2008, s.553.

24 Rasmussen, s.555

YİK verileri oluşturulduğu anda bu veriler havayolu şirketinin mülkü haline gelir ve havayolu şirketleri bu bilgileri konu özellikle milli güvenlik ise yolcunun onayını almadan da üçüncü şahıslarla paylaşabilir veya paylaşmak zorunda kalabilir. 2001 yılından beri ABD'ye uçan tüm şirketlerin bu bilgileri yolcunun bilgisi haricinde paylaştığı bilinmektedir. Buradaki sorun ise, verilerin aktarımı herhangi bir yasal temele dayanmadığı taktirde, yolcunun temel haklarının ihlal edilmesidir.

3. Kişisel Verilerin Paylaşımıyla Ortaya Çıkabilecek Tehditler

Geniş ve çok sayıda bilginin terörle mücadele konusunda faydalı bir ek önlem getirebileceği bir gerçektir, ancak bilgilerin yalnızca bu amaçla kullanılıyor olmasının temin edilmesi gerekir. YİK verileri ayrıntılı, hassas ve bir kişiyi doğru tanımlamada oldukça faydalı bilgiler olarak yanlış yorumlandığında veya toplanış amacından farklı kullanıldığında kişi açsından ciddi sorunlara yol açabilir. Kişisel verilerin hükümetlerce toplanış amacından farklı kullanılması günümüzde yaygın bir sorundur. Veriler bir kez toplandığında hükümetlerin gözetleme stratejileri için bir araç olarak kullanılabilir. Böylelikle yalnıza terörist veya potansiyel teröristler değil, sıradan kişiler siyasi amaçlarla izlenebilir; bu da milli güvenlik amacıyla veri elde etme ile verilerin siyasi emellere hizmet eme amacıyla toplanması arasındaki sınırı bulanıklaştırabilir.[25] Bu durumun hem ülke içinde hem de uluslararası alanda sorun teşkil ettiği bilinmektedir. Örneğin, 2013 yılında eski Amerikan Ulusal Güvenlik Ajansı (NSA, National Security Agency) ve gizlilik aktivistlerinden Edward Snowden, Ajans ve diğer ABD yetkililerinin internetten ve telekomünikasyon şirketlerinden kişisel veriler elde ederek hem bireyleri hem de Brezilya, Hindistan gibi ülkeleri gözetlediğini açıklamıştır.[26] Bu durum Brezilya ve Hindistan ile ABD

---

25 Quirine Eijkman, "Counter-Terrorism, Technology and Transparency: Reconsidering State Accountability", *The Journal of International Security and Terrorism* 3, 1, 2012, s.34.

26 Henry Farrell ve Abraham Newman, "The Transatlantic Data War: Europe Fights Back against the NSA", Foreign Affairs VO - 95. Council on Foreign Relations, Inc., 2016., s130; Courtney Giles, "Balancing the breach: Data privacy laws in the wake of the NSA revelations", *Houston Journal of International Law* 37, 2, s.544.

arasında gerilime sebep olurken, AB ile ABD'nin birlikte geliştirdiği[27] ve kişisel verilerin bu iki ülke arasında ticari maksatla aktarımını sağlayan Safe Harbor Framework (Güvenli Liman) iş birliği AAD'ce sona erdirilmiştir.[28] ABD ve İngiltere'nin sadece kendi ülke vatandaşlarının değil başkalarının da kişisel bilgilerini soruşturma adı altında Google gibi özel şirketlerden elde ettiği bilinmektedir.[29] AB tarafında ise gözetim ve kişisel veri işlemenin daha geniş bir AB terörle mücadele stratejisi oluşturmasına engel olduğu, fakat AB'nin katı kuralları sayesinde şu ana kadar herhangi bir hak ihlali yaşanmadığı söylenmektedir.[30]

Ülke sınırları içerisindeki kişilerin izlenmesi yasa dışı örgütleri destekleyenleri deşifre etme amacı dışında siyasilerin kendisini destekleyen-desteklemeyenleri fişleme amaçlı da yapılmaktadır. Ancak terörle mücadele söz konusu olduğunda devletlerin siyasi emellerini değil milli güvenliği ön planda tuttuğunda başarılı sanal operasyonlar gerçekleştirdiği bir gerçektir. Örneğin, ABD İç Güvenlik Bakanlığı durumsal farkındalık adı altında Huffington Post gazetesinden Jihad-Watch isimli Web bloguna kadar farklı platformlardaki milyarlarca kişisel hesabı izleyerek İslam adı altında aşırı eylemlerde bulunan grupların ABD bağlantılarını ortaya çıkarmıştır.[31]

YİK verilerinin toplanmasından dolayı ortaya çıkabilecek en büyük risklerden biri yolcu verilerinin yolcuları "güvenli uçuş, kayıtlı yolcu ve güvenilir yolcu" olarak sınıflamaktır.[32] Bu tanımlamanın açıklaması, insanları potansiyel terörist olarak sınıflamak veya sınıflamamakla

---

27 U.S. Department of Commerce, "U.S.- EU Safe Harbor Framework: A Guide to Self-Certification", March 2009, s.1. http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf

28 Avurstuyalı bir hukuk öğrencisi ABD'nin Facebook aracılığıyla yaptığı casusluk ve gözetimin Avrupa mevzuatına aykırı olduğunu savunarak İrlanda mahkemelerine dava başvurusunda bulunmuştur. Avrupa Adalet Divanı anlaşmayı yürürlükten kaldırmıştır; Farrell ve Newman, s.130.

29 Giles, s.549

30 Giovanni Buttarelli "Counter-Terrorism Policy and Data Protection", Hearing of the European Economic and Social Committee (EESC) 9 February 2010, s.2.

31 Gözetlenen tüm sitelerin listesi ve hükümet açıklamaları ile ilgili haber için Bkz.:, Reuters Reporter, "Department of Homeland Security monitors Facebook, Twitter and news sites for 'situational awareness", DailyMail, 13 Ocak 2012. http://www.dailymail.co.uk/news/article-2085940/Facebook-Twitter-news-sites-monitored-US-Homeland-Security.html

32 Rasmussen, s.577.

ilgilidir. Özellikle kişisel bilgilerin hatalı veya yanlış yorumlanması insanların yanlış yargılanmalara veya şüpheli sıfatına girmelerine sebep olarak masumiyetlerine zarar verir. Bir kişinin Müslüman olduğunu anlamak için YİK verileri gerçekten de oldukça yeterlidir. Yolcunun yemek seçimi, geldiği ülke, dış görünüşü gibi veriler onun hangi dine mensup olduğunu gösterebilirken, otoritelerce yanlış kararlar alınmasına sebep olabilir. Bu bilgilerin herhangi bir şekilde sızması ayrımcılık, ırkçılık, yabancı düşmanlığı gibi olumsuz durumları tetikleyebilir.

Kişisel verilerin korunması yasal olduğu kadar teknolojik koruma gerektiren bir alandır. Özellikle bilgisayar sistemlerinde her gün onlarca yeni güvenlik açığının keşfedilmesi teknolojik güvenliğin önemini vurgulamaktadır. Ancak bu çalışmadan yalnızca yasal koruma üzerinde durulacaktır. Çünkü aslında iyi tasarlanmış bir yasal düzenleme teknolojik güvenliğin sağlanmasına da katkıda bulunacaktır; bir verinin bir veri tabanı üzerinde 5 yıl saklanması ise 15 yıl saklanması arasında teknolojik açıdan da fark vardır. YİK verilerinin nasıl elde edileceği, nerede ve ne kadar zaman saklanacağı gibi konular öncelikle yasal altyapıda çizilmesi gereken noktalardır. Öyle inanıyoruz ki, yasal altyapı sağlıklı bir uygulama için ilk ve en önemli adımdır.

4. Yolcu İsim Kayıtlarındaki Verilerin Önemi

Teknolojik küreselleşmenin getirdiği olumsuzluklardan biri, teröristlerin de teknolojiden haberdar olması ve onu etkili olarak kullanmasıdır. Internet ve her gün gelişen Bilgi ve İletişim Teknolojileri (BİT) teröristlerce saldırı planlama ve bu planları uygulama çerçevesinde kullanılmaktadır. Teröristler BİT'i reklam yapma ve finans kaynağı olarak da kullanmaktadır. Böylelikle kitlelere daha kolay ulaşabilmekte ve onları daha kolay etkileyebilmektedirler. Örneğin 90'lı yıllarda El-Kaide lideri bin Laden'in kendine inanları Avrupa, Orta Doğu, Güney Asya ve Afrika'ya göndermiş ve tüm bu teröristler arasındaki koordinasyonu internet üzerinden sağlamıştır.[33] Bu teröristler belirtilen bölgelere uçak aracılığıyla da ulaşmıştır.

[33] Joshua W. Hedges, "Eliminating the Learning Curve: A Pragmatic Look at Jihadist Use of the Internet", *Journal of Applied Security Research* 3, 1, 2008, s.75.

Günümüzde terörizmin sınır tanımayan karakteri yüzünden takibi zorlaşmıştır. Sosyal medya hesaplarının, Web bloglarının, Web sitelerinin veya online davranışların incelenmesi yeni bir yöntem olsa da bu yöntemle teröristler hakkında kesin bilgiler elde edebilmek pek mümkün değildir. Teröristin milliyeti, telefon numarası, görüntüsü, banka bilgileri gibi bilgiler İnternetten kolay erişilemeyebilir. Ancak bir terörist ile ilgili havayolu yolculuğu öncesi veya esnasında bilgi edinme, onu teyit etme ve hakkında karar verme çok daha kolay ve garantili bir yöntemdir.

YİK verileri yalnızca terörist avlamak için değil insan kaçakçılığı, uyuşturucu kaçakçılığı yapan veya ölümcül bulaşıcı hastalıklar taşıyan kişileri de tespit etmek için kullanılmıştır. ABD hükümeti gibi başka devlet hükümetlerinin de uçuştan önce yolcu isim listelerini arananlar listeleri ile karşılaştırarak bazı suçlulara ulaştığı bilinmektedir[34]. Bu alanlarda kullanılan bilgisayar tabanlı karar verme sistemleri sayesinde teröristlerin de tespit edilmesi de kolaylaşmıştır.

ABD otoritelerinin YİK verilerini elde etmek istemeleri aslında bu verilerin içerdiği bilgi zenginliğinden kaynaklanmaktadır. Ayrıntılı, kolay erişilebilen ve doğruluk oranı yüksek bilgiler güvenlik otoritelerine kişilerin güvenlik açısından analiz edilmesi ve hakkında karar verilmesi konusunda yardımcı olmaktadır. Veriler yolcunun kendisinden direkt olarak elde edilmiştir ve bu yüzden kimlik tespit işlemi kapsamlı şekilde yapılabilir. YİK verileri çok boyutlu veriler olarak bir ve hatta birkaç kişi hakkında ayrıntılı tespit yapılmasını sağlar.

YİK verileri öncelikle ve temelde bir kişinin milli güvenlik üzerinde yaratabileceği olası tehditlerin ortaya konabilmesi için kullanılır. Toplanan veriler riskli yolcuları sınıflandırmak ve daha sonrasında bu yolcular ile ilgili ne yapılacağı konusunda karar vermek için yorumlanır. Bir sonraki adımda veriler sorgulama veya davalarda kullanılabilir; daha sonra önlem alma ve koruma amaçlarına hizmet eder. Ülkeler veya birimler arası istihbarat ve tecrübe paylaşımı sayesinde hem ulusal hem de küresel güvenliğe katkı sağlanır.

