TÜRKİYE BİLİŞİM DERNEĞİ

Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği

Kamu Bilişim Platformu XXII

1. ÇALIŞMA GRUBU RAPORU

SINIR AŞAN VERİ TRANSFERLERİ

ÇALIŞMA GRUBU

Son Rapor

Sürüm 2.0

http://www.tbd.org.tr

Aralık 2019

TBD Kamu-BİB

Kamu Bilişim Platformu XXII

SINIR AŞAN VERİ TRANSFERLERİ

1. ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği (TBD Kamu-BİB)'nin ***yirmiikinci dönem*** çalışmaları kapsamında, **1. Çalışma Grubu (ÇG1)** tarafından hazırlanmıştır.

Belge No : TBD/Kamu-BIB/2019-ÇG1

Tarihi : Aralık 2019

Durumu : Son Rapor

Yayını Hazırlayanlar

Başkan

Tevfik ÖZHAN	Vodafone

Grup Üyeleri

Alper KARABULUT	Türkiye Noterler Birliği
Ayhan AŞIK	Emekli
Ayşe Nur AKINCI	T.C.C.B. SBB
Prof.Dr. Bahtiyar AKYILMAZ	Gazi Üniversitesi
Burak AKSOY	Türkiye Noterler Birliği
Çiğdem KOŞAN	T.C. Ticaret Bakanlığı
Demet KABASAKAL	BTK
Ece MUTLU	Vodafone
Emre ERGİN	Vodafone
Ferdi ER	GANTEK
Gökçe NUHOĞLU	T.C. UAB
İbrahim Can BAYRAK	T.C. UAB
Levent TAŞ	Argela

Merve YAŞIN YAVUZ	T.C. Ticaret Bakanlığı
Mesut KÜÇÜKİBA	TCDD
Mustafa İŞCAN	KVKK
Nalan MAÇ	Danışman
Nesrin EZER	N5 Bilişim
Olgaç ZAİM	Türkiye Noterler Birliği
Rüştü Korkmaz	UCS
Sançar Sefer SÜER	Serbest Avukat
Tuna DOLANBAY	T.C. Ticaret Bakanlığı
Talip Engin KAYA	T.C. Ticaret Bakanlığı
Tuğçe BARUT	GANTEK
Uğur KARABULUT	Kod Merkezi
Zafer İLLEZLER	Dugan Bilişim

İçindekiler

1 GİRİŞ 5
2 VERİ KAVRAMI VE TİCARİ DEĞERİ 7
2.1 Veri ve Kişisel Veri Kavramları 7
2.2 Verinin Ticari Değeri ve Ticari İşletmeler Bakımından Önemi 8
2.3 Büyük Veri ile Sektörlerdeki İş Problemlerine Çözümler 9
3 VERİLERİN YURTDIŞINA AKTARILMASI (SINIR AŞAN VERİ TRANSFERİ) 11
3.1 Verinin Serbest Dolaşımına İlişkin Sınırlamalar ve Uygulamaya Etkileri 11
3.2 Verinin Serbest Dolaşımı 12
3.3 Sınır Aşan Verinin Güvenliği Sorunu 12
3.4 Verinin Yurt Dışına Aktarılması Gerekliliği 13
3.5 Türk Hukukunda Verilerin Yurtdışına Aktarılmasının Sınırları 14
3.6 Avrupa Birliği Genel Genel Veri Koruma Tüzüğü'nde (General Data Protection Regulation − GDPR) Verilerin Yurtdışına Aktarılmasının Sınırları 17
4 ULUSLARARASI TİCARETTE/ TİCARET ANTLAŞMALARINDA VERİNİN ÖNEMİ 19
4.1 Hizmet Ticareti ve Sınır Aşan Veri Transferi 19
4.2 Küresel Değer Zincirlerinin İşleyişi ve Sınır Aşan Veri Transferi 20
4.3 Büyük Veri Analizi Sonucu Üretilen Mal ve Hizmetler İçin Girdi/Hammadde ve Sınır Aşan Veri Transferi 20
5 TİCARET ANLAŞMALARINDA "VERİ" İLE İLGİLİ TARTIŞMALAR 21
6 ÜLKELERİN TİCARET MÜZAKERELERİNDE "VERİ TRANSFERİ" KONUSUNDA POZİSYONLARI 21
7 ÇEŞİTLİ ÜLKELERDE VERİ TRANSFERİ KONUSUNDA TARTIŞMALAR 23
8 SINIR AŞAN VERİ TRANSFERİ / VERİNİN BAŞKA ÜLKEDE TUTULMASI İLE İLGİLİ SINIRLAMALARIN DAYANAKLARI 24
9 SINIR AŞAN VERİ TRANSFERİ / VERİNİN BAŞKA ÜLKEDE TUTULMASI İLE İLGİLİ ÜLKEMİZİN YAKLAŞIMI 26
10 ÖRNEK MEVZUAT İNCELEMESİ: AB SERBEST VERİ AKIŞI TÜZÜĞÜ 28
11 SONUÇ VE ÖNERİLER 29

TEKNOLOJİ Mİ − GÜVENLİK Mİ?:
İKİSİ BİRDEN NEDEN MÜMKÜN OLMASIN?

"*Malların geçmesine izin verilmeyen sınırlardan askerler geçer***"**
Frederic Bastiat

1 GİRİŞ

Birçok kesim tarafından 4. Sanayi Devrimi olarak kabul edilen "Endüstri 4.0", çağdaş ve modern otomasyon sistemleri ile veri alış verişlerini, üretim teknolojilerini içeren bir sanayi terimidir. Endüstri 4.0, içerisinde nesnelerin internetini, internetin hizmetlerini ve fiziksel-sanal sistemleri barındırır.

Endüstri 4.0 ile birlikte üretici kadar tüketicinin de hayatı kolaylaşmıştır. Nesnelerin interneti ile tüm üretim, internetin sağladığı kolaylıklar ile birlikte daha hızlı ve daha aktif hale gelmiş; birkaç dokunma veya tıklama ile istenilen veriye, bilgiye veya belgeye ulaşmak mümkün olmuştur. Bunu mümkün kılan en önemli öğe ise Endüstri 4.0 devriminin en sağlam teknolojisi olan Bulut Teknolojisidir.

Bulut teknolojisinin gelişmesiyle, büyük verilerin internet üzerinde depolanabilirliği ve verilere erişilebilirlik olanaklı hale gelmiştir. Böylece Endüstri 4.0'ın yapı taşlarından olan büyük veri (big data) endüstride uygulanabilme imkanına sahip olmuştur. Bulut Teknolojisi sayesinde akıllı fabrikalar kendi kendini organize edebilmiş, zorlu üretim süreçleri kolaylaşmış, zaman isteyen raporlama ve veri analizleri daha hızlı ve aktif biçimde yapılır hale gelmiş; daha verimli iş modelleri ortaya çıkmıştır.

Kısaca ifade etmek gerekirse bulut teknolojisinin ve veri analizinin odak noktasında olduğu Endüstri 4.0'ın avantajları şu şekilde özetlenebilir:

- Sistemin izlenmesinin ve arıza teşhisinin kolaylaştırılması,
- Sistemin çevre dostu ve kaynak tasarrufu davranışlarıyla sürdürülebilir olması,
- Daha yüksek verimliliğin sağlanması,
- Üretimde esnekliğin arttırılması,
- Maliyetin azaltılması,
- Yeni hizmet ve iş modellerinin geliştirilmesi.

Bu teknolojinin dezavantajları da yok değildir. Her şeyden önce bulut teknolojisi ile verilerin depolanması konusunda yaşanan güvenlik açıkları, kişisel verilerin korunmasında büyük tehdit oluşturmaktadır. Bu durum ülkeleri koruma tedbirleri almaya yöneltmektedir. Diğer taraftan bu teknolojinin gelişmesi, ülkeler arasındaki teknolojik uçurumu daha da derinleştirmekte; teknolojinin tekelleşmesine; bu yolla politik ve ekonomik baskıların kolaylaşmasına neden olmaktadır. Bu da ülkelerin bağımsızlığı, kişilerin özgürlüğü bakımından ciddi sorunları beraberinde getirmektedir.

İşte bir yandan hayatımızı kolaylaştıran işletmelerde hızı ve verimi artıran, diğer yandan da kişisel ve ulusal bir takım güvenlik risklerini beraberinde getiren bu teknoloji başlıktaki

“soru”nun sorulmasına neden olmaktadır: **teknoloji mi güvenlik mi**?

Bu soru aslında başka soruları da beraberinde getirmektedir: Serbest ticaret mi – ulusal ekonomi mi? Yabancı yatırım mı – ulusal sermaye mi? −ve tabi endüstri 4.0 ve bulut teknolojisi çağında− verilerin serbest dolaşımı mı – verilerin korunması mı?

Biribirine zıt gibi gözüken bu konular ve dijitalleşme, Osaka da yapılan G20 Liderler Zirvesinde de tartışılmıştır. Bu çerçevede liderler zirvesine temel olacak, G20’nin ticaret ve dijital ekonomi bakanları toplantısı sonuç raporundaki şu tespitler konuyla ilgili dikkat çekicidir:

- Refah artacak: Dijitalleşmenin ekonomiler ve toplumlar için bir bütün olarak fayda oluşturması beklenmektedir. Yapay zeka, 5G, nesnelerin interneti (IoT), blokzincir yeni fırsatlar ve istihdam oluşturacaktır. Firmaları güçlendirecek, daha fazla refah ve daha fazla kapsayıcılığa yol açacaktır.

- Dijital eşitsizlik: Dijitalleşme topluma fayda sağlama konusunda muazzam bir potansiyele sahip olsa da bazı endişeleri de beraberinde getirmektedir. Dijitalleşme ile dijital eşitsizlikler konusu birlikte ele alınmalı, dijital ekonomiye güveni artırmak için birlikte çalışılmalıdır.

- Adalet ve şeffaflık: Dijital toplum, işbirliği ekseninde, eşitlik, adalet, şeffaflık ve hesap verilebilirlik gibi ortak değerlere dayanarak, hükümetler, uluslararası kuruluşlar, işletmeler, STK’lar ve üniversiteler dahil tüm paydaşlar arasında güven üzerine kurulmalıdır.

- Serbest dolaşım ve güvenlik: Sınır ötesi veri dolaşımı daha fazla üretim, verimlilik, inovasyon ve iyileştirilmiş bir sürdürülebilir kalkınma sağlamaktadır. Serbest veri dolaşımının bazı zorlukları olmakla beraber, gizlilik, kişisel verilerin korunması, fikri mülkiyet hakları ve güvenlik ile ilgili zorluklar ele alınmaya devam edilerek, verilerin serbest dolaşımı daha da kolaylaştırabilir ve tüketicinin güveni güçlendirilebilir. Güven oluşturmak ve serbest veri akışını kolaylaştırmak için hem yerel hem de uluslararası yasal çerçevelere saygı gösterilmesi gerekir. Güvene dayalı serbest veri dolaşımı, dijital ekonominin fırsatlarını kullanmalıdır.

- Kişisel verilerin korunması: Uygulanabilir çerçevelerle tutarlı olarak kişisel verilerin korunmasını teşvike devam etmek gerekmektedir.

O halde belki sonda söylenmesi gerekeni başta söyleyerek şunu belirtmek gerekir: Bilgi çağı yerini, ana hammaddesi veri olan teknoloji çağına bırakmakta ve dijitalleşme hayatımızın bütün alanlarına girmektedir. Bu durum beraberinde özel hayatın gizliliği ve kişisel güvenlikle beraber uluslararası alanda ulusal güvenlik bakımından önemli riskleri beraberinde getirmekle beraber, verimli bir üretim süreci sağlamakta, sürdürülebilir bir kalkınma ile birlikte hayatımızı büyük oranda kolaylaştırmaktadır. O halde dijitalleşmenin, kişisel ve ulusal güvenlik ile birlikte ele alınması; bu çerçevede kişisel verilerin korunması ile birlikte yeni teknolojinin hammaddesi verinin serbest dolaşımı konusunda da gerekli düzenlemelerin yapılması gerekmektedir.

2 VERİ KAVRAMI VE TİCARİ DEĞERİ

2.1 Veri ve Kişisel Veri Kavramları

Bilişim Terimleri Sözlüğünde "veri", "*olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi. Elverişlilik, kişiler ya da özdevimli makinelerle iletişim, yorum ya da işleme uygunluk biçiminde düşünülür, bk. Bilgi*" şeklinde tanımlanmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3 üncü maddesine göre ise "***kişisel veri: kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder***". Buna göre kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekmektedir. Bu tanımdan hareketle kişisel verinin üç temel unsuru olduğu söylenilebilir:

- **Verinin "*gerçek kişiye ilişkin*" olması**: 6698 sayılı Kanun'a göre "**kişi**", "**gerçek kişi**"yi ifade etmektedir. Bu nedenle tüzel kişilere ilişkin veriler (6698 sayılı Kanun'a göre) "kişisel veri" kapsamı dışındadır[1].

- **Kişinin "*belirli veya belirlenebilir*" olması:** Verinin içeriğinde, ilgili kişinin kimliği açıkça belli olmalı ya da veride yer alan bilgilerden hareketle yapılacak basit bir araştırma veya bir kayıtla ilişkilendirme neticesinde kişinin kimliğinin belirlenebilir olması gerekir.

