YATIRIM ORTAMINI İYİLEŞTİRME KOORDİNASYON KURULU

Bilişim Çalışma Grubu 3. Eylem

Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi

Nisan 2022

İçindekiler

Kısaltmalar

AB: Avrupa Birliği
CDEP: Dijital Ekonomi Politikaları Komitesi
GDPR: Avrupa Genel Veri Koruma Tüzüğü
KVKK: Kişisel Verilerin Korunması Kanunu
ODD: Otomotiv Distribütörleri Derneği
OECD: İktisadi İşbirliği ve Gelişme Teşkilatı
OSD: Otomotiv Sanayi Derneği
PGC: Bilimsel ve Teknolojik Politika Komitesi
TBD: Türkiye Bilişim Derneği
TOBB: Türkiye Odalar ve Borsalar Birliği
TÜBİSAD: Bilişim Sanayicileri Derneği
TÜSİAD: Türk Sanayi ve İşinsanları Derneği
WEF: Dünya Ekonomik Forumu
WPDGP: Veri Yönetişimi ve Gizliliği Çalışma Grubu
YASED: Uluslararası Yatırımcılar Derneği
YOİKK: Yatırım Ortamını İyileştirme Koordinasyon Kurulu

Tablolar

1. Giriş

Yaşadığımız çağın en dikkat çeken özelliği, hızla gelişmekte olan dijital teknolojiler ve bu teknolojilerin ekonomik işleyiş ile iş modelleri üzerindeki dönüştürücü etkisidir. Yeni dijital teknolojiler ve bunlardan kaynaklanan yeni iş modelleri, sınır tanımaz boyutlarda veri akışları oluşturmakta ve veri temelli bir ekonominin oluşmasına zemin teşkil etmektedir. Verinin etkin kullanımı sektörel katma değeri, tüketici faydasını ve ekonomik üretkenliği artırmaktadır. Günümüzde pek çok işletme veriye dayalı karar almanın; işletmenin veya işin mevcut durumunun daha iyi anlaşılması, alternatif seçeneklerin değerlendirilmesi, farklı ihtimaller üzerinde kıyaslama ve doğru analizler yapılması gibi önemli faydaları beraberinde getireceğini bilmektedir.

Günümüzde veriye atfedilen değer arttıkça, verilerin sınır ötesi aktarımı hususu da giderek önem kazanmış, verinin serbest dolaşımı konusunda birçok ülke ile Avrupa Birliği (AB), İktisadi İşbirliği ve Gelişme Teşkilatı (OECD), Dünya Ekonomik Forumu (WEF), G20 ve G7 gibi uluslararası kuruluşlar tarafından çalışmalar başlatılmıştır. OECD gibi kuruluşlar özellikle gelişmekte olan ülkelerin güvenlik çekincelerini mümkün mertebe ortadan kaldırabilecek, yurt dışına veri aktarımlarını zorlaştıran uygulamaları hayata geçirme motivasyonlarını azaltacak genel ilkeler (aktarılan verinin diğer ülkelerin yetkisiz erişiminden korunması, ilgili ülkenin kendi kurumlarının verisine yurt dışında olsa bile erişimine imkân sağlanması, veri mahremiyetini temin edecek harmonize siber güvenlik tedbirlerinin alınması vb.) geliştirmeye çalışmaktadır.

Son yıllarda ülkemizdeki sektörel düzenlemelerde de (6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamı dışındaki düzenlemeler) artan bir şekilde verinin yurt dışına aktarılmadan ülke sınırları içerisinde tutulmasını ifade eden veri yerelleştirmesi[1] anlayışının benimsendiği görülmekte, bu yöndeki düzenlemelerin ise birçok işletmenin ticari ve operasyonel faaliyetlerini doğrudan ve önemli ölçüde etkilediği ilgili sektör temsilcileri tarafından dile getirilmektedir.

Bilindiği üzere, kamu temsilcilerinden ve sivil toplum kuruluşlarından oluşan yapısıyla Yatırım Ortamını İyileştirme Koordinasyon Kurulu (YOİKK) iş dünyasını ilgilendiren birçok konuda yapısal reformlar gerçekleştirilmesi yönünde politika önerileri geliştirmektedir. YOİKK bünyesinde 2021 yılında "Altyapı", "AR-GE ve Sanayi", "Bilişim", "Çalışma Hayatı", "Ticaret, Vergi, Finansman ve Teşvik" ve "Yatırım Ortamı Çerçeve Konular" olmak üzere 7 farklı çalışma grubu oluşturulmuş, bunlardan Bilişim Çalışma Grubu'nun koordinasyonu görevi ise T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'ne tevdi edilmiştir. Bu bağlamda, özellikle son yıllarda ülkemizde ekonomik hayatta etkileri daha yoğun şekilde hissedilen veri yerelleştirmesi düzenlemelerinin, ülkemizin küresel değer zincirlerine daha etkin bir şekilde eklemlenmesi, yatırım ortamının daha da iyileştirilmesi ve rekabet gücümüzün artırılmasını

[1] Veri yerelleştirmesi, işbu rapor kapsamında hem bilgi sistemlerinin ülke sınırları içerisinde tutulması hem de verinin yurt dışına aktarılmadan ülke sınırları içerisinde tutulması anlamlarında kullanılmaktadır.

sağlayacak bir yaklaşımla şekillendirilmesine yönelik politika önerileri geliştirmeyi amaçlayan "**Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi**" eylemi tanımlanarak Bilişim Çalışma Grubu'nca yürütülmesi kararlaştırılmıştır. Eylemin çıktısıysa, bir taraftan sınır aşan veri transferlerini ticareti destekleyecek şekilde kolaylaştırırken diğer taraftan da bu tür veri transferlerinin olası risklerini en aza indirecek yaklaşımı ve bunun hayata geçirilmesine yönelik yol haritasını ortaya koyan bir rapor oluşturulması şeklinde tanımlanmıştır.