---

34 House of Lords-European Union Committee. The EU/US Passenger Name Record (PNR) Agreement, Authority of the House of Lords, 21st Report of Session 2006-07, s.7. http://www.statewatch.org/news/2007/jun/eu-pnr-hol-report.pdf

Diyagram-YİK verilerinin terörle mücadelede fayda piramidi

YİK verileri yolcu **kimlik tespiti** adına birçok önemli bilgi taşır. USHÖ YİK Rehberine[35] göz atıldığında verilerin iki gruba ayrıldığı kolayca fark edilebilir: Kişisel bilgiler ve kişinin (planladığı) yolculuk ile ilgili bilgiler. Kişisel bilgiler isim, soy isim, varsa diğer isimler; adres, telefon numarası veya e-posta adresi gibi iletişim bilgileri ve rezervasyon veya satışta kullanılan banka/kredi kartı ile ilgili bilgiler (son kullanım tarihi, kart numarası vs.) gibi finansal bilgilerden oluşmaktadır. Bu rehberde YİK ve İSYB beraber değerlendirilmektedir ve sebebi olarak havacılık sektöründe YİK verilerinin artık İSYB ile birlikte aktarıldığı gösterilmektedir. Böylece yolcuların pasaport numarası, vize bilgileri gibi çok daha ayırt edici bilgileri de YİK verileri içerisinde aktarılır. Şu ana kadar bile bir kişiyi tanımlamaya yetecek kadar bilgiyi elde etmiş durumdayız.

Yolculuk ile ilgili bilgiler en az diğer bilgiler kadar önemlidir; çünkü bu bilgiler yolculuğa ait en doğru bilgilerdir. Kişisel bilgiler "kim" sorusunda cevap verirken, bu bilgiler "ne zaman, nereye ve nasıl" sorularına cevap verir. Yolculuk öncesi, yolculuk esnası ve yolculuk sonrası bilgiler bu kategoridedir. Yolculuk öncesi bilgiler oldukça geniş kapsamlıdır; neredeyse yolculuğun tam amacının tahmin edilmesini sağlar. Rezervasyonun kim tarafından yapıldığı, ne zaman yapıldığı, uçak kapı bilgisi gibi uçağa biniş ve iniş bilgileri bu bilgilerden birkaçı-

35 ICAO, Appendix 1.

dır. Check-in bilgileri ekstra bilgi kaynağıdır ve bu işlem sonrasındaki bilgiler yolculuk esnasında üretilen bilgileri oluşturur. Örneğin yolcunun hangi koltukta oturduğu, bagaj bilgisi, yemek seçimi gibi bilgiler bu kategoridedir. Yolcunun bagajını alıp almadığı bilgisi ise yolculuk sonrası bilgiler kategorisine örnek olarak verilebilir. Bu bilgiler artık yüzde yüz doğrulukta bilgilerdir. YİK verisine sahip bir yolcu yanında beraber rezervasyon yaptığı başka bir yolcu varsa, o yolcunun da tüm verisine erişilmesi sağlanır.

YİK verileri zaten bilinen suçlu veya teröristleri değil, şüpheliler üzerinden tespit yapmak için kullanılan verilerdir ve bu yüzden çok değerlidir. Tespitler **risk değerlendirme ve karar verme** süreçleri sonunda yapılır. Başarılı bir risk değerlendirme, yolcuların uçuş öncesi ve sonrası belli risk kriterlerine göre sınıflandırılmasıyla doğru orantılıdır. Kriterler ancak kaliteli bilgi sağlama ve edinilen tecrübelerle geliştirilebilir. Karar verme aşamasından sonra otoriteler sorgulama ve yargılama yoluyla koruma önlemleri alır. Avrupa Parlamentosu ve Konseyinin YİK verileri ile ilgili hazırladığı öneri metninde[36] verilerin sadece önleyici değil teröristlerin trend analizi, genel davranışları ve gerçeklere dayalı yolculuk senaryoları oluşturmak için de uzun süreli kullanılabileceği vurgulanmıştır.

İstihbarat ve tecrübe paylaşımı hem güvenlik güçleri birimleri hem de devletler arasında terörle mücadele konusunda sürekli bilgi akışı ve iş birliği kurulmasını sağlar. Uluslararası iş birliğinin önemi birçok başarı öyküsünde görülebilir. Örneğin, Kanada'da konuşlanmış bir şirketin kimyasal madde zinciri adı altında Hizbullah'ı desteklediği narkotik ABD ve Kanada narkotik birimlerinin iş birliği sayesinde ortaya çıkmıştır.[37] Bu örnek direkt olarak YİK verilerinin paylaşımı

---

36 Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. COM (2011) 32 final. Öneride PNR veri kullanımının faydaları arasında suç ile ilgili araştırma ve sorgulamalarda; bir güvenlik önlemi olarak ve yolcular uçuşa başlamadan önce bir güvenlik değerlendirme kriteri olarak kullanılabileceği ifade edilmektedir. Öneri çevirim içi erişilebilir:
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206007%202011%20INIT

37 White House, "National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing" October 2007, s.10

sayesinde kazanılmış bir başarı olmamakla beraber, veri paylaşımının teröristleri avlama konusundaki önemli rolünü göstermektedir.

Devletler arası iş birliği ve güven eksikliği teröristlerin eylemlerini daha cesaretle gerçekleştirmesine sebep olur. Örneğin, eğer Belçikalı yetkililer Türkiye'nin Brüksel katliamcısı Ibrahim el-Bakraoui ile ilgili yaptığı uyarıları dikkate alsaydı, bu katliam gerçekleşmemiş olabilirdi. 24 Mart 2016 tarihli WSJ haberine[38] göre bu terörist Türk polisi tarafından Suriye sınırına yakın bir yerde IŞİD şüphelisi olarak yakalanıp sınır dışı edilmiş ancak istihbarat eksikliği sebebiyle terörist olduğu ortaya çıkarılamamıştır. Diğer bir başarısızlık hikayesi ise, 26 Kasım 2015 tarihli The Economist'in[39] haberi olan 2015 Paris saldırganı Abdelhamid Abaaoud ile ilgilidir. Buna göre terörist, Belçikalı polisler tarafından aranıyor olmasına rağmen Suriye'ye uçak yolculuğu yapmış oradan da Fransa'ya geri dönebilmiştir. Fransa hiçbir Avrupa ülkesinden kendilerine istihbarat gelmediğini ifade etmiş, onlarca insan istihbarat eksikliği yüzünden can vermiştir.

Son olarak YİK verileri çok gelişmiş yazılımlar sayesinde çok kolay aktarılabilen veriler olduğundan, analiz yapabilmek için gereken zaman ve insan gücünü azaltarak işlemi önemli ölçüde kolaylaştırır. Milyonlarca verinin insan gücü ile analiz edilmesi oldukça zor olduğundan YİK verileri gibi standart ve sınıflandırılmış verileri sistemlerde belirlenmiş eşik değerlerine göre analiz yapmak işleri kolaylaştırır ve hızlandırır. Zaten terörle mücadelede hızlı hareket etmek olası saldırıları engelleme adına önemli bir etkendir.

YİK verilerinin aktarımı, analizi ve işlenmesi terörle özellikle aktif olarak mücadele eden ülkelere yardımcı bir güvenlik unsurudur; ancak verilerle ilgili tüm işlemlerin temel haklara zarar getirmeyecek şekilde yasal bir temele dayandırılması gerekmektedir.

---

https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf

38 Matthias Verbergt, Natalia Drozdiak, Dion Nissenbaum, "Brussels Suicide Bomber Slipped Terror Net", The Wall Street Journal, 24 March 2016. https://www.wsj.com/articles/brussels-suicide-bomber-slipped-terror-net-1458779556

39 The Economist, "The terrorist in the data", 26 November 2015. https://www.economist.com/news/briefing/21679266-how-balance-security-privacy-after-paris-attacks-terrorist-data

5. Yolcu İsim Kayıtlarının Yurt Dışına Yasal Aktarımı: Avrupa Birliğinin Yaklaşımı

Avrupa Birliği veri koruma konusunda attığı adımlarla küresel anlamda diğer ülkelere de yön veren örnek bir yapıdır. Kişisel verilerin korunması hakkının 1995 yılında kabul edilen "Kişisel Verilerin İşlenmesi ve Dolaşımı Kapsamında Bireylerin Korunması Direktifi"[40] ile yasal bir temele dayandıran ilk organizasyonlardan biridir. Bu Direktif Avrupa Parlamentosu, AB Konseyi ve özellikle Article 29 Working Party (Çalışma Grubu) olarak bilinen veri koruma danışma grubunun çalışmaları sonucunda 2018 yılında yürürlüğe girecek olan AB Veri Koruma Tüzüğü[41] ile değiştirilmiştir.

Küresel terör olaylarına paralel olarak son yıllarda birçok AB ülkesinde terör saldırılarının arttığı görülmektedir. Özellikle 2012 sonrasında IŞİD gibi yeni ortaya çıkan terör örgütleri Fransa, Almanya ve Belçika'da çeşitli eylemler gerçekleştirmiştir. Sadece 2016 yılında Hamburg, Normandy, Ansbach, Nice, Münih ve Brüksel[42] terör saldırısına maruz kalmış birkaç Avrupa şehrine örnek gösterilebilir. AB üye devletlerinin güvenlik ile ilgili karar ve uygulamaları genelde ülkelerin kendi iç işleri sayılmasına rağmen, AB'nin bu konuda takındığı genel bir tavır vardır: Terörle mücadelede yasal temellere dayanan kapsamlı iş birlikleri sayesinde etkili çözümler üretmek. Nitekim, Avrupa Komisyonu ABD yetkililerine ABD'nin PNR uygulamalarını başlatmasından yaklaşık iki sene sonra, 2003 yılında, uygulamanın Direktife aykırı olduğu konusundaki endişelerini iletmiştir. ABD ve AB 2012 yılında imzaladıkları PNR anlaşması[43] sayesinde şu anda ortak bir PNR programı yürütmektedir, ancak bu anlaşmanın sağlanması için birçok anlaşma ve müzakere yapılması gerekmiştir. Yasal bir temelde PNR veri aktarımının nasıl yapılacağı konusunda tarafların geçirdiği süreci anlamak için 2003'ten 2012'ye geçen süreyi kısaca inceleyeceğiz.

---

40 OJ L 281, 23/11/1995 P. 0031 – 0050. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

41 OJ L 119, 4.5.2016, p. 1–88 Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

42 Saldırılarla ilgili bilgi ve tarihler için Bkz.: https://www.rt.com/viral/370973-terror-attacks-timeline-europe/

43 OJ L 215, 11.8.2012, p. 5–14

Kişisel verilerin korunması konusu AB ile ABD arasında her zaman sorun olmuş bir konudur. Sorunun sebebi ise AB ile ABD'nin gizlilik kavramına farklı açılardan yaklaşımı ve bu yaklaşımın haliyle yasalara yansımasıdır. AB gizlilik konusuna temel haklar çerçevesinde yaklaşmakta, ABD ise konuyu bir tüketici hakkı olarak görmektedir. Bu çok yönlü çatışmalar açıkça şöyle ifade edilmektedir;[44] Gizlilik konusundaki farklı algılar güvenliğe karşı gizlilik; ABD'ye karşı AB terörle mücadele mevzuatı, AB'ye karşı ABD gizlilik rejimi; AP'ye karşı Avrupa Konseyi ve Avrupa Komisyonu; verilerin ticari amaçla işlenmesine karşı güvenlik amacıyla işlenmesi ve veri yönetimine karşı veri madenciliği konularını karşı karşıya getirmiştir. Örneğin Güvenli Liman (Safe Harbor) anlaşması AB'den ABD'ye kişisel verilerin ticari amaçlı akşına kişilerin veri koruma hakkı çerçevesinde izin veren bir anlaşma olarak imzalanmıştı. Ancak bu anlaşma, verileri temin eden ABD şirketlerinin güvenlik veya terörle mücadele kapsamında başka ABD otoriteleriyle paylaşımı hususunu bulanık bırakmıştır. Bunun gibi örnekler çerçevesinde AB, ABD'nin YİK Programına şüpheyle yaklaşmıştır. YİK Programı bir yandan güvenlik için gerekli görülmekteyken bir yandan da AB mevzuatını ihlal etmekte, aynı zamanda da havayolu şirketlerine para cezaları öngörmesiyle AB firmalarını zarar etmekle yüz yüze bırakmıştır[45].