- **"Veri" ile kastedilenin, "*her türlü bilgi*" olması:** Veri kavramı son derece geniş olup, her türlü bilgiyi kapsamaktadır. Kişisel veri kapsamındaki bilgi için temel kriter ise bu bilginin, kişinin kimliğini ifşa eden bilgi olmasıdır. Bu çerçevede kişinin fiziki, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden her türlü bilgi; örneğin kişinin adı, soyadı, doğum tarihi, doğum yeri, telefon numarası, taşıt plakası, kimlik numarası, pasaport numarası, özgeçmişi, resmi, görüntü ve ses kayıtları, parmak izi, e-posta

[1] Ancak gerçek kişilerin özel hayatı ile mesleki hayatlarını birbirinden ayırt etmek her zaman mümkün değildir. Nitekim Amann v. İsviçre davasında AİHM de özel hayat kavramının dar şekilde yorumlanmaması gerektiğini belirterek, kişinin mesleği ile ilgili faaliyetlerin özel hayat kavramının dışında tutulmasını haklı gösterecek herhangi bir sebep olmadığını ifade etmiştir. (Amann v. Switzerland [GC], No. 27798/95) Anayasa Mahkemesi de bir kararında tüzel kişilere ait verilerinde kişisel verilerin korunması kapsamında olacağına hükmetmiştir: "*Anayasa'nın 20. maddesinde kişisel verilerin kişi bakımından korunma alanının gerçek kişiler ya da tüzel kişileri veya her ikisini içine alıp almadığı konusunda bir açıklık bulunmamaktadır. Maddenin gerekçesinde de buna ilişkin bir değerlendirme yoktur. Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır*". Yüksek Mahkemeye göre; "*Esasen her ne kadar 95/46/EC sayılı Avrupa Veri Koruması Direktifi'nde yer alan tanım, tüzel kişilere ilişkin verileri dışlamakta ve kişisel veri kapsamına yalnızca gerçek kişilere ilişkin bilgilerin gireceğini kabul etmekte ise de, gerek 'Elektronik haberleşme sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunması' hakkında 12.7.2002 gün ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'nde, yalnızca elektronik haberleşme sektörüne ilişkin olarak, hem gerçek kişilerin hem de tüzel kişilerin veri sahibi kabul edileceğinin ifade edilmesi; gerekse son yıllarda kabul edilen bazı ülke kanunlarında tüzel kişilerin de kişisel verilerin korunma alanına dâhil edilmesi bir bütün olarak dikkate alındığında, Avrupa ve Dünyadaki gelişimin kişisel verilerin korunmasında tüzel kişilerin de kapsamda yer alması gerektiği yönünde olduğu görülmektedir*". AYM, 4.12.2014, E 2013/84, K 2014/183, RG 13.3.2015-29294.

adresi, hobileri, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi bilgiler, kişisel veri olarak kabul edilmektedir. O halde bilgi bir kişi hakkında ise; bir kişiyi değerlendirmek veya etkilemek amacıyla kullanılıyorsa veya böyle bir ihtimal varsa ya da bu bilginin kullanımı belirli bir kişinin hakkını yahut menfaatini etkileyecekse korunması gereken bir veri var demektir.

"Gerçek kişiye ilişkin her türlü bilgi" olarak tanımlandığında pek çok veri, kişisel veri olarak nitelendirilebilir. Bu noktada koruma alanının ve derecesinin belirlenmesi ve verinin işlenmesi bakımından özel nitelikli kişisel verilerin de tanımlanması gerekir. Niteliği gereği işlenmesi halinde ilgili olduğu kişiye yönelik risk oluşturabilecek; kişinin mağdur olmasına ya da ayrımcılığa maruz kalmasına; onurunun zedelenmesine neden olabilecek bilgiler "**özel nitelikli kişisel veri**" (hassas veri) dir. O halde özel nitelikli kişisel veri, başkaları tarafından öğrenildiği takdirde ilgili kişinin kişilik hakları bakımından olumsuz etkileneceği verilerdir. Önemine binaen 6698 sayılı Kanunda "tahdidi" olarak belirtilmiş olup[2], bu sayılanlar dışındakiler özel nitelikli kişisel veri olarak kabul edilemez. Bu bakımdan, özel nitelikli kişisel verilerin sınırlı olarak sayıldığı kabul edilir.

2.2 Verinin Ticari Değeri ve Ticari İşletmeler Bakımından Önemi

Günümüzde pek çok işletme, veriye dayalı karar almanın, işletmenin veya işin mevcut durumun daha iyi anlaşılması, alternatif seçeneklerin değerlendirilmesi, farklı ihtimaller üzerinde kıyaslama ve doğru analizler yapılması gibi önemli faydaları beraberinde getireceğini bilmektedir. Bununla birlikte çoğu işletme, veri toplamanın faydasının ve veriye sahip olmanın stratejik bir varlık olarak öneminin farkında olmakla birlikte söz konusu veriyi nasıl faydalı bir içgörüye veya doğru kararlara dönüştürebileceği noktasında yeterli beceriye ulaşamamıştır. Bu durumun temel nedeni ise, işletmenin sahip olduğu verileri, iş gereksinimleri ve hedeflerine uygun biçimde işleme konusunda etkin ve yetkin bir yönetime sahip olmayışı gelmektedir.

Özellikle "teknoloji nesli" tarafından yönetilen işletmeler, bu zorluklarla baş etmede giderek daha yetkin bir görünüm arz etmektedir. Bu işletmelerde veriler; mobil iletişim kanalları, akıllı telefonlar, e-postalar, nesnelerin interneti (IoT) ve video içerikleri gibi çeşitli kaynaklardan toplanmaktadır. Yeni nesil işletme sahipleri bu araçların içinde büyümektedir. Dolayısıyla sahip olunan verinin faydalı bir içgörüye veya doğru kararlara dönüştürülebilmesi konusunda yeni nesil bir başlangıç girişimi (start-up) işletmecisi, geleneksel işletmeciye oranla önemli bir avantaja sahip olmaktadır.

Ticari işletmelerde, ticari bilgiler ve şirket sırları olmak üzere pek çok kişisel olmayan bilgi de yer almaktadır. Bu noktada kişisel verilerin işlenmesi bakımından hukuka uygun yöntemler bulmak önemli olmakla birlikte, işletmelerin her gün erişebildiği bu veri zenginliğini yitirmemesi de önem arz etmektedir.

Günümüzde uluslararası alanda ticari rekabet için işletmeler yapay zekâ (AI) araçlarına yatırım yapmaktadırlar. Zira işletmenin sürdürülebilir bir rekabet ortamı için, elinde bulunan tüm veriyi nasıl kullanacağını bilmesi, içgörüleri yorumlaması ve daha sonra buna göre hareket etmesi

---

[2] "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 biyometrik ve genetik verileri özel nitelikli kişisel veridir". (m. 6/1)

gerekmektedir. Elde edilecek gerçek değer, ancak bu şekilde açığa çıkarılabilecektir.

Verinin kişisel veriden, ticari veriye ve günümüzde yapay zekâ (AI) teknolojisine evrimi, beraberinde bir takım zorluklar da getirmektedir. Bu sebeple müşterileriyle olan ticari ilişkilerini güçlendirmek isteyen işletmelerin, algoritmaları ve veriye dayalı yeni araçları kullanmaya daha fazla ihtiyaç duyacakları öngörülmektedir. Söz konusu araçların kullanımı ise her bir işletme açısından yeni sorumlulukları da beraberinde getirmektedir.

Günümüzde en küçük verinin dahi potansiyel ticari değerinin hafife alınamayacağı ve karanlıkta kalamayacağı artık net olarak kabul edilmiş bulunmaktadır. Bu çerçevede veri evriminden faydalanmak isteyen işletmelerin kişisel veya kişisel olmayan verileri inceleyerek ve ellerindeki varlıklar doğrultusunda hareket etmesi gerekmektedir.

O halde veriye “sadece” sahip olmak yetmemektedir. Veri, ancak veri analizi yapıldığı müddetçe işe yaramaktadır. Başka bir ifadeyle akıllı cihazlar, sistemler, müşteriler, nesnelerin interneti derken, devasa bir veri yığını ile karşı karşıya kalan şirketler, öngörüsel veri analizi ile bu veriyi gelecekte kendileri için avantaj sağlayabilecek hale getirebileceklerdir.

Öngörüsel analiz (predictive analytics) temelde her sektörden şirketin faydalanabileceği bir çözümdür. İşletmeye kapasitesini artırmak ve daha iyi bir iş çıkarmak için kullanabilecek bir yol haritası elde etme şansı tanır. Bu da şirketlerin geleceği adına sağlam adımlar atabilmelerini kolaylaştırır. Stratejik hedefler belirlemek isteyen şirketlerin, öngörüsel analizi büyük veri ile birlikte kullanmaları, iş verimliliğini artırma çabalarına da destek olur.

Site davranışları, harcama alışkanlıkları, web sitesinde kalma süresi, sosyal medyadaki hareketleri, ilgi alanları, lokasyon, kullanılan cihaz, demografik bilgiler gibi müşteri davranışlarının görülebiliyor ve analiz edilebiliyor olması, yapılması gereken iyileştirmeler hakkında da fikir verir. Bu veriler bir araya getirildiğinde ve analiz edildiğinde, müşterilerin bireysel ihtiyaçlarına daha hızlı bir şekilde cevap verebilme ve daha kullanışlı hale getirebilme imkânı da söz konusu olur.

O halde veri, teknolojik çağda işletmelerin en önemli hammaddesidir. Başarılı işletmeler ise ellerinde büyük veri bulunduran ve bu verileri en iyi analiz edenlerdir.

2.3 Büyük Veri ile Sektörlerdeki İş Problemlerine Çözümler

Verinin ticari değerini açığa çıkaran etmenler, sektörlerdeki iş problemlerine getirdiği çözümlerdir. Çözümler beş ana sektör için incelenebilir. Bunlar; Perakende Sektörü, Finans Sektörü, Turizm Sektörü, Akaryakıt Sektörü ve FMCG (Fast−Moving Consumer Goods − Hızlı Tüketim Ürünleri) Sektörüdür.

Perakende sektörü ülkemizde ve dünyada rekabetin yoğun olduğu alanlardan bir tanesidir. Bu rekabet ortamı doğal olarak kurumları farklı çözümler aramaya yöneltmektedir. Büyük Veri sektörlerde karşılaşılabilecek alışılmadık problemlere etkili çözümler sunabilecek bir servis potansiyeli taşımaktadır. Perakende Sektöründeki kurumlar “büyük veri” ile birlikte pazar paylarının analizini yapabilirler ve bu sayede sektörde kendi ağırlıklarını ölçebilirler. Bu analiz rekabet içinde oldukları kurumlarla aralarındaki farkı görmelerini sağlayarak belirlenen konular hakkında önlem almalarına yardımcı olur. Müşterilerin demografik özelliklerinin analiz

edilmesinde büyük veri önemli bir rol oynamaktadır. Demografik özellikleri açıklayan raporlar, şirketlere önemli bir iç görü sağlayarak, uygulanacak politikaların müşteri temelli olmasına yardımcı olabilir. Bu analiz sayesinde kurumların hedef kitlesini belirlemesi ve buna uygun yatırım planlarını düzenlemesi kolaylaşır. Ticari kuruluşlar yeni müşteri kazanmayı amaçlamaktadırlar; buna bağlı olarak hali hazırda kendilerini tercih etmeyen; ancak o kuruluşların müşterisi olabilme potansiyeli olan kitleler, büyük veri sayesinde saptanabilir. Müşterilerin dijitalleşme skoru analizi şirketlerin müşteriye ulaşma politikalarına yeni bir soluk getirebilme potansiyeli taşımaktadır. Büyük veri sayesinde yeni oluşturulacak müşteriye ulaşma kanalları, kurumların kârlılığına doğrudan etki edebileceği gibi bilinilirlik açısından da önemli bir rol oynayacaktır.

Dijital dünyanın getirdiği yeniliklerden biri olan büyük veri, Finans Sektörü için de önemli bir çözüm alternatifi olmaktadır. Finans Sektörünün yapıtaşlarından olan bankalar için yeni açılacak şube lokasyonlarını belirlemek, kritik bir önem arz etmektedir. Bu noktada büyük veri yeni şube için düşünülen lokasyonları belirli kriterler ışığında analiz edilmesine ve lokasyonlar arasında karşılaştırma yapılabilmesine yardımcı olabilir. İnsan/araç trafiği, güvenlik, bölge demografisi gibi konuları kapsayıcı analizler bankalara yeni şube açma konusunda yol gösterici olabilmektedir. Bankalar bir yandan büyümeyi, yeni şube açmayı hedeflerken, diğer yandan kendilerinden ayrılmayı düşünen müşterileri tahminlemeyi amaçlamaktadırlar. Churn skoru, müşterinin ilgili kuruluştan ayrılma ihtimalini hesaplayan bir metriktir ve bu metrik büyük veri sayesinde daha doğru bir şekilde hesaplanabilir. Bu analiz bankaların var olan müşterilerini kaybetmesini önleyerek gelir kaybının önüne geçmeye yardımcı olur. Günümüzde bankalar internet bankacılığı üzerine yoğunlaşmaktadırlar ve bunu mobil uygulamalar üzerinden yaygınlaştırmak istemektedirler. Bankalar geliştirdikleri bu uygulamalar üzerinden müşterilerine ulaşma ihtimallerini müşteri dijitalleşme analizi ile tahminleyebilirler. Bu analizin sonucunda ulaşılabilecek olan dijitalleşme skoru uygulamaların hedef kitle tarafından kullanılma ihtimalini ön görebilmektedir.

“Büyük veri”nin yenilikçi çözümler sunabileceği sektörlerden bir tanesi de Turizm Sektörüdür. Turizm Sektörü, gelişen yeni konseptler, değişen gezi etkinlikleri ışığında farklı bir rekabet ortamına ev sahipliği yapmaktadır. Yeni açılacak oteller için büyük veriye dayalı lokasyon analizi kilit bir rol oynayabilir. Şirketlerin hedeflediği otel konseptinin, yapılması planlanan etkinliklerin lokasyona uygunluğu büyük veri sayesinde analiz edilebilir hale gelir. Otel yatırımlarının büyük meblağlara mal olması ve geri dönüşünün zor olması Büyük veriye dayalı lokasyon analizini gerekli kılmaktadır.

Büyük veri, Akaryakıt sektöründeki şirketlerin maliyetlerini azaltabilecek, organizasyonlarını iyileştirebilecek bir çözüm olarak görülmektedir. Yeni açılacak benzin istasyonunun belirtilen lokasyona uygunluğu büyük veri ile kontrol edilebilir. Benzin istasyonu kurmak ciddi bir organizasyon gerektirdiği için şirketlerin lokasyonun uygunluğunu önceden kontrol etmesi zaman ve konuya ilişkin enerji kaybını önler. Şirketlerin hedef kitlelerini belirlemesi halinde berlinen kitlenin kullandığı yollar olası yeni istasyon veya reklam kampanyaları için mercek altına alınır. Lokasyon başına tüketilen akaryakıt miktarı hesaplanarak ileriye dönük kullanılabilecek akaryakıt tahminlenebilir. Bu analiz ile ilgili lokasyonlara gerektiği kadar akaryakıt transferi gerçekleştirilerek tedarik sırasındaki maliyetler azaltılmış olur.

FMCG (hızlı tüketim ürünleri) sektöründeki şirketler genelde geniş bir ürün yelpazesine sahiptirler. Çeşitli ürünler çeşitli kitlelere hitap etmektedir ve her ürünün alıcıları farklı

bölgelerde yoğunlaşmıştır. Bu nedenle her bölgeye aynı ürünü eşit şekilde pay etmek doğru bir yöntem olmayabilir. Ürünün talep edileceği yerlerin önceden tahmin edilmesi, şirketlerin tedarik maliyetlerini azaltmasına yardımcı olur.

Büyük veri ve veri analizi sayesinde sadece bahsedilen sektörlerde değil, diğer tüm sektörler de iş problemleri çok daha kolay çözülmekte; verimlilik çok daha fazla artmaktadır. O halde işletmeler için büyük veriye sahip olmak ve veri analizi vazgeçilmezdir.

3 VERİLERİN YURTDIŞINA AKTARILMASI (SINIR AŞAN VERİ TRANSFERİ)

3.1 Verinin Serbest Dolaşımına İlişkin Sınırlamalar ve Uygulamaya Etkileri

Verinin önem kazanması, işletmelerce üretimde kullanılmaya başlanması ile birlikte, gerek kişisel verilerin korunması düşüncesi ve gerekse ulusal güvenlik kaygıları ile süreç içinde ilk olarak verinin serbest dolaşımını engellemeye yönelik düzenlemelerin ortaya çıktığı görülmüştür.

Tarihsel olarak, verinin serbest dolaşımını engellemeye yönelik ilk eğilim, "**veri yerelleştirme gereklilikleri**" (data localization requirements) dir. Veri yerelleştirme gereklilikleri, −kişisel olsun ya da olmasın− genel olarak verinin bir ülkeden başka bir ülkeye aktarılmasına sınırlama getirilmesini amaçlanmaktadır. Bu alanda öne çıkan düzenlemelerden biri Rusya'dadır. Rusya, vatandaşlarına ilişkin her türlü kişisel verinin Rusya sınırları içerisindeki sunucularda tutulması ve işlenmesi kuralını getirmiştir. Yine Fransa'da Bakanlar Kurulunca kabul edilen bir genelgede Fransız kamu idareleri tarafından üretilen verilerin tutulacağı bulut hizmet sağlayıcısının Fransa'nın egemenlik alanı içerisinde bulunmamasının hukuka aykırı olacağı hususu vurgulanmıştır.

Hemen belirtmek gerekir ki veri yerelleştirme gerekliliklerinin en belirgin ortak özelliği; **sınır ötesi ticaretin maliyetini arttırmalarıdır**. Yalnızca AB'de 25 farklı yargı çevresinde 60'ın üzerinde düzenlemeyle bu tür sınırlamaların öngörüldüğü bilinmektedir. Söz konusu gerekliliklerin çoğu zaman özellikle yasa koyucular ve politika yapıcılardaki "***ülke sınırları içerisinde kalan veri daha güvende veridir***" yönündeki algılarından kaynaklandığı görülmektedir. Söz konusu algı, yanlış olması noktasında eleştirilmektedir. Zira verinin güvenliği, verilerin tutulduğu konumdan (yer–ülke) ziyade söz konusu veriyi korumak için kullanılan güvenlik önlemleriyle ilgilidir. Söz konusu güvenlik önlemleri güçlü ise verinin tutulduğu yerin önemi olmayabilir. Kaldı ki verinin o ülkede tutulması verinin güvenli saklandığı anlamına da gelmez. Örneğin İngiltere'deki güvenli bir sunucu ile Kore'deki güvenli bir sunucu arasında, güvenlik önlemlerinin sağlıklı işletilmesi koşuluyla, bir fark bulunmamakta; dolayısıyla verinin kime ait olduğu da çok önemli olmamaktadır.

Bulut hizmet sağlayıcıları ve uluslararası alanda faaliyette bulunan veri hizmet sağlayıcıları, veri yerelleştirme gerekliliklerinden en çok etkilenen aktörlerin başında gelmektedir. Zira bu gereklilikler, söz konusu hizmet sağlayıcılarının, veri merkezi olmayan pazarlara erişmelerini engellemekte; diğer taraftan kullanıcılar (hizmetten yararlananlar) da başka bir ülkeden

sağlanan bulut hizmeti ya da veri hizmet sağlayıcılığını **kullanmama** eğilimi göstermektedirler. Bu durum özellikle bulut tabanlı iş modellerini olumsuz etkilemektedir.

Sonuç olarak veri yerelleştirmeye ilişkin gereklilikler, hem özel sektörün hem de kamunun yenilikçi ve çok daha ucuz hizmetlere erişmesini önlemekte, ayrıca birden fazla ülkede bulut hizmeti sağlayan teknoloji firmalarını veri depolama ve işleme amacıyla (o ülkede ayrı ve müstakil bir altyapı oluşturmak suretiyle) ilave iş yükü ve maliyet yükü altına sokmaktadır. Bu durum başlangıç firmaları ve KOBİ'lerin yeni pazarlara girmesi, yeni ürün ve hizmet geliştirilmesi önünde önemli bir engel teşkil etmektedir.

3.2 Verinin Serbest Dolaşımı

Verinin serbest dolaşımından, sınır ötesi veri akışı bakımından hiçbir hukuki engelin bulunmadığı ideal senaryo anlaşılmaktadır. Söz konusu ideal senaryonun tam anlamıyla hayata geçirilmesi henüz mümkün olmamakla birlikte, verilerin serbest dolaşımı konusunda başta AB olmak üzere dünyanın çeşitli ülkelerinde ve ülkelerarasında son dönemde yeni düzenlemeler yapıldığı görülmektedir.

Bu konudaki yeni yaklaşımı ortaya koyan önemli bir düzenleme, 2016 tarihli AB "Genel Veri Koruma Tüzüğü" (General Data Protection Regulation − GDPR) dür.

GDPR'nin 1 inci maddesinin üçüncü fıkrası verilerin serbest dolaşımı ile ilgili şu ilkeye yer vermektedir:

> "**Kişisel verilerin Birlik içerisinde serbest dolaşımı, gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunması ile bağlantılı sebeplerle ne kısıtlanır ne de yasaklanır**".

Yeni düzenlemeler göstermektedir ki, yeni anlayış, verinin güvenli olarak kabul edilen belirli bölgelerde serbest dolaşımına imkân sağlanmakta ve günümüzde bu yaklaşım benimsenmeye başlanmaktadır.

3.3 Sınır Aşan Verinin Güvenliği Sorunu

Sınır aşan veride en önemli kaygı, hizmet sağlayıcıların veriyi taşırken veriyi işleyen şirketlerden özel ve gizli bilgileri nasıl koruyacağıdır. Bu çerçevede mevcut risk ve tehditlerin belirlenmesi önem arz etmektedir.

Öncelikle belirtmek gerekir ki verinin ve verinin tutulduğu fiziksel kaynakların, aynı anda birden fazla kullanıcı tarafından ve birden fazla hizmette ortak olarak kullanılması önemli riskleri de beraberinde getirmektedir. Kullanılan ortak fiziksel kaynaklar üzerindeki işlemciler ile depolama ve sanal olarak veriyi birbirinden ayıran iç mekanizmalardaki zafiyetler ve siber saldırılar veri güvenliğini tehdit etmektedir[3]. Diğer taraftan bulut hizmeti veren şirketlerin farklı ülkelerde veri merkezi bulundurması, bulunduğu ülkeye ait yasal düzenlemelere tabi olmasını gerektirir. Bu ülkelerin birbirinden farklı yasal hassasiyetlerinin olması, verinin güvenliği

[3] Örneğin, 2018 yılında Intel işlemcilerde Spectre ve Meltdown adlı iki hata tespit edilmiş; bu hatalar sonucunda çok önemli bulut hizmeti veren şirketlerin kullanıcılarına ait verilerin sızdığı bir olay yaşanmıştır.

konusunda belli bir standartın oluşmamasına yol açmaktadır.

Bugün Avrupa Birliği ülkeleri ve Amerika Birleşik Devletleri arasında bile, kişisel gizlilik ve veri güvenliği alanında belirgin farklılıklar bulunmaktadır. Bulunduğu ülke dışında başka bir ülkede bulunan bir bulut hizmet sağlayıcısından hizmet alan şirketler, dolaylı olarak bu ülkenin yasalarının kapsamına girdiği için, burada saklanan verilerine hizmet sağlayıcının bulunduğu ülke tarafından yargı yoluyla erişilebilmekte ve böylece verilerinin gizliliği tehlikeye girebilmektedir[4].

3.4 Verinin Yurt Dışına Aktarılması Gerekliliği

Dünyada "*veri temelli ekonomi*" kavramı tartışılmakta, bilgi ekonomisi olma yolunda "verileri işleme" ile ilgili açık bir yasal mevzuata sahip olmayan ülkeler rekabet güçlerini giderek kaybetmektedir.

İnternet, arama motorları, sosyal paylaşım siteleri, nesnelerin interneti, uluslararası ticaret ve çokuluslu şirketlerin varlığı verinin ülke içinde kalması ihtimalini ortadan kaldırmıştır.

Diğer taraftan kişisel verilerin korunması; internet ekonomisinin gelişimiyle önemi artan bir konu haline gelmiştir. Veri teknolojisindeki gelişmeler sağlık, eğitim, finans, e-ticaret, dijital pazarlama gibi sektörlerde ekonomik fırsatlar doğurmaktadır. Verinin etkin kullanımı, sektörel katma değeri, tüketici faydasını ve ticari verimliliği artırmaktadır. Kişisel verilerin korunmasına dair yasal düzenlemeler yapılırken; kişisel verilerin korunmasının tüm dünyada tartışılan ve teknolojinin gelişimine bağlı olarak hızla evrilen bir hukuki alan olduğu da göz önünde bulundurulmalıdır. Büyük veri teknolojilerinin tüm ekonominin verimliliğini ve tüketicilerin faydasını artıracak yeni fırsatlar ortaya çıkarması, kişisel verilerin korunmasına ilişkin kanuni düzenlemelerin önemini artırmaktadır. Veri işlenmesine ilişkin teknolojilerin hızlı gelişimi, temelinde verinin yer aldığı internetin hayatımızın merkezine yerleşmesi, kişisel verilerin korunmasına ilişkin hukuki çerçevenin hem önemini artırmakta, hem de ekonominin tüm aktörlerini dikkate alan dengeli bir yaklaşımla oluşturulmasını zorunlu kılmaktadır.

Türkiye, bilgi ve iletişim teknolojileri sektöründe son yıllarda yaptığı atılımlarla oldukça önemli yol kat etmiş ve sektörün kendisi geliştiği gibi diğer sektörlere de küresel düzlemde rekabetçi olmaları yolunda önemli bir katkı sağlamıştır. Dolayısıyla KVKK ile yurtdışına veri aktarımının AB mevzuatına uygun yöntemlerin kabul edilerek önünün açılması bu noktada büyük önem taşımaktadır.

KVKK da ve ulusalüstü normlarda sınır aşan veri kavramına yer verilmesi ve bu hususta düzenleme yapılmasının çeşitli nedenleri bulunmaktadır. Bu konuda düzenleme yapmayı gerektiren bu nedenleri şu şekilde sıralayabiliriz:

- Ana şirket serverlarının yurt dışında bulunması ve Türkiye'de faaliyet gösteren bağlı şirketin grup şirketinin serverından ayrılmasının hem teknik hem operasyonel sebeplerle mümkün olmaması,

[4] Örneğin Amerika Birleşik Devletleri Hükümeti, ABD Vatanseverlik Yasası, Yurtiçi Güvenlik yasası ve benzeri yasaları kullanarak, her türlü elektronik veriye erişebilmektedir.

- Veri koruma standartlarının bağlı bulunduğu şirketler topluluğunun (çokuluslu şirketler) serverların yer aldığı ülkede daha üst düzeyde olması,

- Bulunduğu ülkede daha düşük maliyetlerle verileri koruma ve yönetme imkânının bulunması.