AB YİK veri aktarımının güvenlik artırıcı bir önlem olduğu konusunda her zaman ABD ile hemfikir olmuştur. AB'nin ABD'den önce kendi içinde bir YİK programı planladığı ve bazı üye devletlerin ticari amaçlı da olsa YİK paylaşım sistemleri olduğu bilinmektedir.[46] AB 27 Nisan 2016'de kabul ettiği AB-YİK Direktifi[47] ile bu verilerin AB üye ülkeleri güvenlik birimleri arasında paylaşılmasını yasal hale getirmiştir.

---

44 Maria Tzanou, "The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security Research Article", *Utrecht Journal of International and European Law*, 31, 80, s.88.

45 Alenka Kuhelj, "The Twilight Zone of Privacy for Passengers on International Flights between the EU & USA." *U.C. Davis Journal of International Law & Policy,* 16, 2, 2009, s.403

46 Ibid, s.394

47 OJ L 119, 4.5.2016, p. 132–149 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. http://eur-lex.europa.eu/eli/dir/2016/681/oj

Verilerin AB dışına aktarımı söz konusu olduğunda, AB tarafından veri aktarım kriterlerinin oluşturulması zorunluluğu fark edildi.[48] AB Komisyonu bu boşluğu acele olarak doldurmak amacıyla ABD ile 2004 yılında YİK verilerinin ABD İç Güvenlik Bakanlığı, Gümrük ve Sınır Koruma Bürosuna aktarılması ve Büro tarafından işlenmesine izin veren anlaşmayı imzaladı.[49] Bu anlaşma Avrupa Komisyonu'nun AP ve AAD tarafından sertçe eleştirilip AAD tarafından iptal edildi. AAD iptal gerekçesinde Komisyonun AB mevzuatına göre böyle bir anlaşma imzalama yetkisinin olmadığını belirtmesinin yanı sıra, anlaşmanın YİK verilerinin yeterli düzeyde korunmasını öngören maddelerden hala yoksun olduğunu belirtti. Koruma düzeyinin belirlenmesinde verinin aktarım şekli, sebebi ve aktarılmış verinin saklanma süresinin belirtilmesi gerektiği vurgulandı.[50]

2004'te Madrid tren istasyonuna, 2005'te Londra ulaşım ağına yapılan terör saldırıları AB'nin üye ülkelerin güvenliği için veri paylaşımı konusunda hızlı biçimde hareket etmesini sağladı.[51] Bunun üzerine AB ve ABD 2006 yılında geçici bir YİK anlaşması imzaladı.[52] Bir yıl deneme süresinden sonra 2007 yılında yeni bir YİK veri aktarım anlaşması imzalandı[53]. Bu anlaşma 2012 yılında sona ererken taraflar aynı yıl 2019 yılına kadar sürecek bir anlaşma daha imzaladılar. Her bir anlaşma elde edilen tecrübeler ve değerlendirmeler çerçevesinde yeni-

48 ECLI:EU:C:2006:346 Protection of individuals with regard to the processing of personal data – Air transport – Decision 2004/496/EC – Agreement between the European Community and the United States of America – Passenger Name Records of air passengers transferred to the United States Bureau of Customs and Border Protection – Directive 95/46/EC – Article 25 – Third countries – Decision 2004/535/EC – Adequate level of protection. http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1449729

49 Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 28 May 2004. http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf

50 House of Lords-European Union Committee, s.14.

51 Global Business Travel Association, "EU Passenger Name Record (PNR) & Bilateral PNR Agreements", 21 Kasım 2016 tarihinde http://dbta.dk/wp-content/uploads/2015/10/GBTA-ISSUE-TRACKER-EU-PNR-Bilateral-agreements.pdf adresinden erişildi.

52 OJ L 298, 27.10.2006, p. 27–31

53 OJ L 204, 4.8.2007, p. 16–25

lenerek kabul edildi. Örneğin 2003 yılında imzalanan geçici anlaşma, 2004 Anlaşmasına benzemekle beraber veri aktarım yönteminin değiştirilmesi, verinin paylaşılacağı ABD otoritelerinin sınırlandırılması gibi bazı değişiklikleri de getirdi. 2007 Anlaşması, ABD'nin yolcuları (veri sahiplerini) konuyla ilgili bilgilendirme zorunluluğunu getirdi. Ayrıca bu anlaşma aktarılacak veri sayısını 35'ten 19'a indirip yolculara kendi verilerine ulaşma, verilerinin silinmesini talep etme ve gerekirse yasal yollara başvurma haklarını verdi.[54] 2007 Anlaşması çok daha iyi yapılandırılmış, ayrıntılı ve daha çok yolcu haklarını gözeten bir anlaşma olarak değerlendirilebilir. 2012 Anlaşması[55] 8 yıl süren bir serüvenden sonra imzalanmıştır. Bu anlaşma şu anda YİK verilerinin terörle mücadele amacıyla aktarımı, işlenmesi ve saklanması konusundaki en kapsamlı anlaşma olarak kabul edilebilir. Bu sebeple, AB diğer ülkelerle yapacağı olası YİK veri aktarımı anlaşmalarına 2012 Anlaşmasını temel gösteren bir doküman yayımlamıştır. Bu doküman Türkiye ile AB arasında yapılabilecek bir anlaşmaya temel olması açısından önemlidir.

"YİK verilerinin üçüncü ülkelere transferi için Küresel Yaklaşım"[56] dokümanı 2010 yılında AB Komisyonu tarafından hazırlanmıştır. AB'nin böyle bir Küresel Yaklaşıma ihtiyaç duyma sebebi, ABD ile yapılan anlaşmayla başlayan YİK veri aktarımı küresel bir terörle mücadele aracı olarak kullanmak istemesi olarak düşünülebilir.[57] Mevcutta Kanada ve Avustralya ile YİK anlaşması olan AB, 2015'ten beri Meksika ile görüşmelerini devam ettirmektedir. Konu yalnızca AB'nin değil başka ülkelerin de yakın takibi altındadır. Örneğin Japonya, 2020 Tokyo olimpiyatları öncesinde güvenlik önlemlerini artırmak adına havayolu şirketlerinden YİK verilerini isteyeceğini açıklamıştır.[58] Gün-

54 İç Güvenlik Bakanlığı hassas YİK verilerinin filtrelenmesi için bir otomasyon sistemi kullanmakta ve bu verileri sistemden silmektedir.

55 OJ L 215, 11.8.2012, p. 5–14

56 Ibid.

57 Bu istek AB'nin "Roadmap" European Commission Legislative proposal and Communication on the transfer of passenger data to third countries 10/2013 başlıklı bildirisinde dile getirilmiştir. Çevirim içi erişilebilir: http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_home_004_transfer_pnr_data_3rd_countries_en.pdf

58 Japan Times, "Japan to force airlines to hand over personal data on all passengers", 9 May 2015. http://www.japantimes.co.jp/news/2015/05/09/national/japan-to-force-airlines-to-hand-over-personal-data-on-all-passengers/

den güne bu programdan faydalanmak isteyen ülke sayısı artmaktadır. Ülkemizde ise böyle bir iş birliğinden henüz bahsedememekteyiz. Teknik konular bir yana, bu programdan AB tarafında yararlanmak isteyen tüm ülkeler er ya da geç Küresel Yaklaşım dokümanı gerekliliklerini sağlamak durumundadırlar. Ayrıca, ABD ile böyle bir iş birliğine girmek isteyen ülkeler için yine bu doküman güvenli bir temel oluşturabilir. Türkiye'nin terörle mücadeledeki küresel önemi ve ülke içindeki terör olaylarına karşı alınabilecek ek önlemler açısından uluslararası iş birliğinin hem Türkiye hem de Avrupa açısından gerekli olduğuna inanmaktayız. Bu sebeple, Küresel Yaklaşım Türkiye'yi de yakından ilgilendiren bir doküman olarak kabul edilebilir.

6. Avrupa Birliğinin Yolcu İsim Kayıtlarının Aktarımına Küresel Yaklaşımı

Kişisel verilerin terörle ve suçla mücadelede AB tarafından bir istihbarat olarak görülüp başka ülkelerle iş birliği içerisinde elde edilmesi, YİK verileri için de aynı yaklaşımı benimsediklerini göstermiştir. Bu yaklaşımın uluslararası kapsamda daha fazla veri aktarımını gerektireceği aşikardır. Küresel Yaklaşım dokümanı bu veri alışverişi için gerekli asgari yasal şartları gösterdiği için önemlidir.

Küresel Yaklaşım dokümanı ilk defa 2003 yılında hazırlanmasına rağmen zaman içerisinde AB içerisinde değişen gizlilik ve kişisel veri koruma yaklaşımları dokümanın güncellenmesine sebep olmuştur. Güncellenen doküman, üçüncü ülkelerle olası YİK veri alışverişi için gerekli yasal standartları gösterirken aslında AB'ye göre yeterli korumanın ne demek olduğunu da açıklamaktadır.

Küresel Yaklaşıma göre YİK verileri ile İSYB verileri farklı olarak tanımlanmamıştır. İSYB verilerinin teröristleri tanımlamaktan öte bilinen terörist ve suçluları doğrulamaya yönelik olduğunu belirtmiştik. Bu sebeple dokümanda İSYB verileri YİK verilerinin içerisinde düşünülerek bir tutulmuştur. Dokümanda bu iki veri türünün yanı sıra "hassas veri" kavram ve tanımına yer verildiği görülmektedir. Buna göre kişilerin dini, etnik kökeni, siyasi görüşü gibi verileri hassas veri olarak tanımlanmıştır. Bu bilgiler hayati tehlike teşkil eden durumlarda ve gerekli güvenlik önlemleri alındığı sürece aktarılabilmekte ve YİK verisinden ayrı olarak düşünülmektedir. Veriler yalnızca *duruma*

göre, görevi yüksek bir pozisyonda olan görevlinin gözetiminde ve aktarımın asıl gerçekleşme sebebinden asla ayrılmayacak biçimde paylaşılabilmektedir.

YİK verisinin AB'ye göre ne demek olduğunu gördükten sonra, dokümanın temelde üç bölümde incelenebileceği görülmektedir: Veri aktarım ve işleme kuralları; Yolcu hakları, ve Genel kural ve prensipler.

AB ile herhangi bir ülke arasında yapılacak YİK veri aktarımı anlaşmasında yer alması gerek Genel kural ve prensipler şunlardır:

- Gözetim ve hesap verilebilirlik: Bu ilke temelde YİK verilerini elde eden kurumların verilerle ilgili işlemlerinde bağımsız bir otorite tarafından gözlemlenmesini öngörür. Bu otorite Ombudsman veya Veri Koruma Kurulu gibi bağımsız bir kurum olmalıdır.
- Karşılıklılık: İkili anlaşma karşılıklılık ilkesi gereği AB üye devletleri ve Europol, Eurojust gibi AB ajanslarının da karşı taraftan YİK verilerini elde etmelerini ve işleyebilmelerini sağlamalıdır.
- Periyodik gözden geçirme, inceleme ve değerlendirme: Anlaşmanın hem etkili biçimde uygulanabilmesi hem de eksikliklerinin giderilebilmesi için periyodik gözlemlere ve değerlendirmelere ihtiyaç duyulmaktadır. Anlaşma gerektiğinde karşılıklı istişarelerle yeniden düzenlenebilir olmalıdır.
- Anlaşmanın geçerlilik süresi ve anlaşmazlıkların çözümü: Anlaşmanın ne kadar süre yürürlükte olacağı anlaşmada açıkça belirtilmelidir. Tarafların anlaşmanın icrası veya ilgili anlaşmazlıklar karşısında başvurabilecekleri bir mekanizmanın tanımlanması gerekir.