Söz konusu nedenler dikkate alındığında yabancı yatırımcının ülkeye çekilmesi; teknolojinin dolaşımı ve aynı zamanda teknoloji üreten milli üreticinin de yurtdışına açılması için sınır aşan veri hususunda tatmin edici bir düzenlemenin varlığı önem arz etmektedir. Aksi halde verilerin yurtdışına aktarılmasında gereksiz sıkıntı yaşanması; belirsizliklerin söz konusu olması; sorunların kısa bir süre içinde çözümlenememesi hem ulusal hem de çokuluslu yatırımcıların yatırım kararlarını olumsuz yönde etkileyecektir.

3.5 Türk Hukukunda Verilerin Yurtdışına Aktarılmasının Sınırları

Ülkemizde, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleyerek hem gerçek ve tüzel kişilere hukuki güvence getiren; kişisel verilerle katma değerli hizmetler sunan şirketlere de ekonomik anlamda değer katan düzenleme 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) dır.

6698 sayılı Kanun'da "*Kişisel verilerin yurt dışına aktarılması*" başlıklı 9 uncu maddede Sınır aşan verilerle ilgili bir düzenlemeye yer verilmiştir:

> "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.
>
> (2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;
>
> a) Yeterli korumanın bulunması,
>
> b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,
>
> kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.
>
> (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.
>
> (4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;
>
> a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri,
>
> b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,
>
> c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,
>
> ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,
>
> d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri,

değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

(5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

Söz konusu hükme göre "**genel kural**"; kişinin açık rızası olmadan kişisel verisinin yurt dışına aktarılamayacağıdır.

Genel "**kuralın istisnası**" olarak kişilerin açık rızası aranmaksızın, yeterli korumanın bulunması ya da Kurul'un izni olması ve Türkiye'deki ve yurt dışındaki veri sorumlularının yazılı taahhüdü ile ancak şu hallerden biri varsa verinin yurtdışına aktarılması mümkündür:

- Kanunlarda açıkça öngörülmüşse (özel nitelikli kişisel verilerden sağlık ve cinsel hayata ilişkin olanlar ayrıca Kanun'da gösterilen amaçla ve kurum ve kişilerce tarafından),
- Kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunluysa,
- Bir sözleşmenin kurulması veya ifası için ya da bir hakkın tesisi, kullanılması veya korunması için verinin işlenmesi zorunluysa,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi ya da meşru menfaatleri için için zorunluysa,
- Veri, sahibi tarafından alenileştirilmiş ise,
- Bir hakkın tesisi, kullanılması veya korunması için zorunlu ise,
- Veri sorumlusunun meşru menfaati için veri işlenmesi zorunlu ise.

KİŞİSEL VERİLERİN YURTDIŞINA AKTARILMASI
(KVKK UYGULAMASI)

AÇIK RIZA VARSA

- **KANUNDA AÇIKÇA ÖNGÖRÜLÜYOR İSE**
- **KİŞİNİN HAYATI VEYA BEDEN BÜTÜNLÜĞÜNÜN KORUNMASI İÇİN ZORUNLU İSE**
- **SÖZLEŞMENİN TARAFLARINA AİT KİŞİSEL VERİLERİN İŞLENMESİ GEREKLİ İSE**
- **VERİ SORUMLUSUNUN HUKUKİ YÜKÜMLÜLÜĞÜ İÇİN ZORUNLU İSE**
- **KİŞİNİN KENDİSİ TARAFINDAN ALENİLEŞTİRİLMİŞ İSE**
- **BİR HAKKIN TESİSİ, KULLANILMASI VEYA KORUNMASI İÇİN ZORUNLU İSE**
- **VERİ SORUMLUSUNUN MEŞRU MENFAATİ İÇİN VERİ İŞLENMESİ ZORUNLU İSE**

VERİ YURTDIŞINA AKTARILABİLİR

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla

YETERLİ KORUMA VARSA

VERİ YURTDIŞINA AKTARILABİLİR

YETERLİ KORUMA YOKSA

Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması halinde

VERİ YURTDIŞINA AKTARILABİLİR

Sınır aşan verilerle ilgili 6698 sayılı Kanun'da söz konusu düzenleme yer almakla birlikte yurtdışına veri aktarılması bakımından gerekli olan şartlardan "**güvenli ülke ilanı**" henüz yapılmamıştır[5]. Diğer taraftan Kurul'un 31.05.2019 tarihli ve 2019/157 sayılı kararı (Gmail

[5] 02.05.2019 tarihli ve 2019/125 sayılı Kurul Kararı ile Yeterli Korumaya Sahip Ülkelerin Belirlenmesinde Esas Alınacak Kriterler belirlenerek "Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan form" erişime açılmıştır.

Kararı) da konuya ilişkin olarak son derece önemlidir:

> "Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesi hükümlerine uygun olarak gerçekleştirmesine;
>
> Server'ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine karar verilmiştir."

Henüz güvenli ülke ilanının yapılmamış olduğu dikkate alındığında, 9 uncu maddede kişilerin açık rızası alınmadan yurtdışına aktarılması mümkün olan veriler, ancak Kurul'un izniyle yurt dışına aktarılabilecektir. Kurul izin prosedürünün uzun sürmesi; kararın somut başvuru üzerinden veriliyor olması, özellikle güvenli ülke ilan edilmesi muhtemel ülke yatırımcıları bakımından çekingenliğe neden olmaktadır.

3.6 Avrupa Birliği Genel Genel Veri Koruma Tüzüğü'nde (General Data Protection Regulation − GDPR) Verilerin Yurtdışına Aktarılmasının Sınırları

Bilindiği üzere 1995 yılında, AB bünyesinde veri koruma kanunlarındaki farklılıkların devletler arasındaki veri paylaşımında yasal belirsizliklere neden olması nedeniyle, bu sorunu çözmek amacıyla 95/46/AT sayılı AB Veri Koruma Direktifi yürürlüğe girmiştir. Söz konusu Direktifin veri koruma standartlarını uyumlulaştırmada yeterince başarılı olmaması üzerine 2016 yılının Nisan ayında da 95/46/AT sayılı AB Veri Koruma Direktifi yerini Veri Koruma Tüzüğü'ne (GDPR) bırakmıştır[6]. 24 Mayıs 2016 tarihinde AB üyesi ülkelere GDPR'yi kendi iç hukuklarına eklemeleri için iki yıl süre tanınmasını takiben GDPR 25 Mayıs 2018 tarihinde uygulanmaya başlanmıştır.

"*Üçüncü ülkeler veya uluslararası kuruluşlara veri aktarımları*" GDPR'nin Beşinci Bölümünde (m. 44–50) düzenlenmiştir.

GDPR'ye göre "*Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hallerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Böylesi bir aktarım için özel bir onay gerekmez*".

Görüldüğü üzere GDPR ile Komisyona, güvenli ülke belirleme yetkisi dışında güvenli bölge, güvenli kuruluş (organizasyon), güvenli sektör, güvenli uluslararası kuruluş (organizasyon)

---

[6] Bilindiği üzere tüzükler (regulations) AB üyesi her devlette hukuki zorunluluğa sahiptir ve tüm üye devletlerde belirli bir tarihte yürürlüğe girer. Direktifler (directives) ise ulaşılması gereken belirli hedefleri ortaya koyar ama üye devletler, direktiflerin ulusal yasalara nasıl dönüştürüleceğine karar vermekte serbesttir. Bu nedenle GDPR, AB Veri Koruma Direktifi'ne göre daha bağlayıcı ve etkilidir.

belirleme yetkisi verilmiştir[7]. Komisyon bu yetkisini kullanarak, "*koruma düzeyinin yeterliliği*"ni değerlendirirken 45 inci maddede belirtilen hususları dikkate alacak ve maddede belirtilen periyotlarda da yeterlilik düzeyini gözden geçirecektir.

46 ncı maddeye göre ise Komisyonun yeterli düzeyde koruma sağlandığına ilişkin bir kararı olmaması halinde de üçüncü ülkede bulunan veri sorumlusu veya veri işleyen veya uluslararası bir organizasyon tarafından **1) yeterli güvenlik düzeyinin sağlandığına dair güvencenin verilmiş olması** ve **2)** o ülkede **veri sahiplerine yönelik etkili kanun yollarının mevcut olması** koşuluyla, başkaca herhangi bir **izin aranmaksızın** üçüncü ülkede bulunan veri sorumlusu veya veri işleyen veya uluslararası bir organizasyona kişisel veri aktarabilir.

GDPR'de **hangi hallerde** (ayrıca özel bir izin alınmaksızın) "**yeterli güvenlik düzeyinin sağlandığına dair güvencenin verilmiş sayılacağı**" belirtilmiştir:

- Kamu kurumları ve makamları bakımından yasal bağlayıcılığı bulunan bir belgenin bulunması,
- 47 nci madde uyarınca hazırlanmış ve onaylanmış Bağlayıcı Şirket Kuralların (Binding Corporate Rules – BCR) bulunması,
- Komisyon veya üye ülke veri koruma otoritesi tarafından kabul edilen standart veri koruma hükümlerinin bulunması,
- Etik davranış kurallarının (Code of Conduct) bulunması ve bununla ilgili üçüncü ülke veri koruma otoritesi, veri işleyen veya veri sorumlusunun ilgili kişinin haklarının korunması dahil yeterli güvenlik seviyesinin sağlanmasına ilişkin bağlayıcı ve icra edilebilir taahhütlerinin bulunması,
- Sertifikasyon (belgelendirme) mekanizmasının bulunması ve bununla ilgili üçüncü ülke veri koruma otoritesi, veri işleyen veya veri sorumlusunun ilgili kişinin haklarının korunması dahil yeterli güvenlik seviyesinin sağlanmasına ilişkin bağlayıcı ve icra edilebilir taahhütlerinin bulunması.

Bunların yanı sıra, taraflar arasında imzalanmış (standart sözleşme hükümleri olmayan) sözleşme hükümlerinin Üye Ülke veri koruma otoritesi tarafından onaylanmış olması halinde de kişisel veriler AB dışına aktarılabilmektedir.

AB uygulaması incelendiğinde, ilgili idari makamların onay iradelerini, yayınladıkları standart prosedürlerin uygulanmasıyla (standart sözleşmeler, BCR ya da sertifikasyon gibi) ortaya koydukları görülmektedir. Veri gönderen ve veri alıcısının söz konusu standart prosedürleri uygulamayarak kendilerine özgü sözleşme hükümleri kullanmaları halinde ise onay iradesi, ilgili standart dışı sözleşmelerin incelenerek uygun bulunması yoluyla ortaya konulmaktadır. Burada dikkate değer nokta, AB uygulamasında hem standart prosedürlerin uygulanması hem de ilgili otoritelerin ayrıca onayının alınmasının bir arada aranmadığıdır. **Söz konusu yöntem**

[7] Komisyon tarafından yeterlilik kararı verilen ülkeler şunlardır: Andorra, Arjantin, Kanada (Ticari organizasyonlar), Faroe Adaları, Guernsay, İsrail, Man Adası, Japonya, Jersey, Yeni Zelanda, İsviçre, Uruguay, ABD (Privacy Shield Sertifikasyonu).

sayesinde hem yeterli denetim mekanizması kurulmuş hem de sınır ötesi veri akışının sağlanması kolaylaştırılmış olmaktadır.

Diğer taraftan AB açısından "**Genel Veri Koruma Tüzüğü**"nün 2018 yılından itibaren uygulanmaya başlaması veri koruma konusunda önemli bir kapı aralamakla birlikte, AB'li işletmeler açısından kişisel verinin tam olarak ne olduğu ve mevzuata tam uyumun nasıl sağlanacağı hususu hala belirsizliğini korumaktadır. Birlik'te öncü büyük şirketler (bilhassa perakende, sağlık, bankacılık sektörü) mevzuat ile uyum içinde görünmekle birlikte küçük ve orta ölçekli işletmelerin çoğunda durumun net olmadığı görülmektedir. Bu çerçevede alınan bir dizi önlemin uygulamada işe yarayıp yaramadığı hususunda da henüz bir tespit yapılamamıştır. Bu noktada işletmelerin temelde veri koruma hukukuyla çelişmeyen bir iş yapış süreci tesis edebilmelerinin üç temel aşamada başarılabileceği değerlendirilmektedir. Buna göre;

- İşletmenin sahip olduğu veri kaynakları ve veriye ilişkin mevcut durumunun açıkça ortaya konulması gerekmektedir.

- İşletmenin gizlilik politikalarını ve sözleşmelerini gözden geçirerek önleyici mekanizmaları doğru tesis etmesi gerekmektedir.

- İşletmede en üst seviyeden aşağıya doğru gerekli eğitimlerin alınması gerekmektedir. Bu uygulama adımlarının ardından mevzuat uyumunun sağlanması ile toplanan müşteri verilerinden tam olarak yararlanabilmenin faydası açığa çıkabilecektir.

4 ULUSLARARASI TİCARETTE/ TİCARET ANTLAŞMALARINDA VERİNİN ÖNEMİ

4.1 Hizmet Ticareti ve Sınır Aşan Veri Transferi

GATS (The General Agreement on Trade in Services) Hizmet Ticareti Genel Anlaşması'dır. 1947 yılında imzalanan GATT-Tarifeler ve Ticaret Genel Anlaşması kapsamında 1986-1994 yıllarında yapılan Uruguay Görüşme Turunda GATT'a dahil edilmiş ve 01.01.1995 tarihinde resmi olarak faaliyete geçirilen Dünya Ticaret Örgütü (DTÖ) bünyesine aktarılmış olan hizmet ticaretini düzenleyen ilk çok taraflı anlaşmadır. Türkiye 1994 GATS anlaşmasına DTÖ kurucu üyesi olarak imza atmış ve anlaşma TBMM'de 25.02.1995'te onaylanmıştır.