İkili anlaşmanın diğer bir kısmında Veri aktarımı ve işleme kuralları açıklanmalıdır. Veri aktarım kuralları aşağıdaki gibi belirlenmiştir:

- Veri aktarım yöntemi: Verileri talep eden otoriteler verileri istediği zaman istediği şekilde karşı tarafın sistemlerinden çekememeli (pull yöntemi), karşı tarafın kontrolünde verilerin itilmesi (push yöntemi) şeklinde aktarılmalıdır.
- Sınırlamalar: Anlaşmada belirtilen YİK veri alanlarından daha

fazlası aktarılmamalı veya daha fazla verinin gerekliliği söz konusuysa tarafların tekrar anlaşması beklenmelidir.

- Paylaşım Kısıtlamaları: Elde edilen veriler anlaşmada belirtilen otorite, kurum veya kuruluşlar haricinde başka kurumlara aktarılmamalıdır. Bu kural hem ülke içindeki hem de dışındaki yetkisiz birimlere veri akışının engellenmesi için önemlidir. Ancak anlaşma dışında kalan başka bir ülkeye veri aktarımı şartsa, o ülkede Küresel Yaklaşım kurallarına uyulduğunun kanıtlanması halinde veri aktarımı gerçekleştirilebilir.

YİK verilerinin nasıl kullanılması gerektiğini gösteren İşleme kuralları aşağıdaki şekildedir:

- Verilerin saklanma süresi: Verilerin veri tabanlarında ne kadar süreyle saklanacağının mutlaka belirtilmesi gerekmektedir. Veriler gerek görülen zamandan daha fazla elde tutulmamalıdır.
- Veri güvenliği: Veri güvenliğinin sağlanması için gerekli tüm teknik tedbirler alınmalıdır. Verilerin dışarı sızmaması, amaç dışı kullanılmaması ve verilere yasa dışı erişimin engellenmesi için gerekli tüm tedbirler alınmalıdır.
- Otomatik Karar Mekanizması: YİK veri işleme sistemleri yolcular hakkında önemli kararların (sorgulama, yargılama gibi) verilmesine yardım etmeli ancak, tek başlarına karar verici sistemler olarak kullanılmamalıdır. Verilerin belli listelerdeki profillere göre sistem içi değerlendirmesi yapıldıktan sonra mutlaka insan gücünün dahil olması ve kararların insanların yaptığı analiz sonucu alınması gerekir.

Anlaşmada olması gereken son kısım ise verilerin sahibi olan kişilerin haklarının yani Yolcu Haklarının belirlenmesidir. Bu haklar:

- Şeffaflık ve Bilgilendirme: Yolcular verilerinin neden, nerede ve nasıl işleneceği hakkında ayrıntılı biçimde bilgilendirilmelidir. Bilgiler aynı zamanda yolcuların haklarını nasıl ve nerede arayacaklarını içermelidir. Bilgilendirme hava yolları şirketleri tarafından yapılabileceği gibi verileri talep eden kurumlar tarafından da yapılabilir.
- Erişim, düzeltme ve silme talebi: Tüm yolcular kendi verilerine

erişme, verilerini düzeltme ve silinmesini talep etme hakkına sahip olmalıdır.

- Tazminat: Şeffaflık ilkesinde belirtilen hakların aranması konusunda bilgilerin toplanış amacı dışında kullanılmaması veya korunamaması üzerine hangi mahkemelerin yetkili olduğu açıkça belirtilmelidir.

Sonuç olarak Küresel Yaklaşım dokümanında belirtilen tüm standartların AB'nin veri koruma mevzuat ve uygulamalarıyla uyumlu olduğu gözlenmiştir. Anlaşma içeriği taraflarca değiştirilebilir veya geliştirilebilir ancak AB ve Türkiye arasındaki olası YİK anlaşmasının standart olarak bu dokümanı temel alacağı kesindir.

7. Olası Türkiye-AB YİK Veri Aktarımı Anlaşması

Avrupa'nın en kalabalık ve en büyük ülkelerinden biri olan Türkiye, coğrafi konumu açısından Asya, Avrupa ve Afrika kıtasına bağlantısı olan tek ülkedir. Coğrafi konumunun etkisiyle örneğin yalnızca 2015yılında[59] yaklaşık 100 milyon uluslararası yolcu, 623.715 kez yapılan hava trafiği ile Türkiye üzerinden geçmiş veya Türkiye'ye gelmiştir. Bu yaklaşık 100 milyon verinin de Türkiye'ye uçtuğu anlamına gelmektedir. 2011 yılından beri 128 ülkeden yaklaşık 38 bin kişinin ülkeye girişi reddedilmiş; bunlardan 2016 Brüksel teröristi İbrahim el Bakraou'nin de içinde bulunduğu 3 bin kişi, terörist veya terör örgütleriyle ilişkisi olması sebebiyle ülkeye kabul edilmemiştir.[60]

Türkiye'nin coğrafi konumundan oldukça etkilenen güvenlik durumu, komşu ülkelerde devam etmekte olan iç savaşlar ve siyasi anlaşmazlıklar sebebiyle şimdi çok daha zor bir durumdadır. IŞİD olarak bilinen terör örgütü sadece Türkiye'nin değil Avrupa devletlerinin de güvenliğini tehdit etmektedir. Türkiye Cumhuriyeti Hükümetinin Iraklı ve Suriyeli insanların hayatını kurtarmak için iyi niyetle başlattığı mülteci programları ülkeye milyonlarca masum mültecinin girmesini

59 Türkiye İstatistik Kurumundan konuyla ilgili daha fazla istatistiğe göz atmak için: http://www.tuik.gov.tr/PreTablo.do?alt_id=1051 23 Kasım 2016 tarihinde ziyaret edildi.

60 Sertaç Bulur, "Türkiye'nin yabancı terörist savaşçılarla mücadelesi", Anadolu Ajansı, 24.03.2016 tarihli haber. http://aa.com.tr/tr/turkiye/turkiyenin-yabanci-terorist-savascilarla-mucadelesi-/543046?amp=1

sağlarken belki de teröristlerin de girmesini engelleyememiştir. Çevre ülkelerden Türkiye'ye giren mülteci ve göçmenlerle artan terör olayları arasındaki ilişki kesin biçimde kanıtlanamasa da teröristlerin sadece kara yoluyla değil hava yoluyla da ülkeye giriş yaptığı bilinmektedir. Giriş kısmında belirttiğimiz terör olayları ile ilgili sayıları hatırlayarak, Türkiye'nin 2015'ten beri yoğun bir terör tehdidinde olduğunu tekrarlayabiliriz. Bazen neredeyse her iki haftada bir gerçekleşen saldırılar komşu ülkelerde de aynı sıklık ve şiddetle gözlenmiştir. Saldırıların hep ülke dışında değil ülke içinde de planlanıp gerçekleştirildiği bilinse de biz bu çalışmada dışarıdan gelecek tehditlere karşı AB/ABD-Türkiye YİK veri aktarımını ek bir güvenlik önlemi olarak önereceğiz.

7. Türkiye'de Kişisel Verilerin Korunması Mevzuatı

Kişisel verilerin korunması hakkı 2010 yılında gerçekleşen anayasa referandumunda 1982 Anayasasına 8. madde olarak eklenmiştir.[61] Kişisel Verilerin Korunması Kanunu'nu bu referandumdan 6 yıl sonra kabul edebilen ülkemiz aslında 108 Sayılı Sözleşmeyi ilk imzalayan ülkelerdendir. Ancak 1981'de imzalanan bu Sözleşmenin mevzuata girmesi yaklaşık 30 yıl sürmüştür. Bu süre zarfında yapılan bazı çalışmaların etkisiz kaldığı bir gerçektir. Konuyla ilgili 2000 yılına kadar herhangi bir anayasa maddesi teklifi yapılmamış, 2000 yılından sonra ise AB'deki gelişmelere paralel olarak bir hareketlilik gözlenmiştir.[62] Çünkü 2000 yılında AB Temel Haklar Şartı kabul edilmiş, 2009 yılında ise tüm AB kurum ve üyelerinde insan haklarının gözetimi için yasal temel haline getirilmiştir. Şartın 8. maddesi kişisel verilerin korunması hakkını ayrı bir satırda göstermesi bakımından önemlidir. AB'ye aday ülkelerden biri olan Türkiye'nin bu gelişmelerden etkilendiği düşünülmektedir.

Türkiye ile AB arasında pembe dizileri aratmayacak ilişki 1959'den beri devam etmektedir.[63] Bu uzun sürede Türkiye gerçekten de AB ile

---

61 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete

62 Elif Küzeci, "Kişisel Verilerin Korunması", Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Doktora Tezi, 2010, s.285. https://tez.yok.gov.tr/UlusalTezMerkezi/

63 Türkiye'nin AB üyelik süreci ile ilgili kısa tarihçeye Avrupa Komisyonu'nun Avrupa Komşluk Politikası ve Genişleme web sitesinde erişilebilir: http://ec.europa.eu/enlargement/countries/detailed-country-information/turkey/index_en.htm

uyumlu olma adına önemli adımlar atmış, bu adımların bazıları başarılı bazıları başarısız olmuştur. Bazı adımların atılması ise zaman almıştır. AB Türkiye ilerleme raporlarına göz atıldığında uzun zaman alan başarı hikayelerinden birinin de veri koruma olduğu görülmektedir. 1998 ile 2015 yıllarında Türkiye ile ilgili yayınlanan her raporda,[64] Türkiye'de bir veri koruma yasasının olmadığı tekrar edilmiştir. 1999'da yayınlanan ilk Düzenli Rapor, konuya İç Pazar (Internal Market) değerlendirmesi olarak yaklaşmaktadır. Sonrasında "veri koruma kanunun ve bağımsız bir veri koruma kurulunun eksikliği" her Düzenli Rapor ve İlerleme Raporunda karşımıza çıkar. Raporlarda ticaret alanında, ilaç sektöründe; gizliliğin korunması hakkı ve aile yaşamına saygı konusunda; vizelerin kaldırılması, gümrük birliği (veya iş birliği) ve iletişim konularında zaman zaman veri koruma ile ilgili yasal eksikliğe değinildiği görülmektedir. Ancak raporlarda bahsedilen ve çalışmamızla en ilişkili olan konu şüphesiz 2008-2015 yılları arasındaki tüm raporlarda tekrarlanan "terörle ve organize suçlarla mücadelede uluslararası iş birliği ve uluslararası yargı iş birliği"[65] konusudur. Raporlara göre Türkiye, AB ajanslarından Europol ve Eurojust ile veri koruma mevzuatının zayıflığı sebebiyle iş birliği yapamamaktadır. Bu gerçeğin Türkiye'de terörle mücadelede bazı somut adımların atılamamasına sebep olduğunu düşünmekteyiz.