GATS çerçevesinde hizmet ihracatı (ticareti), "**sınır ötesi hizmet sunumu**" (mod 1), "**yurtdışında tüketim**" (mod 2), "**ticari varlık**" (mod 3) ve "**gerçek kişilerin varlığı yoluyla hizmet arzı**" (mod 4) olarak tanımlanan dört biçimde yapılmaktadır. Bunlardan "sınır-ötesi hizmet sunumu (cross-border service suplly) bir ülkede kurulmadan o ülke topraklarına uzaktan hizmet sunmak anlamına gelmektedir. Başka bir ifadeyle hizmetin bir ülkeden diğer ülkedeki tüketiciye (hizmeti sunan ve hizmetten yararlananın kendi ülkelerinden ayrılmadan) sağlanmasını ifade eder. Burada sınırı geçen hizmetin kendisidir. Uzaktan online veri işletimi ve veri tabanı hizmetleri, her türlü elektronik vb. teknolojik ortamda sağlanan danışmanlık, muhasebe, mali vb. hizmetler. Dizi−film, uzaktan eğitim, bulut bilişim, yazılım, telekomünikasyon, rezervasyon hizmetleri, paylaşım platformları, oyunlar, arama motoru ve sosyal medya üzerinden reklamcılık gibi hizmetler **sınır ötesi hizmet sunumuna örnek**

olarak verilebilir.

Sınır ötesi hizmet sunumu için uluslararası veri transferi olmazsa olmaz bir araç olup verinin "belirli bir kalitede, hızda ve engellenmeden" transferi bu hizmetlerin "pazara girişi (market access)" için son derece önemlidir. Bu çerçevede hizmet ticaretinde pazara giriş ticaret anlaşmaları kapsamında bir müzakere konusu olduğundan, sınır-ötesi hizmet sunumuna ilişkin olarak da veri transferi başlı başına bir pazarlık unsuru olarak anlaşmalarda yer alabilmektedir.

4.2 Küresel Değer Zincirlerinin İşleyişi ve Sınır Aşan Veri Transferi

Çok uluslu işletmeler (Multinational Enterprise-MNE) başta olmak üzere, ticaret partnerleri, iştirakler, şubeler, müşteriler ve tedarikçiler arasında (kişisel olmayan) kurumsal bilginin paylaşımı ile kişisel verinin de paylaşımı gerekmektedir. Örneğin ana üretim/montaj hattı bir ülkede olan başka ülkelerden ara mal, hammadde ve hizmet tedariki yoluyla üretim süreçlerini sonuçlandıran büyük bir MNE; envanter/stok denetimi, lojistik izleme, insan kaynakları, müşteri ilişkileri yönetimi gibi bilgi işlem ihtiyaçlarını düşük maliyet sunan bulut bilişim kullanarak çözmekte, iştirakleri ve ticaret ortakları arasında daimi bilgi transfer etmektedirler. Başka bir ifadeyle MNE'ler için üretim ve ticaret süreçlerinin aksamaması için veri transferi büyük önem arz etmektedir. Bu anlamda, veri transferi küresel değer zincirleri kapsamında mal ve hizmet ticaretini etkilemekte ve bu sebeple ticaret anlaşmalarının da konusu olmaktadır.

4.3 Büyük Veri Analizi Sonucu Üretilen Mal ve Hizmetler İçin Girdi/Hammadde ve Sınır Aşan Veri Transferi

"Veri" günümüzde artık kıymetli bir doğal kaynaktır ve yeterince büyük olduğunda kendi başına katma değer yaratan bir ürüne, hizmete ya da fikri mülkiyet hakkına dönüşmektedir.

ABD Uluslararası Ticaret Komisyonunun raporuna göre 2011 yılında dijital ticaretin yarattığı değer gayrısafi milli hasılanın % 5'ine denk gelmekte 2.5 milyon kişiye istihdam yaratmaktadır. Yine McKinsey tarafından yapılan bir çalışmaya göre uluslararası veri transferinin yarattığı ekonomik değer 2014 yılında 2,8 trilyon dolar olarak gerçekleşmiş ve söz konusu yıl itibariyle toplam dünya mal ticaretinin yarattığı değeri geçmiştir.

Bu açıdan bakıldığında da "veri" konusu, ticaret anlaşmalarında başlı başına bir talebe dönüşmekte ve serbestleştirilmesi için hükümler müzakere edilmektedir.

Aslında "veri" konusunda uluslararası kurallara duyulan ihtiyaç sebebiyle G-20, OECD ve APEC gibi platformlarda bildirgeler, rehberler vs. görüşülmekte; ancak bunların hiçbiri ülkeler için bağlayıcı kurallar içermediğinden konu "anlaşmazlıkların halli (dispute settlement)/tahkim (arbitration)" mekanizmaları yoluyla yaptırım içeren "ticaret anlaşmaları" müzakerelerine taşınmaktadır. Bu müzakereler, ikili (serbest ticaret antlaşmaları−STA'lar ve diğer ikili anlaşmalar), çoklu (Trade in Services Agreement−TiSA) ya da çok taraflı (DTÖ) platformlarda yürütülmektedir.

5 TİCARET ANLAŞMALARINDA "VERİ" İLE İLGİLİ TARTIŞMALAR

Dünya Ticaret Örgütü (DTÖ)'nün bazı üyeleri, Hizmet Ticareti Genel Anlaşması'nda (GATS) yer alan hükümlerin veri transferini (sınır ötesi hizmet sunumu için pazara giriş unsuru olarak) kapsadığını, dolayısıyla veri transferine ilişkin yeni hükümlere ihtiyaç olmadığını iddia etmektedirler. Diğer taraftan, GATS kapsamında üstlenilen sektörel taahhütler yetersiz görülmekte, sektör tanımlarının yeni gelişen hizmetleri (bulut bilişim, sosyal medya gibi) sınıflandırmakta kullanılamadığı öne sürülmekte ve GATS'ın yalnızca hizmet ticaretini etkileyen önlemlere uygulanması sebebiyle dar kapsamlı kalabileceği de karşı argümanlar olarak dile getirilmektedir.

Bu sebeple, yeni nesil kapsamlı Serbest Ticaret Anlaşmaları (STA)'nda "mal ve hizmet" ticaretini bir arada ele alan ve özetle elektronik yolla yapılan tüm ticareti kapsayan müstakil (stand-alone) "E−ticaret" fasılları bulunmakta ve "veri" ile ilgili hükümlere de burada yer verilmek suretiyle yukarıda ifade edilen tartışmaya mahal bırakmayacak şekilde yatay kurallar geliştirme yoluna gidilmektedir.

Kendi başına müstakil bir fasıl olarak E-ticaret fasıllarında (Chapter on E−commerce) ya da "Hizmet Ticareti" faslının Eki olan E-ticaret eklerinde (Annex on E−commerce), "sınır ötesi veri transferi (cross border data flows)" ve/veya "verinin yerelleştirilmesi (data localization)" başlıklı maddeler bulunmakta ve söz konusu maddelerde; "*Taraflardan hiçbiri veriye erişimi, verinin depolanmasını ve verinin transferini engelleyecek bir önlem almayacaktır*" şeklinde ifade edilen "veri serbestisi" yükümlülüğü yer almaktadır.

Bu noktada belirtmek gerekir ki "veri transferi serbestisi" ile "güvenlik" ve "gizlilik" gibi kamusal amaçlarının "ticareti en az etkileyecek (least trade−restrictive)" şekilde dengelenmesi gerektiğinden, öneri metinleri incelendiğinde "meşru kamu politikası amaçları (legitimate public policy objectives)" kapsamında veri akışının sınırlandırılması ve veri merkezlerinin konumuna ilişkin düzenlemelerin de yapıldığı görülmektedir.

Bununla birlikte, anlaşmazlıkların halline/tahkime gidecek bir süreçte hangi politikanın meşru kabul edileceği, düzenlemenin ticaretin önünde zımni bir engel olup olmadığı ve orantılı bir düzenleme yapılıp yapılmadığı, (uyuşmazlığı çözmeye yetkili) heyetin kararına bağlı olabilecektir. Bu anlamda, ticari korumacılıkla meşru politika önlemlerinin ayırt edilebilmesi gibi üst üste binen bazı önlemlerin hangi amaca hizmet ettiğine heyet karar verecektir ki böylesi önemli bir hususu heyet yorumuna bırakmayı birçok ülke, egemenlik hakkının ihlali olarak görmektedir.

6 ÜLKELERİN TİCARET MÜZAKERELERİNDE "VERİ TRANSFERİ" KONUSUNDA POZİSYONLARI

Bugüne kadar "veri serbestisi"ne ilişkin en geniş hükümler CPTPP (Comprehensive and Progressive Agreement for Trans−Pacific Partnership) anlaşmasında yer almıştır. Esasen anlaşmanın adı TPP iken ABD'nin Trump yönetimi altında anlaşmadan çekilmesinden sonra 11 Asya−Pasifik ülkesinin imzacı olduğu CPTPP adını almıştır. Anlaşmanın "*E-ticaret Faslı*", "*sınır ötesi veri akışı*" "*verinin yerelleştirilmesi*" ve "*kişisel verilerin korunması*" gibi veriye ilişkin yükümlülükler ile "*istisna*" maddelerini içermektedir. Hemen belirtmek gerekir ki veriye ilişkin

bu yükümlülükler "mali hizmetler" söz konusu olduğunda uygulanmayacak şekilde tasarlanmıştır. Bunun sebebi; ABD'de ticaret müzakerelerinden sorumlu USTR (United States Trade Representative − Amerika Birleşik Devletleri Ticaret Temsilciliği Ofisi) ile mali hizmetlerin düzenlenmesinden sorumlu US Treasury (United States Department of the Treasury − Amerika Birleşik Devletleri Hazine Bakanlığı) arasında ortak bir politika belirlenmemiş olmasıdır.

TPP/CPTPP Anlaşmasıyla eşanlı olarak ülkemizin de içinde yer aldığı TiSA müzakereleri devam etmiştir[8]. TiSA yalnızca hizmet ticaretini kapsayan çoklu bir anlaşma girişimidir. TiSA'da da ABD'nin talebiyle "*veri transferi serbestisi*" ve "*verinin yerelleştirilmesini yasaklayan*" hükümler müzakere edilmiştir. 2016 yılı sonunda ABD seçim sonuçlarının ardından müzakereler askıya alınmıştır.

Benzer şekilde yeni NAFTA olarak da adlandırılan USMCA (ABD−Meksika−Kanada Anlaşması) ve Japonya-ABD arasında imzalanan STA içerisinde de "Dijital Ticaret" başlıklı bir fasıl ve altında veri serbestisine yönelik iddialı hükümler yer almıştır.

DTÖ bünyesinde ise Ocak 2019 itibariyle "E−ticaret Müzakereleri" altında "veri transferi" hususu en önemli başlık olarak müzakere edilmeye devam edilmektedir.

Ticaret anlaşmaları müzakerelerine bakıldığında "verinin serbest dolaşımı" başta olmak üzere dijital hizmetlerin sunumuna yönelik engellerin kaldırılmasını isteyen başlıca ülkeler; dijital dönüşüm alanında önde, büyük veri analizi yapabilen ve piyasaya hâkim dijital şirketleri olan gelişmiş ülkelerdir. Hâlihazırda bu ülkeler DTÖ E—ticaret Müzakerelerini başlatan ABD, Japonya ve Singapur'dur. Bu ülkelerle daha önce bir STA imzalamış ülkeler (örneğin Latin Amerika ülkeleri) ise iktisadi anlamda "veri" konusunda talepkâr olmamakla birlikte başka bir anlaşmada kabul etmiş olmalarından dolayı itiraz da etmemekte, hatta bazı durumlarda kendileriyle benzer durumda olanları artırma çabası içine girerek talepkâr ülkelerin yanında yer alabilmektedirler.

Bu müzakerelerde, ülkemiz açısından dikkatle takip edilmesi gereken husus AB'nin pozisyonu ve "veri" konusuna yaklaşımıdır. AB, uzun bir süre boyunca "veri" konusunun ticaret anlaşmalarında müzakere edilemeyeceğini iddia etmiş ve "veri" konusunda bağlayıcı hükümler içeren maddeleri müzakere dahi etmemiştir. Ancak AB, Mayıs 2019'da bu pozisyonunu değiştirmiş ve "veri merkezlerinin yerelleştirilmesi" konusunda ABD'den bile daha iddialı bir öneri sunmuştur. Bu şekilde AB, "veri" konusunun ticaret müzakerelerinin önemli bir gündem başlığı olduğunu kabul etmiş ve bu alanda talepkâr ülkeler tarafına geçmiştir.

AB'nin DTÖ E−ticaret Müzakereleri kapsamında sunduğu öneri incelendiğinde sınır ötesi veri transferinin "*veri merkezlerinin yerelleştirilmesi*" önlemleriyle engellenemeyeceğini ifade etmektedir. AB'nin yaklaşımına göre "veri merkezlerinin ülke içinde kurulmasını zorunlu tutmak" ya da "verilerin başka bir ülkede tutulmasını yasaklamak", "sınır ötesi veri transferi"ni engelleyen bir önlemdir. AB'ye göre, mevcut durumda konunun ticaret boyutu "verinin yerelleştirilmesi"nden ibarettir. Diğer taraftan,

[8] Hizmetlerde Ticaret Anlaşması (Trade in Services Agreement), Avrupa Birliği ve ABD de dahil olmak üzere 23 Taraf arasında önerilen uluslararası bir ticaret anlaşmasıdır. Anlaşma, bankacılık, sağlık ve ulaştırma gibi dünya çapında hizmet ticaretini serbestleştirmeyi amaçlıyor.

AB başlı başına "serbest veri transferi" hükmünü (kişisel verilerin güvenliği konusundaki hassasiyetler sebebiyle) hala kabul etmemektedir.

Ticaret müzakerelerinde "veri" konusuna "defansif" ve/veya "hassas" yaklaşan ülkelerin başında ise Çin, Rusya ve Türkiye gelmektedir.

7 ÇEŞİTLİ ÜLKELERDE VERİ TRANSFERİ KONUSUNDA TARTIŞMALAR

Veri transferini engelleyen ülkeler arasında Çin birinci sırada yer almaktadır. Çin'i Rusya, Hindistan, Endonezya, ve Vietnam izlemektedir. Aynı endekste ABD 22. sırada olup mali hizmetler konusundaki önlemleri sebebiyle Kanada ve Avustralya'dan daha kısıtlayıcı bir ülke olarak ortaya çıkmaktadır.

Veri transferinin yanı sıra veri yerelleştirilmesi, verinin belli süre tutulması gibi diğer engellerin de katıldığı kompozit endekste ise 64 ülke arasında en kısıtlı ülke Rusya olmuştur. Rusya'yı Türkiye ve Çin takip etmektedir.

Burada incelenmesi gereken en önemli iki yaklaşım Çin ve AB'nin yaklaşımlarıdır. Çin "veri" konusuna "milli güvenlik (security)", AB ise "gizlilik (privacy)" gözlüğüyle bakmaktadır.

AB, kişisel verilerin gizliliğini temel insan hakkı olarak görmekte ve korunması için çok detaylı bir düzenleme olan GDPR (General Data Protection Regulation) düzenlemesini uygulamaktadır. Verinin AB dışına transferi söz konusu olduğunda "koruma" hükümlerine uygun olarak transferine izin vermektedir. Öte yandan, AB bunun dışında kalan verinin yerelleştirilmesi önlemlerini yasaklayan bir dizi mevzuat değişikliği yapmış ve üye ülkelerin de 2020 yılına kadar verinin yerelleştirilmesine yönelik önlemlerini kaldırmalarını öngörmüştür. Esasen Almanya ve Fransa başta olmak üzere birçok AB üyesinin yerelleştirme yani veri merkezlerini ülke içinde kurma ve işleme zorunlulukları bulunmaktadır. Bunlar özellikle mali hizmetler, sağlık, vergiye yönelik muhasebe bilgileri, uydu verileri ve devlet verisi için geçerlidir. Ancak AB Komisyonu etki analizi değerlendirmesi sonucu bu önlemler nedeniyle ticari kaybın çok olduğuna ve AB'nin dijital ekonomide rekabetçiliğini yitirdiğine kanaat getirdiğinden verinin yerelleştirmesini zorunlu tutan önlemleri yasaklamıştır. AB içerisinde uygulanması öngörülen söz konusu yasağın DTÖ E−ticaret müzakerelerine de yansımaları olmuş ve AB bu konuda benzer bir öneriyi DTÖ müzakere masasına taşımıştır. Oysa 2015-2016 yıllarında TiSA müzakereleri, AB'nin "veri" konusundaki hassasiyeti sebebiyle uzamış; müzakereler boyunca AB "veri" konusunun ticareti aşan boyutları olduğunu belirtmiştir. AB'nin hızla değişen bu yaklaşımının ülkemizce takip edilmesi AB ile iş yapan ülkemiz yatırımcıları açısından son derece önemlidir.

Çin'in aldığı önlemler, milli güvenlik saikiyle aldığı kısıtlamalardan oluşmaktadır. Örneğin, Çin'e akan ya da Çin'den dışarı çıkan tüm internet trafiği bir "firewall" denetiminden geçerek transfer edilmektedir. "Büyük Çin Ateş Seddi (Great Firewall of China)" olarak da adlandırılan bu sistem, verileri anahtar kelime bazında tarayarak incelemeye almakta ve onay verildikten sonra geçişine izin verilmektedir. 2015 tarihli "terörizmin önlenmesi kanunu" tüm telekomünikasyon operatörlerine ve internet erişim sağlayıcılarına bireylerin tüm verilerini Çin hükümeti ile paylaşma zorunluluğu getirmektedir. Bunların dışında, "internet egemenlik politikaları" "siber

güvenlik kanunu" "kişisel bilgi güvenlik tespiti kanunu" şirketlere verilerini Çin'de tutma ve işleme zorunluluğu getirerek uluslararası veriye erişim, verinin kullanılması ve transferine engel oluşturmaktadır.

2014 yılında Çin, şirketlerin ve bireylerin davranışlarını şekillendirmek amacıyla bir "sosyal kredi sistemi" oluşturacağını, "güvenilir" vatandaş ve şirketlerin devlet hizmetlerinden daha fazla ve daha ucuza faydalanmasını sağlayacağını açıklamıştır.

DTÖ Hizmet Ticareti Konseyi toplantılarında Çin'in aldığı önlemler son zamanlarda sürekli gündeme getirilmekte ve eleştiri konusu yapılmaktadır. Çin, 2019 Ocak ayı itibariyle başlayan DTÖ E-ticaret İnisiyatifi müzakereleri kapsamında yayımladığı pozisyon kâğıdında "veri" konusunu konuşmayacağını belirtmiştir. Vietnam, Endonezya ve Hindistan gibi ülkeler de Çin'in aldığı önlemlere benzer düzenlemeler yürürlüğe koymaktadırlar.

8 SINIR AŞAN VERİ TRANSFERİ / VERİNİN BAŞKA ÜLKEDE TUTULMASI İLE İLGİLİ SINIRLAMALARIN DAYANAKLARI

Sınır aşan veri transferi ve verinin başka ülkelerde tutulması ile ilgili sınırlamanın dayanaklarını şu şekilde sıralayabiliriz:

- **Kişisel verilerin güvenliği ve gizliliği**

Devletler vatandaşlarının kişisel verilerinin kötüye kullanılmadığından, kişilerin rızası dışında işlenmediğinden ya da başka kişilerle paylaşılmadığından emin olmak istemekte, vatandaşlarının kişisel verilerinin gizliliğini korumanın devletin temel görevlerinden olduğunu değerlendirmektedirler.

- **Ulusal güvenlik ve kamu düzeninin korunması**

Devletler vatandaşlarının arama ve mesajlaşma kayıtları, lokasyon ve harita bilgileri, mali işlem bilgileri (financial transactions) gibi verilere "ulusal güvenlik"le ilgili durumlarda anında erişebilmek istemekte ve bu verilerin belli siber−güvenlik standartlarında korunduğundan emin olmak istemektedirler. Yine sosyal medyanın halkı yönlendirmede araç olarak kullanıldığı, sivil hareketlere yol açabildiği düşünüldüğünden, bu tür risklerin ortaya çıktığı düşünüldüğünde internet erişimi kısıtlamak, veri transferini engellemek eğilimi sergilemektedirler.

Bunun dışında, azınlık, dezavantajlı ve kırılgan gruplarla ilgili "nefret söylemi" içeriğine sahip web sitelerinin de yine manipülasyona yol açması durumunda kamu düzeninin korunması için veriye erişim ve veri transferinin engellenmesi söz konusu olabilmektedir.

Dayanaklardan bir diğeri de "**ahlakın ve ulusal değerlerin korunması**"dır. Bu çerçevede kumar siteleri ve cinsel içerikli sitelere erişim mahkeme kararıyla engellenebilmekte, ulusal değerlerin korunması ve tarihe ilişkin yanıltıcı bilgilerin yer alması durumunda da veriye erişim ve veri transferi engellenebilmektedir.

- **Siyasi etkiler**

Günümüzde sosyal medya, yeni "radyo−televizyon" olarak görülmekte ve kitleleri yönlendirme aracı olarak kullanılabilmektedir. Özellikle, siyasi parti seçimleri gibi hassas dönemlerde elde edilen veriler, seçim sonuçlarını etkilemek amacıyla kullanılabilmektedir. Bu gibi riskler sebebiyle, verinin yurt içinde tutulması, bazı dönemlerde veri transferinin yavaşlatılması/engellenmesi ya da yerli hizmet sunucuların tercih edilmesine yönelik önlemler alınabilmektedir.

- **Siber güvenlik ve kritik önemi haiz altyapı ve hizmetlerin güvenliği**

İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran alt yapılara **kritik alt yapı**, bu alt yapılar üzerinden sunulan hizmetlere de **kritik hizmet** denilmektedir. Söz konusu alt yapı ve hizmetlerin devamlılığını ve güvenliğini sağlamak üzere alınan önlemler, siber güvenlik önlemleridir.

Kritik alt yapı ve hizmetlerin tanımı her ülke için değişmektedir. Ülkemizde; 20.06.2013 tarih ve 2 Sayılı Siber Güvenlik Kurulu Kararı uyarınca "*elektronik haberleşme*", "*enerji*", "su yönetimi", "*kritik kamu hizmetleri*", "*ulaştırma*", ve "*bankacılık ve finans*" sektörleri kritik alt yapı sektörleri olarak tespit edilmiştir. 2016-2019 Siber Güvenlik Stratejimiz kapsamında, belirlenen sektörlerde verinin ülke içinde tutulması, transferi ve erişime yönelik önlemler alınabileceği ile yerli ürün ve hizmet kullanımına öncelik ve teşvik verileceği belirtilmektedir.

- **Terörle, kara paranın aklanmasıyla ve suçla mücadele**

Özellikle mali hizmet sunucularının, bilgi işlem sistemlerini ülke içinde kurmaları, belirli bir süre geriye dönük olarak veriyi yine ülke içinde kurumların her an erişebileceği ve belli standartlarda tutmaları, terörizmin finansmanının ve kara paranın aklanmasının önlenmesi ile mücadele kapsamında suçluların tespiti açısından önem arz etmektedir.

- **Mevzuatın uygulatılması ve yaptırımlar**

Ülke içinde kurulu olmayan dijital hizmet sunucuları, ülke mevzuatına tabi olmamakta ve ulusal mevzuata aykırılık halinde bu işletmelere yaptırım uygulamada sıkıntılar yaşanmaktadır. Bu çerçevede kamu düzenini ihlal ve milli güvenlik söz konusu olduğunda ulusal mevzuat ve yargı kararları çerçevesinde veriye erişimin engellenmesi gerekli olabilmektedir.

- **Vergilendirme**

Bir ülkeye hizmet sunan şirketlerin ekonomik faaliyetlerinin uygun bir biçimde vergilendirilebilmesi ve bu minvalde gerekli denetimlerin yapılabilmesi için ticari işlemlere ilişkin bilgi ve belgelerin (fatura, mali defterler vs) belirli bir süre (ülkemizde 10 yıl) boyunca yurt içinde ve Maliye Bakanlığının her an erişebileceği şekilde tutulması gerekmektedir.

- **Dijital Ayrım/Uçurum (Digital Divide) ve Dijital Sömürgecilik (Digital Colonization) ile Mücadele/ Yerel Dijital Ekonominin Geliştirilmesi**

Dijital teknolojilere dayalı ekonomik kazanımlar gelişme yolundaki ülkeler (GYÜ) açısından

çoğunlukla sınırlı düzeyde kalmaktadır. Büyük veri, yapay zeka, 3D yazılım, IoT (internet of things) ya da robotik süreç otomasyonuna dayalı firmalar, çoğunlukla ABD ve Japonya'da toplanmış olup Batı Avrupa, Çin, ve Güney Kore gibi az sayıda ülke/bölgede ise hala rekabet açığını kapatabilmek için çalışmalar yürütülmektedir. Dünyada piyasa değeri en yüksek ilk 5 şirket dijital hizmet sunan şirketlerdir ve tamamı ABD sermayelidir.

Günümüzde veriye ulaşım, verinin toplanması, işlenmesi ve transferi uluslararası alanda mal ve hizmet ticareti yapan her türlü firma için bir ihtiyaç ve öncelik haline gelmektedir.

Özellikle E−ticaret firmaları açısından veri, müşteri tercihlerinin anlaşılması ve kullanıcıya özel dijital pazarlama tekniklerinin kullanılması açısından elzemdir. Daha fazla veri daha etkin analiz ve öngörü anlamına gelmekte, piyasaya ilk giren firma avantajı artmakta, ayrıca network etkisi ile daha fazla kişiye hitap eden firmalar daha fazla kullanılmakta (örneğin facebook, whatsApp vb.) bu da daha fazla veri anlamına gelmekte ve kendi kendini besleyen bu süreç belli firmaların hâkim duruma yükselmesine neden olmaktadır.

Sanayileşmiş ülkeler tarafından firmalarının piyasaya ilk giren avantajlarının ve bu sayede elde edilen kazanımlarının korunması için STA'lar yoluyla dijital ticaretin tamamen liberalleşmesinin amaçlandığı görülmektedir. Diğer taraftan, gelişme yolundaki ülkelerin de kendi yerli dijital şirketlerini geliştirme yönünde adım attıkları, hatta yukarıda sayılan bazı meşru önlemlerin "de facto" yabancı hizmet sunucuları dışarıda bırakması sebebiyle yerli firmaları kayırdığı ve geliştirdiği görülmektedir.