Kişisel Verilerin Korunması Yasası'nın kabulüne kadar geçen zamanda Türkiye'de elbette veri koruma ile ilgili düzenlemeler yer almaktaydı.[66] Türk Ceza Kanunu, Dokuzuncu Bölüm ve 135, 136, 137, 138 ve 139. maddelerinde kişisel verilerin hukuka aykırı olarak kaydedilmesi, yok edilmemesi ve nitelikli haller gibi durumlarda verilecek cezaları düzenlemektedir. Türk Medeni Kanunu'nun 23. maddesine göre kişisel veriler kişiliğin bir parçası olarak görülmekte ve biyolojik veya genetik bilgiler ancak kişilerin yazılı rızası ile alınabilmektedir.

---

64 European Commission, Regular Report from the Commission on Turkey's Progress Towards Accession, 1998, s.45. European Comission, Turkey 2015 Progress Report, s.5. Tüm raporlar yıllık olarak yayımlanmkta olup, çevirim içi erişilebilir: European Commission, 'Enlargement Policy Strategy and Reports' https://ec.europa.eu/neighbourhood-enlargement/countries/package_en

65 European Commission, Turkey 2008 Progress Report, s.73. European Commission, Turkey 2015 Progress Report, s.20.

66 Mehmet Bedii Kaya ve Furkan Güven Taştan, "Veri Koruma Hukuku: Mevzuat&İçtihat", Sinerjik.org, 2010. http://www.sinerjik.org/veri-koruma-hukuku/

Ceza Muhakemesi Kanunu, Medeni Kanun gibi, 80. maddesinde Genetik inceleme sonuçlarını kişisel veri niteliğinde saymakta ve bu bilgilerin amacı dışında kullanımını kısıtlamaktadır. Saydığımız kanunların hiçbirisinde, verilerin yurt dışına aktarımı ile ilgili bir düzenleme geçmemektedir.

Bu kanunlara ek olarak kişisel verilerin korunması hakkını çeşitli sektörler içerisinde tek tek düzenleyen yönetmelikler bulunmaktadır. Bu sektörler: Bilgi ve İletişim Teknolojileri,[67] bankacılık,[68] sağlık,[69] ticaret[70] ve kamu sektörüdür.[71] Farklı alanlarda aynı konuyu farklı yaklaşımlarla çözmeye çalışan mevzuatın bütünleştirilmesi gerekliliği açıktır. Yine de bu düzenlemelerin Türkiye'de kişisel verilerin korunması konusunda belli bir altyapı sağladığı söylenebilir.

Kişisel Verilerin Korunması Kanunu 2010 yılında Türkiye Cumhuriyeti Anayasası'nın Özel hayatın gizliliği başlığı altında 20. maddesi çerçevesinde kabul edilmiştir. Anayasada ifade edildiği şekliyle kişisel verilerin korunması hakkı:

"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

---

67 23.05.2007 tarih ve 26530 sayılı Resmi Gazetede yayımlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun; 23/1/2004 tarih ve 25355 sayılı Resmi Gazetede yayımlanan 5070 sayılı Elektronik İmza Kanunu; 24.10.2003 tarih ve 25269 sayılı Resmi Gazetede yayımlanan 4982 sayılı Bilgi Edinme Hakkı Kanunu; 10.11.2008 tarih ve 27050 sayılı Resmi Gazetede yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu; 28.07.2010 tarih ve 27655 sayılı Resmi Gazetede yayımlanan Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği.

68 01.03.2006 tarih ve 26095 sayılı Resmi Gazetede yayımlanan 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu; 07.04.2001 tarih ve 24366 sayılı Resmi Gazetede yayımlanan 6740 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanunu.

69 01.08.1998 tarih ve 23420 sayılı Resmi Gazetede yayımlanan Hasta Hakları Yönetmeliği.

70 05.11.2014 tarih ve 29166 sayılı Resmi Gazetede yayımlanan 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun.

71 18.11.2005 tarih ve 25997 sayılı Resmi Gazetede yayımlanan 5429 sayılı Türkiye İstatistik Kurumu Kanunu; 23.05.2013 tarih ve 28655 sayılı Resmi Gazetede yayımlanan 6425 sayılı Posta Hizmetler Kanunu; 10.06.2003 tarih ve 25134 sayılı Resmi Gazetede yayımlanan 4857 sayılı İş Kanunu; 20.05.2006 tarih ve 26173 sayılı Resmi Gazetede yayımlanan 5502 sayılı Sosyal Güvenlik Kurumu Kanunu.

hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Kanunu ayrıntılı biçimde incelemek, Kanundaki veri aktarımı ile ilgili düzenlemeleri görebilmek açısından faydalı olacaktır.

a) Kişisel Verilerin Korunması Kanunu

Kanun akademik çevrelerce ilk bakışta her ne kadar yakın zamanda yürürlükten kalkacak da olsa AB'nin 95 Direktifi ile 108 Sayılı Sözleşme'nin bir harmanı olarak değerlendirilmektedir.[72] Kanunun Avrupa mevzuatı örnek alınarak hazırlanmış olması Türkiye'nin bu alanda en gelişmiş mevzuatı göz önünde bulundurması açısından olumludur. Türkiye'nin AB Genel Veri Koruma Tüzüğü karşısında nasıl bir tepki vereceği bilinmemekle birlikte, bir Veri Koruma Kanunun kabul edilmiş olmasının başlı başına önemli bir adım olduğunu söyleyebiliriz. Ancak Türkiye'nin Kanun hazırlık aşamasında neden Tüzüğü es geçtiği başka bir çalışmanın konusu olabilir.

Kanun AB'nin 95 Direktifine benzer şekilde, 7 Bölüm ve 33 maddeden oluşmaktadır.[73] İlk Bölümde Kanunun amacı, kapsamı ve Kanunda geçen temel terimlerin tanımı yapılmıştır. Kanunun 3. maddesinin birinci fıkrasının (d) bendine göre kişisel veri "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Ayrıca Kanunda Özel nitelikli kişisel veri ayrımı ve tanımı yapılmıştır. Kanunun 6. maddesine göre "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, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyomet-

72 İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme." *T*ürkiye Barolar Birliği Dergisi 124, 2016: 81–152. http://tbbdergisi.barobirlik.org.tr/m2016-124-1571 Gökhan Uğur Bağcı, "14 Soruda Kişisel Verilerin Korunması Kanunu", E-ticaret ve internet hukuku, 10 Mayıs 2016. http://www.eticarethukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu#more-176 Fevzi Toksoy, Bahadır Balkı ve Sera Erzene Yıldız, "Data Protection in Turkey: Overview" Practical Law Multi-Jurisdictional Guide 2016/17 Data Protection 2016. http://us.practicallaw.com/7-520-1896?q=turkey
Zihni Bilgehan ve Yusuf Mansur Özer. "Turkey, Data Protection 2016", ICLG, 9 Mayıs 2016. https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/turkey#chaptercontent1

73 Direktifte 7 Bölüm ve 34 Madde bulunmaktaydı.

rik ve genetik verileri özel nitelikli kişisel veri" olarak tanımlanmıştır. Tanımlar hangi çerçevede kişisel verilerden bahsettiğimizi anlamamız açısından önemlidir.

Her iki tür veri için geçerli genel kural, verilerin ilgili kişinin açık rızası olmadan işlenemeyeceğidir. Açık rıza kavramı Kanunun 3. maddesi (a) bendine göre "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" olarak tanımlanmıştır. Bu tanıma göre eğer ilgili kişinin bilgisi dahilinde verileri işlenmişse, işleyen kişi veya kurumun Kanunu ihlal edeceği anlamı ortaya çıkmaktadır. Açık rıza kavramı, Kişisel Verileri Koruma Kurulu tarafından hazırlanan kitapçıklarda açıklanmıştır.[74]

Kanun veri işleme ile ilgili temel prensipleri, koşulları ve istisnaları, veri işleyenlerin sorumluluklarını ve haklar ve yükümlülükleri açıklamaktadır. Kanunda, Kanunun kabulünü takiben 6 ay içerisinde kurulması öngörülen Kişisel Verileri Koruma Kurulu'na da ayrıntılı biçimde yer verilmiştir. Kanun Nisan 2016'da kabul edilmiş ancak Kurul üyeleri 12 Ocak 2017'de yeminlerini ederek görevlerine başlamıştır.[75]

Kişisel Verilerin Korunması Kanunu'nun şüphesiz göz atılması gereken birçok önemli kısmı vardır ancak çalışmamız kapsamında yalnızca Kanunun 9. maddesi olan "Kişisel verilerin yurt dışına aktarılması" üzerinde duracağız.

b) Kişisel Verilerin Yurt Dışına Aktarılması

Kanunun 9. maddesinin birinci fıkrası uyarınca kişisel verilerin yurt dışına aktarımı için ilgilinin açık rızası olması gerekmektedir. Ancak bazı durumlarda ilgilinin açık rızası aranmayabilir. Bu durumlar Kanunun 5. maddesinin ikinci fıkrasında belirtilen "Kişisel verilerin işlenmesi" kuralları ile aynıdır:

- Kanunlarda açıkça öngörülmesi.
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin ken-

74 http://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf
75 http://kvkk.gov.tr/haber-kuruluyelerigorevebasladi.html

disinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kanun ışığında YİK verilerinin aktarılması için ilk gerekli şart, aktarımın Kanunlarda açıkça öngörülüyor olması gerekliliğidir. Mevcutta, YİK veri aktarımını öngören herhangi bir kanun veya Türkiye'nin taraf olduğu herhangi bir uluslararası anlaşma bulunmamaktadır. Kanunun 5. maddesinin ikinci fıkrasının (ç) bendinde veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi veri aktarımı yapabileceği öngörülmektedir. Örneğin ABD hukuku karşısında Türk hava yolları şirketlerinin sorumluluğunu yerine getirebilmek için veri aktarımı yapma durumunda kalması bu kapsamda örnek verilebilir. Burada dikkatimizi çeken husus ise AB'nin ABD otoriteleri ile ilgili yaşadığı endişelerin Türkiye tarafından da değerlendirilmesi gerektiği gerçeğidir. O halde Türk hava yolları şirketlerinin YİK verilerini eksik bir hukuki zeminde aktarıldığını söylememiz yanlış olmayacaktır. Kanaatimiz, Türkiye'nin bu eksikliği ancak bir YİK anlaşması ile doldurabileceği şeklindedir.

Hassas kişisel verilerin yurt dışına aktarılması için gereken koşul 6.Maddenin Üçüncü fıkrasında düzenlenmiştir. Buna göre sağlık ve cinsel hayat dışındaki hassas kişisel veriler, yani kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri kanunlarda öngörülen hâllerde ilgili kişinin açık rıza-

sı aranmaksızın işlenebilir. Burada tekrar YİK verilerinin yurt dışına aktarılması ile ilgili herhangi bir mevzuatın olmadığını belirtmemiz gerekir.

Kanunun 9. maddesinin 3, 5 ve 6. fıkrasında Kişisel verilerin yurt dışına aktarılması kuralları devam etmektedir. Maddenin üçüncü fıkrasına göre Kişisel Verileri Koruma Kurulu (Kurul) verilerin aktarımı için güvenli ülkelerin listesini duyuracaktır. Kurul henüz bu duyuruyu yapmadığı için örneğin YİK verilerinin güvenli olmayan ülkelere hala aktarılıyor olma olasılığı sürmektedir. 9. maddenin beşinci fıkrasına göre Türkiye'nin veya ilgili kişinin veri aktarımı sebebiyle menfaatlerinin zarar göreceği ihtimaline karşı verilerin aktarılma durumuna, ilgili kurum ve kuruluşların görüşü ışığında Kurul karar verecektir. Kişisel verilerin yurt dışına aktarılması ile ilgili diğer kanun hükümlerinin saklı olduğu 9.maddenin altıncı fıkrasında belirtilmiştir.

Çalışmamız açısından Kanunda en önemli olan madde 9.maddenin dördüncü fıkrasıdır Buna göre kişisel verilerin yurt dışına aktarımı ancak verinin aktarılacağı ülke tarafından yeterli koruma sağlanması şartıyla yapılabilir. Hatırlayacak olursak, ABD ile AB arasındaki bazı YİK veri aktarımı anlaşmaları tam olarak bu şart yüzünden iptal edilmiş veya yetersiz kalmıştır. Kurulun bu noktada hızlı biçimde çalışmalarına başlaması çok önemlidir, çünkü Türkiye'den (kamu veya tüzel kişilerden) kişisel veri talep eden herhangi bir ülkede yeterli koruma bulunup bulunmadığını yalnızca Kurul belirleyebilecektir. İşte 9.Maddenin dördüncü fıkrası yeterli koruma ilkelerini belirlemesi açısından bu yüzden çok önemlidir. Kurul bir ülkede yeterli koruma sağlanıp sağlanmadığını şu hususlara göre değerlendirecektir:

- Türkiye'nin taraf olduğu uluslararası sözleşmelere bakılacaktır. Ülkemizin uluslararası alanda yalnızca 108 Sayılı Sözleşme 'ye taraf olduğunu belirtmiştik. Bu sözleşme YİK veri aktarımı için belki taraf devletler için yeterli ancak AB için yeterli olmayacaktır. AB Küresel Yaklaşım dokümanı ile nasıl bir YİK anlaşması yapılabileceğini zaten göstermiştir.
- Aktarılacak verinin kullanım amacı, kapsamı ve süresine bakılacaktır.
- Kişisel verilerin aktarılacağı ülkenin konuyla ilgili kendi mevzuat

ve uygulamaları ile veri sorumlusunun taahhütlerine bakılacaktır. Her ülkede gizliliğin ve kişisel verilerin korunması ile ilgili yaklaşımın aynı olmadığını, bunun mevzuata ve uygulamalara da yansıdığını ABD ile AB arasındaki olaylardan hatırlayabiliriz.

- Kişisel veri aktarımı konusunda karşılıklılık ilkesi göz önünde bulundurulacaktır. Çalışmamız açısından en önemli sayılabilecek nokta karşılıklılık ilkesidir. ABD ile AB örneğinde olduğu gibi ikili veya çok taraflı veri aktarma anlaşmalarında bu ilkenin mutlaka konmuş olması önemlidir.

Kanunda geçen tüm kurallar kişisel verilerin yurt dışına aktarımı ile ilgilidir. Ancak Kanunda aktarımla ilgili ayrıntılı teknik bilgi bulunmamakta ve aktarımdan sonra verilerin korunması ile ilgili kısıtlı bir bilgi bulunmaktadır. Bu sebepler YİK veri aktarımı için ABD ve AB arasında olduğu gibi ikili anlaşmaların gerekliliğini ortaya çıkmaktadır. Özellikle AB ile yapılacak olası bir YİK anlaşması için Türkiye'de Küresel Yaklaşıma göre bir temel hazırlanmalıdır. Aslında Türkiye'nin örgütlü suçlar ve terörle mücadele kapsamında bazı AB devletleri ve ABD halihazırda anlaşması bulunmaktadır. Bu anlaşmalar terörle ve suçla mücadelede kişisel veri değişimi ile ilgili maddeleri bulunması bakımından önemlidir. Bu anlaşmaları Küresel Yaklaşıma göre inceleyip değerlendirmeye çalışacağız.

b) Türkiye'nin Terörle ve Suçla Mücadele Alanında Başka Ülkelerle Yaptığı İşbirliği Anlaşmalarında Kişisel Veri Aktarımının Yeri

Türkiye Cumhuriyeti Hükümeti ile Polonya Cumhuriyeti Hükümeti Arasında Örgütlü Suçlar, Terörizm ve Diğer Suçlarla Mücadelede İşbirliği Anlaşması[76] 2003 yılında organize suçlar, terörle mücadele ve diğer suçlarla mücadelede iş birliği yapmak amacıyla imzalanmıştır. Polonya'nın terör örgütü PKK'nın yoğun olarak konuşlandığı Almanya, İsviçre, Danimarka ve Hollanda gibi ülkelerle bu ülkelerin doğusunda kalan diğer ülkeler arasında köprü konumunda bulunması sebebiyle böyle bir anlaşmanın faydalı olacağı düşünülmüştür. Ayrıca Polonya'nın PKK gibi terör örgütlerine ve terör olaylarına karşı duyar-

[76] 15.06.2004 tarihli ve 25493 sayılı Resmi Gazete

lı bir ülke olduğu bilinmektedir. Bu anlaşma Polonya ve Türkiye'nin terörle mücadeledeki ciddiyetini, kişisel veri paylaşımının ise ciddi bir güvenlik önlemi olarak algılandığını göstermektedir. Anlaşmada veri aktarımının yapılacağı otoriteler belirtilmiş, bunlar dışındaki otoritelere veya taraf ülkeler dışına veri aktarımı yapılması gerektiğinde taraflar arasında yazılı bir izin gerektiği vurgulanmıştır. Böylelikle verilerin anlaşma haricindeki kurumlara ve taraf olmayan ülkelere aktarımı ile ilgili düzenleme anlaşmada yer almıştır. Anlaşmada kişisel verinin ne olduğu ile ilgili dar bir tanım yapılmamış "kişilere ait tüm bilgiler" şeklinde bir tanım yapılmıştır. Bu bilgilerin yalnızca amacına uygun aktarılması ve kullanılması gerektiği vurgulanmıştır.

Anlaşmaya göre taraflar aktarılan bilgilerin doğruluğu ve güvenliğinden sorumludur. Bu kapsamda taraflar, yetkisiz kişilerin veriye erişimini, verilerin değiştirilmesini veya verilerin açıklanmasını engelleme adına gerekli önlemleri almalıdırlar. Bu önlemler veri güvenliği ile ilgili alınan teknik ve idari önlemler olarak yorumlanabilir. Yeterli düzeyde korumanın her iki taraf için ne anlama geldiği bu anlaşma içerisinde çok açık olmasa da, tarafların yürürlükteki mevzuatları ve uluslararası anlaşmaların bağlayıcı nitelikte olduğu belirtilmiştir. Verilerin aktarımında hangi yöntem izleneceği bilinmemekte ancak verilerin bilgisayar dosyaları şeklinde aktarılacağı anlaşılmaktadır. Verilerin sistemlerde tutulma süresi için herhangi bir süre belirtilmemiş ve verileri aktarılan kişilerin konuyla ilgili bilgilendirilmesi öngörülmemiştir. Bu iki durum Küresel Yaklaşım kriterleri ile çelişmektedir. Anlaşma kapsamında iki ülke arasında YİK verilerinin aktarılıp aktarılamadığı bilinmese de bunun için bir zemin hazırlıyor olması önemlidir.

Türkiye Cumhuriyeti Hükümeti ile Slovenya Cumhuriyeti Hükümeti Arasında Örgütlü Suçlar, Uyuşturucu Madde Kaçakçılığı, Uluslararası Terörizm ve Diğer Ciddi Suçlarla Mücadelede İşbirliği Anlaşması[77] 2004 yılında Slovenya'nın Türkiye üzerinden Avrupa'ya doğru uyuşturucu ve insan kaçakçılığı olaylarından fazlaca etkilenen bir ülke olması sebebiyle imzalanmıştır. Anlaşmanın temel amacı uyuşturucu ve insan kaçakçılığını önlemek olsa da anlaşmada suç ve terörle mücadele konularına da yer verilmiştir. Bu anlaşma yukarıda açıkladığımız Türkiye-Polonya anlaşmasından çok farklı değildir, ancak bazı farklı

77 27.10.2004 tarihli ve 25626 sayılı Resmi Gazete

yönler tarafımızca tespit edilmiştir. Anlaşmada verileri aktarılan kişilerin konuyla ilgili bilgilendirilmesi gerektiği ifade edilerek şeffaflık ilkesi vurgulanmıştır. Ayrıca, verilerin korunması konusunda 108 Sayılı Sözleşme ilkelerinin bağlayıcılığı kabul edilmiştir. Verilerin ne kadar süre için tutulacağı ve nasıl yok edileceğinin belirtilmemesi, Küresel Yaklaşım kriterlerine uygun değildir.

Türkiye 2005 yılında Bulgaristan ile Polis İşbirliği anlaşması[78] imzalamıştır. Bu anlaşma veri aktarımı kriterleri bakımından Polonya ve Slovenya anlaşmalarına oldukça benzemektedir. Örneğin, şeffaflık ilkesi; verilerin amaç ve kapsam çerçevesinde kullanımı, verileri alan otoritenin verilerin doğruluğu ve güncelliğinden sorumlu olması; verilerin yetkisiz kişilerce erişiminin yasak olması gibi kriterler bu anlaşmalardaki ortak kriterlerdendir. Bulgaristan anlaşmasında farklı olarak verilerin yok edilmesi ile ilgili kuralların ayrıntılı olarak açıklandığı görülmektedir. Buna göre, eğer taraflardan biri verilerin kapsam dışı kullanıldığını veya verilerin güncel olmadığını tespit ederse, verileri yok edebilmektedir. Aksi halde verileri tarafların sistemlerinde zaman sınırı olmaksızın kalabilmektedir.

Türkiye Cumhuriyeti Hükümeti ile Finlandiya Cumhuriyeti Hükümeti Arasında Suçun Önlenmesi ve Suçla Mücadelede İşbirliği Anlaşması[79] 2004 yılında imzalanmıştır. Anlaşmanın 4. maddesine göre taraflar, kişisel veri aktarımları için kendi mevzuatlarındaki kurallara ve uluslararası anlaşmalara uyacaktır. 2004 yılında Türkiye'de kişisel verilerin korunması ile ilgili herhangi bir düzenleme bulunmamakta ve hatta gizlilik kavramını bile ayrı bir maddede ele almamış 1926 tarihli Ceza Kanunu yürürlükte idi. Konuyla ilgili tek yasal dayanak Medeni Kanun olmakta bunun haricinde 108 Sayılı Sözleşme de o tarihte henüz geçeli değildi. Bu durumda iki ülke arasında YİK veri aktarımının, eğer gerçekleşmişse, belli bir yasal temele dayanarak gerçekleşmediği söylenebilir.

Türkiye'nin 2004'te Europol ile teknik ve stratejik bilgi değişimi yardımıyla suçların tanımlanması, kontrol edilmesi ve önlemlerin alınmasını öngören bir İşbirliği Anlaşması imzalamıştır.[80] Ancak bu

78 03.06.2005 tarihli ve 25834 sayılı Resmi Gazete
79 29.08.2004 tarihli ve 25568 sayılı Resmi Gazete
80 15.07.2004 tarih ve 25523 sayılı Resmi Gazete

anlaşma Türkiye'de bir veri koruma kanununun olmaması sebebiyle yürürlüğe girememiştir. Anlaşmada iş birliği kapsamında kişisel verilerin aktarımının anlaşma dışında tutulduğunu belirten bir maddenin olması konuyu açıkça ortaya koymaktadır. Ancak Emniyet Genel Müdürlüğünün Interpol-Europol-Sirene Dairesi Başkanlığı web sitesinde Kişisel Verilerin Korunması Kanunun kabulü sonrasında olumlu bir gelişme olarak konu ile ilgili girişimlerde bulunulduğu haberine yer verilmiştir.[81]

Türkiye ile ABD arasında 2000 yılında imzalanan ve Nisan 2001'de yürürlüğe giren Hava Taşımacılığı Anlaşması'nın[82] asıl amacı iki ülke arasındaki hava taşımacılığını standart ve eşitlik çerçevesinde gerçekleştirebilmektir. Anlaşma daha çok ticari bir anlaşma olmasına rağmen Bilgisayarlı Rezervasyon Sistemlerinin ve bu sistemler içindeki bilginin eşit, rekabetçi ve iş birliği çerçevesinde kullanılması ile ilgili konulara yer vermiştir. Anlaşmanın 7. maddesine göre iki ülke arasında güvenli uçuşların yapılabilmesi için gerekli bazı kurallar vardır. Havacılık Güvenliği başlığı altında iki ülkenin birbirlerinin mevzuatlarına uygun hareket edecekleri, aynı zamanda yolcular uçağa binmeden veya bagajlar yüklenmeden önce kabin ekibi ile yolcuların kendilerinin, özel eşyalarının ve bagajlarının bir güvenlik önlemi olarak kontrol edileceği belirtilmiştir. Bu anlaşma direkt olarak YİK aktarımından bahsetmemekte ancak buna zemin hazırlamaktadır. İlerleyen bölümde Türkiye'de bulunan havayolları firmalarından ABD'li otoritelere kişisel verilerin aktarıldığını göreceğiz.