9 SINIR AŞAN VERİ TRANSFERİ / VERİNİN BAŞKA ÜLKEDE TUTULMASI İLE İLGİLİ ÜLKEMİZİN YAKLAŞIMI

Ülkemizin de dahil olduğu gelişmekte olan ülkeler tarafından gerek ikili gerek çoklu ticaret müzakerelerinde dijital ekonominin en önemli değeri olarak görülen "veri"nin hem kalkınma hem de ulusal güvenlik amaçlarıyla ülke içinde muhafaza edilmesi talep edilebilmektedir.

6698 sayılı Kişisel Verilerin Korunması Kanunu Yukarıda belirtildiği üzere kişisel verilerin yurt dışına aktarılmasını kişinin rızasına bağlamış; 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması halinde ilgili kişinin açık rızası aranmaksızın da yurt dışına aktarılabilmesine imkân tanımıştır. Yeterli korumanın bulunmaması durumunda ise Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması halinde verinin aktarılmasını mümkün kılmıştır.

Yeterli korumanın olduğu ülkeler henüz belirlenmediğinden, kişisel verilerin transferi hususunda hukuki belirsizlik hâkim olup, konuyla ilgili politika netleşmeden herhangi bir anlaşmayla kurumların politika alanına müdahalenin doğru olmayacağı değerlendirilmektedir.

Kişisel olmayan verilerle ilgili ise yatay bir mevzuat bulunmamakta, birtakım özel kanunlarda verilerin yurt içinde tutulması veya transferinin belli şartlara bağlanmasına dair hükümler yer almaktadır. Bu çerçevede örneğin, ödeme kuruluşlarına belge ve kayıtlarını yurt içinde saklama zorunluluğu getiren 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" çerçevesinde lisans

başvurusunda bulunan ödeme sistemi sunucusu Paypal'ın başvurusu, bu koşulu sağlamaması nedeniyle, kabul edilmemiş ve Paypal ülkemizdeki faaliyetlerini durdurmuştur.

Bilgi sistemlerinin düzenlenmesi ve denetlenmesine yönelik çalışmalar yapan düzenleyici kurumlardan biri de Sermaye Piyasası Kurulu'dur ("SPK"). Bu çalışmalar kapsamında halka açık ortaklıklar da dahil olmak üzere SPK'nın düzenleme ve denetim yetkisi kapsamında olan kurum ve kuruluşlara yönelik olarak 5 Ocak 2018 tarihinde Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) ("Tebliğ") yayınlanmıştır. Anılan Tebliğ ile söz konusu kurum ve kuruluşların birincil sistemlerinin yurtiçinde bulundurulması zorunluluğu getirilmiştir.

Tebliğ'in yayınlanmasından kısa bir süre sonra, söz konusu zorunluluğun halka açık ortaklıklar tarafından hem derhal, hem zaman içerisinde uygulanması açısından bir takım belirsizliklerin ve bu sebeple de uygulamada sorunların olabileceği görülmüştür.

Gündeme gelen öncelikli sorunlardan biri söz konusu halka açık ortaklıkların birçok farklı sektörde faaliyet göstermeleri nedeniyle getirilen yükümlülüğün halka açık ortaklığın iştigal ettiği her bir sektör bakımından farklı neticeler doğurması olmuştur. Bir diğer sorun birincil sistem kavramı içerisine hangi sistemlerin girdiğinin net bir şekilde belirli olmamasıdır. Yine bir başkası da maliyet ve hizmet kalitesi endişeleri nedeniyle gerek Türk gerek uluslararası yatırımcıların rekabet gücünün zayıflamasıdır.

Yukarıda açıklanan belli başlı problemlerin yeniden gözden geçirilmesi neticesinde SPK tarafından 8 Mart 2018'de yayınlanan i−SPK.62.1 (01.03.2018 tarihli ve 9/327s.k.) sayılı İlke Kararı ile birlikte birincil sistemlerin yurtiçinde tutulması yükümlülüğünün halka açık ortaklıklar açısından şu aşamada bulunmadığı ifade edilmiştir. Ancak İlke Kararında, ilgili yükümlülüğün kapsamının tedrici olarak genişletilmesinin planlandığı da ifade edilmiştir. Yükümlülüğün genişletilmesine yönelik bu ifadenin yarattığı belirsizlik ortamı, yatırımcılar üzerinde olumsuz etkiler yaratmaya devam etmektedir.

433 sıra nolu Vergi Usul Kanunu Genel Tebliğine göre; mükellefler elektronik fatura bilgilerini; kendi bilgi işlem merkezlerinde ya da GİB'den izin almış Türkiye'de yerleşik kuruluşlarda ilgili bulundukları yılı takip eden takvim yılından başlayarak beş yıl süre ile muhafaza etmeye mecburdurlar.

27 Eylül 2001 tarihinde New York'ta imzalanan "Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme"nin 18/(iv) hükmüne göre malî kurumların ulusal veya uluslararası işlemlere ilişkin tüm gerekli belgeleri asgari beş yıl saklamaları gerekmektedir.

Elektronik Haberleşme Kanunu çerçevesinde tespit edilen verilerin, internet erişim sağlayıcıları tarafından ülke içinde ve belli bir süre tutulması gerekmektedir. Yine elektronik sertifika hizmet sağlayıcılarının kendi imza oluşturma ve doğrulama verileri ile sertifikalarını Türkiye Cumhuriyeti sınırları içerisinde oluşturması ve imza oluşturma verisini hiçbir şekilde bu sınırların dışına çıkarmaması gerekmektedir. Kayıtlı elektronik posta hizmet sağlayıcılarının Kayıtlı Elektronik Posta Sistemine ilişkin ana ve yedek sistemlerini Türkiye Cumhuriyeti sınırları içerisinde bulundurmaları gerekmektedir. Elektronik tebligata ilişkin yapılan düzenlemeler ile elektronik tebligata ilişkin PTT tarafından kurulan ana ve yedek sistemlerin, Türkiye Cumhuriyeti mülki sınırları içerisinde bulundurulması gerekmektedir.

Son olarak Cumhurbaşkanlığının 2019/12 sayılı "Bilgi ve İletişim Güvenliği Tedbirleri" konulu Genelgesi de bazı verilerin ülke içinde tutulması, yerli yazılım ve yerli hizmet sağlayıcılar ile çalışılması ve bulut−bilişim hizmeti alınmamasına ilişkin bazı hükümler içermektedir.

Halihazırda yürürlükte olan mevzuat dışında, Sayın Cumhurbaşkanımız tarafından birçok konuşmasında "veri" konusunun hassasiyetine değinilmekte ve kamu kurumları başta olmak üzere herkesin Türk vatandaşlarının verileri konusunda dikkatli olmaları gerektiği belirtilerek, milli teknoloji ve dijital Türkiye vurgusu yapılmaktadır. Bu çerçevede Cumhurbaşkanımız örneğin 24 Ocak 2019 tarihinde Kara Harp Okulu Harita Genel Müdürlüğü Küre Uygulamaları tanıtım töreninde yaptığı konuşmasında "*kendi ürettiğimiz verinin ülkemizin kontrolünde olması da siber dünyadan gelecek saldırılara karşı gereken tedbirlerin alınması da başlı başına bir milli güvenlik meselesidir*" ifadelerine yer vermiştir.

Bütün bunlar dikkate alındığında ülkemizde verinin yerelleştirmesini zorunlu tutan −bir kısmı yeni yürürlüğe girmiş− bir yasal düzenleme olduğunu söylemek mümkündür. Buna bağlı olarak her geçen gün resmi kurumlarda "veri"ye ilişkin hassasiyet de artmaktadır. Kişisel verilerin transferi konusunda ise "güvenlik ve gizlilik" ilkeleri çerçevesinde transferin mümkün olduğu kabul edilmekle birlikte, uygulamaya yönelik kriterlerin belirlenmemiş ve bu konuda yerleşik bir uygulamanın da olmadığını söylemek yanlış olmayacaktır.

Bundan sonraki süreçte; verinin yerelleştirilmesi önlemlerinin kaldırılmasına yönelik yeni AB politikasının ülkemizce yakından takip edilmesi, arka planının tüm dijital tek pazar stratejisi çerçevesinde detaylı olarak incelenmesi ve AB'nin verinin yerelleştirilmesi konusundaki endişelerinin başka yollarla giderilip giderilmediğinin tespit edilmesi önemlidir.

10 ÖRNEK MEVZUAT İNCELEMESİ: AB SERBEST VERİ AKIŞI TÜZÜĞÜ

Avrupa veri ekonomisinin sağladığı büyüme ve yenilikçiliğin, AB ülkelerinde uygulanmakta olan verinin sınır ötesi serbest dolaşımını engelleyen düzenlemeler ve uygulamalar dolayısıyla yavaşlayabileceği öngörülmektedir. Bu sebeple Avrupa Komisyonu AB'de kişisel olmayan verilerin serbest dolaşımını öngören bir tüzük önerisi sunmuştur. Söz konusu Tüzük (Regulation on a Framework for the Free Flow of Non-Personal Data in the EU−Serbest Veri Akış Tüzüğü) 14 Kasım 2018 tarihinde kabul edilmiş, Mayıs 2019 itibarıyla da yürürlüğe girmiştir. Serbest Veri Akış Tüzüğü, GDPR kapsamında tanımlanan kişisel veriler dışında kalan tüm elektronik verilerin işlenmesi bakımından geçerli olacaktır. Bu düzenleme, kişisel verilere uygulanan temel yasal çerçeve olan GDPR'nin uygulama alanı dışında kalan alanın düzenlenmesini ve ihtiyaç duyulan çerçevenin çizilmesini amaçlamaktadır. Böylece, Tüzük hem GDPR'yi hem de E−Mahremiyet Direktifini (2002/58 / EC sayılı Direktif) tamamlamayı hedeflemekte ve dijital tek pazardaki tüm verilerin serbest dolaşımı için kapsamlı ve uyumlu bir AB çerçevesi oluşturma yolunda önemli bir adımı teşkil etmektedir.

Serbest Veri Akışı Tüzüğü AB'de veri yerelleştirme gerekliliklerine ilişkin temel kuralı getirmektedir: "***AB içerisinde veri yerelleştirme gerekliliği öngörülmesi yasaktır***". Buna göre üye devletlerin veri işleme faaliyetlerinin belirli bir ülkenin sınırları içerisinde yapılmasına ilişkin bir kural getiremeyecekleri, ayrıca verinin başka bir üye ülkede işlenmesine yönelik

sınırlamalar getirilmesiyle aynı sonuca matuf düzenlemeler de yapılamayacağı hüküm altına alınmaktadır.

Bu temel kurala ilişkin tek istisna ise, yalnızca kamu güvenliğinin gerektirdiği durumlarda ve orantılılık ilkesiyle uyumlu olmak kaydıyla veri yerelleştirmeye ilişkin bir gerekliliğin kabul edilebilir olduğuna ilişkin hükümdür.

Hâlihazırda veri yerelleştirme gereklilikleri bulunan üye devletler için ise çifte zorunluluk öngörüldüğü görülmektedir. Söz konusu üye devletlerin bir taraftan yukarıda belirtilen temel kurala uyumlu olmayan mevcut yasalarını ve/veya düzenlemelerini yürürlükten kaldırmaları, diğer taraftan ise belirli bir konuda veri yerelleştirme gerekliliği getirmeyi öngörüyorlar ise söz konusu gerekliliğin haklı bir gerekçeye dayalı olarak getirileceğini açıkça ortaya koymaları gerekmektedir.

Üye devlet kuruluşlarının görevlerini yerine getirirken kişisel olmayan verilere erişebilir durumda olması gerekmektedir. Bu çerçevede bir kuruluşun kişisel olmayan verilerin üye devlet dışında bir yerde işlenmesi dolayısıyla onlara erişiminin reddedilmeyeceğine ilişkin temel prensip ortaya konulmaktadır. Bir resmi kuruluşun böyle bir gerekçeyle kişisel olmayan verilere erişememesi durumunda, Tüzük'te belirtilen prosedüre uygun olarak ilgili üye devletin yetkili makamlarından yardım talep edilebileceği düzenlenmektedir.

Veri taşıma konusunda, zorlayıcı yükümlülükler getirilmemektedir. Tüzükte bunun yerine, Komisyon tarafından AB düzeyinde düzenleyici davranış kuralları geliştirilmesinin teşvik edilmesi ve kolaylaştırılması öngörülmektedir.

Serbest Veri Akışı Tüzüğü, Avrupa Birliğinde sınır ötesi veri akışı ve buna ilişkin kısıtlamaların ortadan kaldırılması konusunda önemli bir adım olarak değerlendirilmektedir. Tüzüğün özellikle şirketler bakımından veri yerelleştirme gereksinimlerinin maliyetlerini ortadan kaldırma yolunda önemli bir düzenleme olması beklenmektedir. Nitekim özellikle KOBİ'ler ve başlangıç girişimleri için veri yerelleştirme gerekliliklerinin kaldırılmasının AB'de bir işletme kurma maliyetini azaltmak bakımından büyük önem arz ettiği değerlendirilmektedir. Bilhassa kapsamlı veri depolama ve işleme faaliyeti yürüten başlangıç girişimleri açısından farklı ülkelerde veri depolama ve organizasyon teşkil etme ihtiyacı maliyetleri önemli ölçüde artırmaktadır. Bu tür gereksinimler büyük veri analitiği gibi yenilikçi teknolojilerden faydalanamama gibi olumsuz sonuçlar doğurabilmektedir. Pek çok sektörde yeni başlayan şirketlerin, giderek artan bir şekilde ürün veya hizmetleri için rekabetçi bulut teknolojilerine güvenmekte oldukları görülmektedir. Bu doğrultuda veri yerelleştirme gerekliliklerinin ortadan kaldırılmasının AB bulut hizmet pazarının rekabet gücünü artıracağı öngörülmektedir. Bu türlü destekleyici hukuki düzenlemelerin, yeni girişimlerin pazara daha hızlı girişlerini ve yenilikçilik hızlarını artırmalarını sağlayarak ölçeklenebilirliği ve ölçek ekonomilerinin oluşumunu destekleyeceği öngörülmektedir.