Yukarıda saydığımız bütün anlaşmalar terörle mücadele kapsamında kişisel veri, bilgi ve tecrübe paylaşımını gerekli ve önemli gören anlaşmalardır. YİK verilerinin bu anlaşmalar kapsamında aktarılması olasıdır, ancak anlaşmaların hiçbiri AB Küresel Yaklaşım kriterlerini tam olarak karşılamamaktadır. Çünkü bu anlaşmalar verilerin amaç ve kapsamı dışında kullanılmaması, veri güvenliği ile ilgili bazı kurallar, şeffaflık, paylaşım kısıtlamaları ve gözden geçirme kurallarından bahsetmesi dışında aşağıdaki noktalarda noksan kalmıştır:

81 http://www.interpol.pol.tr/Sayfalar/turkeuropoliliski.aspx
82 09.05.2001 tarihli ve24397 sayılı Resmi Gazete

- Hesap verilebilirlik ve gözetim,
- Anlaşmazlıkların çözümü,
- Veri aktarımı yöntemi,
- Otomatik Karar Mekanizması,
- Erişim, düzeltme ve silme talebi,
- Tazminat,
- Gözetim ve hesap verilebilirlik,
- Sınırlamalar,
- Paylaşım Kısıtlamaları,
- Verilerin saklanma süresi,
- Kişisel verileri aktarılanları bilgilendirme.

Hemen belirtmek gerekir ki bu anlaşmalar aslında daha çok bilgisi bir yerlerde kayıtlı şekilde bilinen suçlu veya teröristlerin yakalanmasında uluslararası bir iş birliğine yöneliktir. Türkiye'nin terörle mücadelede bu gibi anlaşmalardan çok daha fazlasına ihtiyacı olduğunu göz önünde bulundurmakla beraber yasalara ve insan haklarına dayanan her uygulamanın ülkenin yararına olacağını düşünmekteyiz. Bu anlaşmaların YİK veri aktarımına izin verip vermediği net olmamakla birlikte konu terör olduğunda bu tür ek güvenlik önlemlerinin göz ardı edilmemesi gerektiği açıktır. Anlaşmaların Avrupa kısmı 2004-2006 yıllarında imzalanmış, ABD anlaşması ise 9/11 olaylarından önce imzalanmıştır. Geçen süre içerisinde teknolojik gelişmelerin, terör algı ve anlayışının, kişisel veri mevzuatının dünyada değişmiş olduğu kesindir. Bahsedilen anlaşmalar çerçevesinde Türkiye'nin kişisel veri alışverişi yapıp yapmadığını pratikte bilemiyoruz ancak Türkiye terörle mücadele konusunda her türlü adımı atmak zorunda olan bir ülke olarak dünyadaki her türlü gelişmeyi takip etmek durumundadır. Sonuç olarak ülkemizde YİK verilerinin Küresel Yaklaşım dokümanında öngörülen kriterler çerçevesinde karşılıklı aktarımını sağlayacak ayrı bir anlaşma veya anlaşmalara ihtiyaç duyulmaktadır

c) Türk Havacılık Mevzuatında Kişisel Verilerin Yurt Dışına Aktarılması

Daha önce de aktardığımız üzere, ülkemizde Kişisel Verilerin Korunması Kanunundan önce kişisel veriler, farklı alanlarda karşımıza çıkan mevzuatla düzenlenmiştir. Bu yüzden konu havacılık olduğu için kişisel verilerin yurt dışına aktarımı konusunda Türk havacılık hukukuna da bakmamız gerekir. Konu ile ilişkisi olduğunu düşündüğümüz iki Yönetmelik bulunmaktadır: Havayolu ile Seyahat Eden Yolcuların Haklarına İlişkin Yönetmelik[83] ve Havayolu Taşıyıcılarının Yükümlülükleri Yönetmeliği.[84]

Havayolu ile Seyahat Eden Yolcuların Haklarına İlişkin Yönetmelik'in amacı "havayolu ile seyahat eden yolcuların sahip olduğu haklar ve bu hakların geçerli olduğu durumlar ile yolcuların uçağa kabul edilmediği, uçuşlarının iptal edildiği ve uçuşlarının ertelendiği durumlardaki asgari haklarını belirlemek ve düzenlemektir". Yönetmelikte yolcuların kişisel verileri ile ilgili hakları konusunda hiçbir madde bulunmamaktadır. Ancak yolcu verilerinin en azından ABD güvenlik otoritelerine aktarılıp orada işlendiği bilinmektedir. Yönetmeliğin daha çok olası seyahat olumsuzluklarına karşı yolcu haklarını belirttiği açıktır, ancak yine de bu başlıkta bir yönetmeliğin yolcuların kendi bilgileri ile ilgili en azından bilgilendirilme hakkı olduğu belirtilebilirdi. Yönetmeliğin AB'nin EC 261/2004 sayılı Tüzüğüne[85] paralel olarak hazırlandığı atfı yapılmıştır. Bu Tüzükte de kişisel verilerle ilgili herhangi bir madde olmamasına rağmen AB'nin zaten 95 Direktifi ve YİK anlaşmaları aracılığıyla belli bir mevzuat sahip olduğunu bilmekteyiz. Bu Yönetmelik 2012 yılında yürürlüğe girmiş ancak geçen zaman içerisinde konu ile ilgili herhangi bir düzeltme yapılmamıştır. Düşüncemiz, Sivil Havacılık Genel Müdürlüğünün konuyu havayolu şirketleri ile ilgisi bakımından onlara bırakmış olduğu yönündedir. Bu yüzden konu ile ilgili yurt dışına da taşımacılık yapan hava yolu şirketlerinin web sitelerini inceleyerek ve onlarla iletişime geçerek bilgi

83 03.12.2011 tarihli ve 28131 sayılı Resmi Gazete
84 07.11.2015 tarihli ve 29525 sayılı Resmi Gazete
85 OJ L 46, 17.2.2004, p. 1–8. Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91

almaya çalıştık.[86] Öncelikle ziyaret ettiğimiz 6 havayolu şirketinin web sitelerinde konuya yaklaşımları bakımından farklılıklar olduğunu tespit ettik. Şirketler konuyu gizlilik, yolcu hakları ve kişisel verilerin korunması başlıklarında aktarmaktadır. Bu değerlendirmelerin hiçbiri yanlış veya eksik değildir. Ancak yolcuların bilgilendirilmesinde atıf yapılan yasaların birbirinden farklı olması ilgi çekicidir. Yalnızca 2 havayolu şirketi yeni Kanuna atıf yapmakta, biri Yolcu Hakları Yönetmeliğine atıf yapmakta, biri kişisel verilerin Alma Federal Yasalarına göre işlendiğini belirtmekte, sonuncusu ise yolcuların Web sitesine verdiği bilgilerin başkalarıyla paylaşılmayacağını taahhüt etmektedir. E-posta yoluyla iletişim kurduğumuz ve yurt dışına uçuşları bulunan 18 havayolu şirketinin 3'ü "YİK verilerini yurt dışına aktarıyor musunuz?" sorusuna şu yanıtları vermiştir:

- Şirket A, Internet üzerinden rezervasyon için verilen bilgileri yalnızca bu amaçla kullanmakta ve üçüncü şahıslarla paylaşmadığını belirtmiştir. Ancak yolcular verilerinin belli amaçlar doğrultusunda Şirket tarafından kullanılma hakkına sahip olduğunu kesinlikle kabul etmek durumundadır. Bu amaçlar, Şirketin deyimiyle, "Türkiye'nin ve herhangi bir ülkenin tüm uygulanabilir kanunlarına, kurallarına ve düzenlemelerine uygun bir şekilde ve belirtilmekte olan şartlar ve koşullar altında uygulandığı sürece" ve hizmetlere ilişkin rezervasyonlar ile seyahat ve giriş formalitelerinin yerine getirilmesi, bilgilerin uçuşun gerçekleştirilebilmesi amacıyla ilgili mercilere bildirilmesi" olarak belirtilmiştir. Bu amaçlarla yetkili bürolara, yetkili acentelere, yurt içindeki ve yurt dışındaki yetkililere, güvenlik güçlerine, adli makamlara, diğer uçak şirketlerine ve sair kişilere kişisel bilgileri vermektedir.
- Şirket B, YİK verilerinin kişisel veri kapsamında bulunduğundan ve kişisel veriler ancak 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri uyarınca paylaşılabilmektedir cevabını vermiştir.
- Şirket C ise Amerika, İngiltere, İsrail gibi bazı ülkelerin vize-pasaport güvenlik prosedürleri konusunda çok sıkı kurallarının

86 Web siteleri incelemeleri ile şirketlerle yapılan e-posta yazışmaları Ocak 2017'de gerçekleşmiştir. Makalenin yayımlandığı tarihte bu sonuçların değişebilme olasılığı göz önünde bulundurulmalıdır.

olduğunu, bu ülkelere seyahat edecek yolcuların vize-pasaport bilgisi kontrollerinin ve yolcu verilerinin aktarımının ilgili ülkelerin onayı ile bir firma tarafından yapıldığı aktarılmıştır. Firma ile kurduğumuz iletişim sonucunda kişisel veri ile ilgili hizmetlerin ilgili Bakanlıklardan temin edilen ruhsatlara istinaden, Milli Sivil Havacılık mevzuatı çerçevesinde, anlaşmalı bulunan havayolları adına gerçekleştirildiği bilgisi edinilmiştir.

Bu bilgilere göre havayolları şirketlerinin YİK verilerini yurt dışına aktardığı kesinleşmiştir. Web site değerlendirmelerine göre bazı havayollarının yolcularını konu ile ilgili Kanun veya Yönetmeliklere dayanarak bilgilendirme yaptığı anlaşılmıştır. Buna göre YİK verilerinin yasal bir çerçevede aktarıldığı söylenebilir. Şirketler YİK verilerini aktarmaktadır ancak verilerin aktarım dışında örneğin ne kadar zaman tutulacağı, hangi yöntemle aktarıldığı, açıkça hangi otoritelere aktardığı, yolcuların kendi verileri ile ilgili hakları gibi konularda garanti verememektedir. Bu noktaların Küresel Yaklaşım kriterlerine göre düzenlenmesi önerilir.

Diğer bir önemli kaynak olan Havayolu Taşıyıcılarının Yükümlülükleri Yönetmeliği hava yolu şirketlerinin düzenli göçe teşvik ve düzensiz göç ile mücadele konularındaki yükümlülükleri ile ilgilidir. Yönetmelik daha çok Türkiye'ye gelen veya Türkiye üzerinden başka ülkelere yolculuk eden yabancıları kapsamaktadır. Buna göre hava yolu şirketleri düzenli göçün teşviki kapsamında çeşitli önlemler almalıdır. Önlemlerden biri ise ilk defa bir mevzuatta tanımı yapılan YİK ve İSYB verilerinin şirketler tarafından Göç İdaresi Genel Müdürlüğüne aktarılmasıdır. Genel Müdürlük aktarılacak verilerin kapsamına uluslararası standartlar çerçevesinde karar verecek kurum görevini üstlenmiştir. Verilerin kullanımı ise yalnızca Yönetmelik sınırlarında olacaktır. Genel Müdürlük verilerin yurt içinde başka kurumlara veya yurt dışına aktarılmasına karar vermeye yetkilidir. Buna göre istihbarat birimleri, polis ve terörle mücadele kapsamına giren kurumlara verilerin aktarılabileceği belirtilmiştir. Bu Yönetmelik sayesinde yabancıların verileri gerçekten de güvence altına alınmıştır. Genel Müdürlüğün karar verme yetkisinin Kişisel Verilerin Korunması Kurulu ile nasıl değişeceği henüz bilinmemekle beraber, Müdürlüğün bu yetkiyi Kurula aktarması beklenebilir.

Bahsi geçen Yönetmeliklerde, Kişisel Verilerin Korunması Kanuna atıf yapılabilir veya yolcuların kişisel verileri ile ilgili haklarına dair bir bölüme yer verilebilirdi. Bu durum, Kanun öncesinde yolcu bilgilerinin aslında Türkiye tarafından yasal güvenceye alınmadan yurt dışına aktarıldığını göstermektedir. Yeni Kanun ile birlikte ek bir güvenlik önlemi olarak YİK verilerinin yurt dışına aktarılması ve Türkiye'ye yolcu taşıyan hava yolu şirketlerinin bu verileri Türk yetkililerine aktarabilmesi ile verilerin güvenlik güçlerince kullanımı işlenmesi, saklanması gibi konuların yasal temellere dayandırılması uygun olacaktır. Bu sebeple, ilk adımın AB ile atılmasını, Küresel Yaklaşım çerçevesinde imzalanacak ikili bir anlaşma ile hem temel hakların korunması hem de güvenlik önlemlerinin artırılması önerilmektedir.

Sonuç

Bilginin güç olduğu günümüzde kişisel bilgilerin temini de her alanda gerekli görülmekte, özellikle Avrupalı devletlerce temel bir hak olarak kabul edilmesi sebebiyle yasal güvence altına alınması gereken bir kavramdır.

Kişisel bilgiler teröristlerin tespiti, hakkında karar verilmesi ve terör eylemlerine karşı ek bir güvenlik önlemi niteliğinde olması sebebiyle istihbarat değeri yüksek bilgilerdir. Terörle mücadelede son yıllarda uluslararası iş birliğinin gerekliliği bilgi, veri ve tecrübe paylaşımı olarak şekillenmiştir. 9/11 terör saldırıları sonrasında alınan ek güvenlik önlemlerinden biri de ABD'ye veya ABD'den havayolu ile seyahat edecek yolcu bilgilerinin havayollarınca ABD yetkililerine aktarılması olmuştur. AB, verilerin yasal bir çerçevede aktarılabilmesi için ABD ile ikili anlaşmalar imzalamış, başka devletlerle aynı kapsamda anlaşmalar yapmıştır. AB açısından YİK verilerinin oldukça önemli bir güvenlik önlemi olduğu görülmekte ve AB'nin bu tür anlaşmaları artıracağı bilinmektedir.

İnsan hakları konusunda gelişmiş bir mevzuata sahip AB, YİK verilerinin aktarımı ile ilgili hazırladığı Küresel Yaklaşım dokümanında, verilerin AB üyesi olmayan ülkelere aktarımını standart bir temel dayandıran kriterleri açıklamaktadır. AB ile bu programda yer almak isteyen herhangi bir ülkenin bu kriterleri sağlaması üzerine veri aktarımı yapılabilecektir.

Terörle mücadele konusunda her türlü önlemi almak ve değerlendirmek zorunda olan ülkemizin AB ile ABD arasında örneği olan YİK verilerinin aktarımı programını örnek olarak almalıdır. Bu programda suçlu-masum ayrımı olmadan her yolcunun verileri aktarılıp işlenmeye tabi olduğu için herkese eşit bir şekilde yasal korumanın sağlanması gerekmektedir. Kişisel verilerin korunması konusunda belli bir mevzuatı olan ancak kanun düzeyinde bir düzenlemede Avrupa'daki gelişmeleri henüz yakalayabilen ülkemiz, bu durumdan dolayı böyle bir programdan şimdiye kadar faydalanamamıştır. Kanunda verilerin yurt dışına aktarılması ile ilgili bölümünde belirtilen kurallar dahilinde veri aktarımın yapılacak olması önemlidir. Bu kurallara göre veri aktarımı yapılacak ülke ile Türkiye arasındaki anlaşmalar ve karşılıklılık ilkesi birer kriterdir. Türkiye'nin terörle mücadele kapsamında kişisel verilerin paylaşımını bir kriter olarak ele alan ikili anlaşmalarına baktığımızda anlaşmaların oldukça eski tarihlerde imzalanmış olması, daha sonra güncellenmemiş olması ve AB'nin Küresel Yaklaşım kriterlerinden uzak kalmış olması bu anlaşmaların yetersiz olduğunu göstermiştir. Ayrıca Türk havacılık mevzuatında gerek yolcu hakkı olarak gerekse havayolu şirketlerinin sorumlulukları altında yolcuların kişisel verilerinin korunması ile ilgili herhangi bir düzenleme bulunmuyor olması YİK verilerinin aktarımı ile ilgili bir boşluğa işaret etmektedir. Türkiye'nin konu ile ilgili mevzuatı gözden geçirip AB ile YİK veri aktarımı anlaşması imzalaması hem ülkedeki güvenlik için hem de insan haklarının güvence altına alınması açısından faydalı olacaktır.

Kaynakça

Bilgehan, Zihni ve Özer, Yusuf Mansur, "Turkey, Data Protection 2016", ICLG, 9 Mayıs 2016. https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/turkey#chaptercontent1.

Chang, Chen-Hung, "New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory." *National Taiwan University Law Review* 10, no. 1, 2015: 127–75.

Eijkman Quirine, "Counter-Terrorism, Technology and Transparency: Reconsidering State Accountability." *The Journal of International Security and Terrorism* 3, 1, 2012: 29-40. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2199118

Farrell Henry ve Newman Abraham, "The Transatlantic Data War: Europe Fights Back against the NSA." Foreign Affairs *VO - 95*. Council on Foreign Relations, Inc., 2016. http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.439135741&lang=tr&site=eds-live&authtype=ip,uid.

Giles Courtney, "Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations." *Houston Journal of International Law* 37, no. 2, 2015: 543–79. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=102839256&site=ehost-live.

Bağcı Gökhan Uğur, "14 Soruda Kişisel Verilerin Korunması Kanunu", E-ticaret ve internet hukuku, 10 Mayıs 2016. http://www.eticarethukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu#more-176

Buttarelli Giovanni, Counter-Terrorism Policy and Data Protection, Hearing of the European Economic and Social Committee (EESC), 9 February 2010. http://www.eesc.europa.eu/resources/docs/edps_counterterrorismanddataprotection.pdf

Bulur Sertaç, "Türkiye'nin yabancı terörist savaşçılarla mücadelesi", Anadolu Ajansı, 24.03.2016 çevirim içi haberi. http://aa.com.tr/tr/turkiye/turkiyenin-yabanci-terorist-savascilarla-mucadelesi-/543046?amp=1

Gutwirth Serge, Yves Poullet, ve de Hert Paul, Data Protection in a Profiled World. Dordrecht; New York : Springer, c2010., 2010. Ebsco veri tabanından erişildi.

Hedges Joshua W. "Eliminating the Learning Curve: A Pragmatic Look at Jihadist Use of the Internet." *Journal of Applied Security Research* 3, no. 1, 2008: 71–91. doi:10.1300/J530v03n01_07

House of Lords-European Union Committee. The EU/US Passenger Name Record (PNR) Agreement, Authority of the House of Lords, 21st Report of Session 2006-07. http://www.statewatch.org/news/2007/jun/eu-pnr-hol-report.pdf

International Civil Aviation Organization, "Guidelines on Passenger Name Record (PNR) Data", ICAO, 2010. https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf

Kaya Mehmet Bedii ve Taştan Furkan Güven, "Veri Koruma Hukuku: Mevzuat&İçtihat", Sinerjik.org, 2010. http://www.sinerjik.org/veri-koruma-hukuku/

Korkmaz İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme." *Türkiye Barolar Birliği Dergisi* 124, 2016: 81–152. http://tbbdergisi.barobirlik.org.tr/m2016-124-1571

Kuhelj, Alenka. "The Twilight Zone of Privacy for Passengers on International Flights between the EU & USA." *U.C. Davis Journal of International Law & Policy* 16, no. 2 2009: 383–436.

Küzeci Elif, "Kişisel Verilerin Korunması / Data Protection." Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Doktora Tezi, 2010. https://tez.yok.gov.tr/UlusalTezMerkezi/

Rasmussen D Richard, "Is International Travel Per Se Suspicion of Terrorism - The Dispute between the United States and European Union over Passenger Name Record Data Transfers Notes and Comments." *Wisconsin International Law Journal* 26, 2008: 551–90.

Reuters Reporter, "Department of Homeland Security monitors Facebook, Twitter and news sites for 'situational awareness", DailyMail, 13 Ocak 2012 http://www.dailymail.co.uk/news/article-2085940/Facebook-Twitter-news-sites-monitored-US-Homeland-Security.html

Robinson, Neil, Hans Graux, Maarten Botterman ve Lorenzo Valeri. "Review of the European Data Protection Directive." The RAND Corporation, 2009.

Savoiu Alina and Catalin Capatina Basarabescu, "The Right to Privacy." Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series 2013, no. 1 (2013): 89–96.

Sondergaad Peter, "Big Data Fades to the Algorithm Economy", Forbes/Tech, 14 August 2015. https://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/#2f3b5c1a51a3

The Wall Street Journal, "2016 Belgium's Tragic Terror Lessons" 24 Mart 2016 http://www.wsj.com/articles/belgiums-tragic-terror-lessons-1458861105

The Economist, "The terrorist in the data", 26 Novemver 2015. http://www.economist.com/news/briefing/21679266-how-balance-security-privacy- after-paris-attacks-terrorist-data

Toksoy Fevzi, Balkı Bahadır ve Yıldız Sera Erzene, "Data Protection in Turkey: Overview" Practical Law Multi-Jurisdictional Guide 2016/17 Data Protection 2016. http://us.practicallaw.com/7-520-1896?q=turkey

Tzanou Maria, "The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security Research Article." *Utrecht Journal of International and European Law* 31, no. 80, 2015: 87–103. doi:http://doi.org/10.5334/ujiel.cq.

U.S. Department of Commerce, "U.S.- EU Safe Harbor Framework: A Guide to Self-Certification", March 2009. http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf

White House, "National Strategy for Information Sharing: Successes and Challenges In Improving Terrorism-Related Information Sharing" October 2007 https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf

Wright David ve Charles Raab, "Privacy Principles, Risks and Harms." *International Review of Law, Computers & Technology* 28, no. 3 , 2014: 277–98.

Nouskalis Georgios, "Biometrics, E-Identity and the Balance between Security and Privacy: A Case Study of Passenger Name Record (PNR) System Comment." *The Scientific World Journal,* 11, 2010: 474–77. doi: http://10.1100/tsw.2011.48