11 SONUÇ VE ÖNERİLER

Teknoloji / serbest ticaret / yabancı yatırım / verilerin serbest dolaşımının artılarını şu şekilde sıralayabiliriz:

- Yüksek teknoloji,
- Konfor,
- Kaynak israfının önlenmesi,
- Verimlilik,
- Zaman israfının önlenmesi,
- Çevrenin korunması,
- Yabancı sermaye.

Buna karşılık **eksileri için şunlar söylenebilir:**

- Yerli teknolojinin gerilemesi,
- Dışa bağımlılık,
- Genç endüstrilerin rekabet gücünün kalmaması,
- Milli güvenlik tehditleri.

Güvenlik / milli ekonomi / milli teknoloji / verilerin güvenliği düşüncesinin artıları ise şunlardır:

- Milli güvenlik,
- Genç endüstrilerin gelişmesi ve rekabet gücünün artması,
- Haksız rekabetin önlenmesi,
- Ticarette koşulların eşitlenmesi,
- Stratejik ticaret politikası (özel koruma),
- İşsizliğin önlenmesi,
- Dış ödemeler dengesinin iyileştirilmesi (ihracatın teşviki),
- Milli pazar, yerli malı,
- İşgücü istismarının önlenmesi,
- Çevrenin korunması.

Bu hususta eksiler de şöyle sıralanabilir:

- Tüketicinin sömürülmesi,

- Kaynak israfı,
- Rant kollama faaliyetinin özendirilmesi,
- Teknolojik gerilik ve rekabet gücünün yitirilmesi,
- Genç endüstriler asla büyümezler,
- Ticareti var kılan, koşullarının eşitsizliğidir,
- Korumacılık işsizliği önlemez, sadece başka sektörlere kaydırır,
- Korumacılık orta ve uzun vadede ödemeler bilançosunu iyileştirmez,
- Etki-tepki mekanizması, misilleme ve ticaret savaşları,
- Refah kaybı.

Artılar ve eksiler değerlendirildiğinde teknoloji ve serbest ticaretten de güvenlik den de vazgeçilemeyeceği ortadadır.

Milli güvenlik endişesiyle (bazen de bu endişenin arkasına sığınıp vergi baskısıyla) uluslararası yatırımcının ülkemizden uzaklaşması, teknolojinin, inovasyonun, üretimin, verimliliğin, sürdürülebilir kalkınmanın, dolayısıyla refahın uzaklaşması anlamına da geliyor. Diğer taraftan "özgür bireyler, özgür devletlerde yaşar" ilkesinin gereği olarak kişisel verilerin güvenliği, mülkiyet hakkı, milli güvenlik de modern devletin vazgeçilmezleri.

O halde yapılması gereken: teknoloji ile güvenlik arasında sağlıklı bir dengenin oluşturulmasıdır. **Bu noktada;**

Lokal çözümlerin "zor" ve "yeterli" olmadığı ortadadır. Yapılması gereken teknolojiden maksimum seviyede yararlanılacak ve ticareti üst boyutlara çıkararak refah seviyesini eşit boyutlara çıkarabileceğimiz bir eko sistem içinde yer alarak, bu sistem içindeki çözümlere adapte olmaktır. Bu eko sistem ise her halde AB'dir.

Ülkemizde kişisel verilerin yurt dışına aktarılması (sınır aşan veri transferi) bakımından bir yandan güvenli denetim mekanizmalarının oluşturulması, diğer yandan da veri akışının kolaylaştırılması için GDPR deki "bağlayıcı şirket kuralları" (bağlayıcı kurumsal kurallar) ve "sertifikasyon" (belgelendirme) uygulaması, standart hükümler model olarak alınabilir.

Bu çerçevede önemli bir tedbir, **bağlayıcı şirket kurallarıdır**. Bağlayıcı şirket kuralları (BCR), AB bünyesinde üye devletler dahilinde bulunan veri sorumluları veya işleyenler tarafından AB dışındaki bir veya birden fazla ülkede bulunan ortak bir ekonomik faaliyetle iştigal eden teşebbüsler grubu veya işletmeler grubu içerisindeki teşebbüs veya işletmelere (bir kez veya sürekli olarak) yapılacak veri aktarımlarında uyulması zorunlu politikadır[9]. GDPR uyarınca

[9] 47 nci maddeye göre bağlayıcı kurumsal kurallarda asgari şu hususlara yer verilmelidir: Ortak bir ekonomik faaliyette bulunan işletmeler grubunun ve her üyesinin yapısı ve irtibat bilgileri, kişisel veri kategorileri, işleme türü ve amaçları, etkilenen veri sahiplerinin türü ve söz konusu üçüncü ülke veya ülkelere ilişkin

BCR, Komisyon tarafından alınmış bir yeterlilik kararı bulunmaması halinde, kişisel verilerin AB dışındaki bir ülke veya uluslararası organizasyona aktarılması için gerekli olan yeterli güvenlik düzeyini sağlamanın yöntemlerinden birisidir. Bu yöntem uyarınca üye ülke kişisel verilerin korunması otoritesinin onayı bir kez alınır ve BCR dahilinde onaylanan veri aktarımları için her bir aktarımda ayrıca üye ülke kişisel verilerin korunması otoritesinin onayının alınması gerekmez.

Verilerin güvenliğinin en üst düzeyde sağlanabilmesi ancak son teknolojilerle donatılmış veri merkezlerinde tutulması, dünya standartlarında saklanması ve güvenli ağlar üzerinden iletilmesi ile mümkündür. Üstelik bu hizmetler kullanıcılarına verileri üzerinde tam bir hakimiyet sağlaması sebebiyle, veri sorumlularına verilerini etkin şekilde yönetme ve bu sayede ilgili mevzuattan kaynaklanan yükümlülüklerine de uymalarında destek olmaktadır.

Bilindiği üzere bulut hizmeti sağlayıcıları ana faaliyet alanlarının verilerin yönetimi ve güvenliği olması sebebiyle her yıl siber güvenlik alanında milyarlarca dolarlık yatırım yapmakta olup bu sayede kesintisiz olarak en güncel güvenlik önlemleri ve araçlarıyla bulut hizmeti sunabilmektedir. Bulut hizmeti sağlayıcıların bu niteliklerinin düzenli şekilde ölçümü ve denetimi, ulusal ve uluslararası alanda kabul gören sertifikalar yoluyla yapılabilmektedir.

Sınır ötesi veri aktarımını sağlamak için önerilebilecek yöntemlerden birisi de yurtdışındaki veri alıcıların belirli sertifikalara sahip olması yoluyla kişisel veriler hakkında yeterli korumayı sağladıklarının teyit edilmesidir. Nitekim benzeri bir uygulama AB'de yürürlükte bulunan GDPR içerisinde de yer almaktadır.

AB dışında bulunan veri alıcılarının yeterli koruma sağlayıp sağlayamadığını ölçmek için GDPR m. 42 çerçevesinde verilen sertifikalar kullanılabilmektedir (GDPR m. 46/2/f). GDPR m. 42, AB sınırları içerisinde bulunan düzenleyici otoritelere, veri sorumlusu ya da veri işleyenlerin GDPR ile uyumluluğunu gösteren sertifikalar düzenleme konusunda yetki vermektedir. Söz konusu sertifikalar, doğrudan düzenleyici otoritelerce verilebileceği gibi düzenleyici otoritelerin akredite ettiği sertifikasyon kuruluşları tarafından da verilebilmektedir.

---

açıklama da dahil olmak üzere veri aktarımları veya aktarım dizisi; bunların hem içsel hem de dışsal olarak hukuki bağlayıcılık yapısı; amaç sınırlaması, verilerin en alt düzeye indirilmesi, sınırlı saklama süreleri, veri kalitesi, özel ve olağan veri koruması, işleme faaliyetine yönelik yasal dayanak, özel kategorilerdeki kişisel verilerin işlenmesi başta olmak üzere genel veri koruma ilkeleri, veri güvenliğinin sağlanmasına ilişkin tedbirler ve bağlayıcı kurumsal kurallara bağlı bulunmayan organlara transit aktarımlara ilişkin gerekliliklerin uygulanması; yalnızca otomatik işleme faaliyetine dayalı kararlara tabi olmama hakkı, üye devletlerin yetkin denetim makamına ve yetkin mahkemelerine şikayette bulunma ve tazminat alma hakkı; bağlayıcı kurumsal kurallara ilişkin bir ihlalden dolayı tazminat hakkı da dahil olmak üzere veri sahiplerinin işleme faaliyetine ilişkin hakları ve bu hakları kullanma yöntemleri; üye devletteki veri sorumlusu ya da işleyenin AB dışında bağlayıcı kurumsal kuralların ihlal edilmesi halinde sorumluluğu üstlenmesi; bağlayıcı kurumsal kurallara ilişkin bilgilerin veri sahiplerine nasıl sağlandığı; bağlayıcı kurumsal kurallara uyumluluğun izlenmesinin yanı sıra eğitimin izlenmesi ve şikâyetlerin ele alınmasından sorumlu olan diğer kişiler veya kuruluşların görevleri; şikayet usulleri; ortak bir ekonomik faaliyette bulunan işletmeler grubu içerisinde bağlayıcı kurumsal kurallara uyumluluğun doğrulanmasının sağlanmasına yönelik mekanizmalar; kurallara ilişkin değişikliklerin raporlanması ve kaydedilmesi ile bu değişikliklerin denetim makamına raporlanmasına ilişkin mekanizmalar; denetim makamı ile kurulan işbirliği mekanizması; ortak bir ekonomik faaliyette bulunan işletmeler grubunun üçüncü bir ülkede tabi olduğu bağlayıcı kurumsal kuralların sağladığı teminatlar açısından olumsuz etkisinin bulunmasının muhtemel olduğu yasal gerekliliklerin denetim makamına raporlanmasına ilişkin mekanizmalar; kişisel verilere daimi veya geçici olarak erişimi bulunan personele uygun veri koruma eğitimi.

"*Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir*" hükmünü içeren KVKK m. 9/2/b de sınır ötesi veri akışının sağlanabilmesi için bir sertifikasyon sistemi kurulmasına cevaz vermektedir. Bu çerçevede KVKK kapsamında da bir sertifikasyon sistemi önerilebilir. Bu öneri kapsamında yurtdışında yerleşik olan veri alıcılarının sağlaması gereken temel koşullar özetle şunlar olmalıdır:

- Gerekli sertifikaların alınması,
- Yurtdışındaki veri alıcısı tarafından sertifikaların gereklerine uygun hareket edileceğine dair imzalı taahhütname verilmesi,
- Yurtdışındaki veri alıcısının, 108 sayılı sözleşmeye taraf ve Türkiye tarafından tanınan bir ülkede yerleşik/kurulmuş olması.

Kurul tarafından GDPR'a uygun olarak Standart Hükümlerin yayınlanması ve veri gönderen ile veri alıcısı arasında bu hükümleri içeren bir sözleşmenin imzalanması halinde ayrıca Kurul'dan bir izne gerek olmaksızın yurt dışına verinin aktarımına imkân verilmesi de uygun olacaktır.

Bu arada ülkemizin şartları da dikkate alınarak global düzeyde dijital eşitsizliği ortadan kaldırmak için hem iktisadi hem de güvenlik noktasında tedbirler alınması gerektiği de muhakkaktır. Bu çözümlerde bu güne kadar olduğu gibi işin güvenlik boyutu yanında iktisadi boyutuna da odaklanılmalıdır. Güvenliğin de teknoloji ile ilgili olduğu; teknoloji olmadan güvenliğin mümkün olmadığı göz ardı edilmemelidir. Bu nedenle işin ekonomik boyutunun ön plana çıkarılarak teknolojinin gelişmesi için çaba harcanılmalıdır.

Güvenlikle ilgili eko sistem tedbirleri dışında "genel güvenlik tedbirlerinin sakıncalı olduğu ortadadır. Bu nedenle güvenlik tedbiri noktasında (booking örneğinde olduğu gibi) spesifik tedbirler alınmalı; bu tedbirlerden ekonomik fayda sağlamak amaçlanmalıdır.

Dijital /teknolojik toplumun işbirliği ekseninde, eşitlik, adalet, şeffaflık ve hesap verilebilirlik gibi ortak değerlere dayanarak, hükümetler, uluslararası kuruluşlar, işletmeler, STK'lar ve üniversiteler dahil tüm paydaşlar arasında güven üzerine kurulması gerektiği unutulmamalıdır. Bu noktada resmi – özel işbirliği, ihtiyaçların hızlı bir şekilde belirlenmesi, acil ve doğru çözümler bulunması noktasında son derece önemlidir. Söz konusu işbirliği ise bu konuda üst bir otoritenin varlığını gerektirmektedir. Cumhurbaşkanlığı hükümet sistemi modelinde, kamu ile özel kesimi (işletmeler STK'lar, üniversiteler gibi) de aynı ortamda buluşturacak otorite olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi önemli bir rol oynayabilecektir.