Bu çalışma kapsamında öncelikle mevzuat taraması yapılarak Türkiye'deki veri yerelleştirmesiyle ilgili mevzuat hükümleri tespit edilmiş, söz konusu mevzuat hükümlerinin firmaların ticari operasyonlarını nasıl etkilediği ve kamu kurumlarının bu mevzuata neden ihtiyaç duyduğu belirlenmiştir. Bu amaçla, ilgili kamu kurumları, sivil toplum kuruluşları ve özel sektör firmaları ile çeşitli tarihlerde toplantılar düzenlenmiş, yukarıda bahsi geçen hususlarda bu tarafların görüş ve değerlendirmeleri alınmıştır. Ayrıca, bu raporda yer verilen öneriler de yine yukarıda bahsi geçen paydaşların görüş ve değerlendirmeleri dikkate alınarak şekillendirilmiştir.

"Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi" eyleminin çıktısı olarak hazırlanan bu raporun ikinci bölümünde ülkemizde veri yerelleştirmesi hükümleri içeren mevzuata ilişkin bilgilere, üçüncü bölümünde bu mevzuatla ilgili olarak kamu kurumları ile özel sektör işletmelerinin ve sivil toplum kuruluşlarının görüşlerine, dördüncü bölümünde de AB, OECD, WEF, G20 ve G7 gibi uluslararası kuruluşların konu hakkındaki genel yaklaşım, tespit ve önerilerine yer verilmiştir. Raporun beşinci ve son bölümünde ise konuya ilişkin genel değerlendirmeler ve öneriler açıklanmıştır.

2. Ülkemizde Veri Yerelleştirmesi Hükümleri İçeren Mevzuat

Hem çok uluslu firmaların farklı ülkelerdeki ticari operasyonlarının hem de yurtdışındaki firmalarla iş yapan yerli firmaların iş süreçlerinin etkin bir şekilde yürütülebilmesi ve bulut bilişim hizmetlerinin yaygın kullanılması, verilerin farklı ülkeler arasında hızlı bir şekilde aktarılması ihtiyacını ortaya çıkarmıştır. Yurt dışına veri aktarımının yaygınlaşmasıyla birlikte birçok ülkede genellikle güvenlik ve/veya veriden ilgili ülkenin sadece kendisinin değer yaratması gibi yönlerden çekinceler ortaya çıkmıştır. Yurt dışına veri aktarımının veri temelli ekonominin önemli unsurlarından biri olduğunun farkında olan kimi ülkeler (örneğin; ABD, Kanada, Avustralya ve Japonya) bu tür çekincelere rağmen veri aktarımını esnekleştirirken kimi ülkelerse (örneğin; Rusya, Çin, Vietnam ve Hindistan) belirli nitelikteki verilerin ülke dışına çıkarılmasını zorlaştıran veri yerelleştirme düzenlemeleri getirmiştir.

Bu dokümanda, 6698 sayılı KVKK kapsam dışında bırakılarak, ülkemizde veri yerelleştirilmesi düzenlemelerinin mevcut durumunun tespit edilmesi amacıyla bankacılık, telekomünikasyon, ulaşım, sağlık, finans, ödeme hizmetleri ve e-ticaret gibi çeşitli sektörleri etkileyen[2] birincil ve ikincil mevzuat incelenmiştir. Bu incemeler doğrultusunda veri yerelleştirmesi içerdiği tespit edilen mevzuata ilişkin bilgiler Tablo-1'de sunulmaktadır[3].

Tablodan da görüleceği üzere, ülkemizde farklı sektörlerde faaliyet gösteren işletmelerin ticari ve operasyonel kararlarını doğrudan etkileyebilecek veri yerelleştirmesi mevzuatı bulunmaktadır. Üstelik, tarihsel olarak bakıldığında, başlangıçta kritik sektörlerde veri yerelleştirmesi şartlarının getirilmesi şeklinde olan eğilimin giderek artan bir şekilde diğer sektörlere de yayıldığı ve veri yerelleştirmenin yaygın bir düzenleme yapma anlayışı olarak yerleşmeye başladığı da görülmektedir.

[2] Veri yerelleştirmesine ilişkin mevzuat incelemesi yapılırken ülkemiz gayrisafi yurtiçi hasılasına yüksek katkı sağlayan sektörler dikkate alınmış olup bu sektörler dışında da veri yerelleştirilmesine sebep olabilecek birincil ve ikincil mevzuatın olabileceği göz önünde bulundurulmalıdır.

[3] Veri yerelleştirmesine ilişkin mevzuat incelemesi yapılırken bazı taslak düzenlenmelerde de veri yerelleştirmesi hükümleri ile karşılaşılmış, ancak yürürlüğe girmedikleri için bunlar raporun kapsamı dışında bırakılmıştır.

Tablo 1: Veri Yerelleştirme Hükümleri İçeren Mevzuat

Kurum	İlgili Mevzuat	İlgili Madde
Cumhurbaşkanlığı	2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi	**Madde 1:** Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi **kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.** **Madde 3:** Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar **hariç bulut depolama hizmetlerinde saklanmayacaktır.** **Madde 20:** Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim **trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.**
	Bilgi ve İletişim Güvenliği Rehberi	**Tedbir No. 4.3.1.1:** Kritik verilerin yurt içinde depolandığı ve yurt dışında barındırılmayacağı garanti altına alınmalıdır. Kurumlara ait özel bulut sistemleri haricinde, bulut servis sağlayıcılardan yer, sunucu veya servis tabanlı bulut hizmeti kullanılacaksa, • Erişen personel, yetki ve yetkinlik düzeyleri • Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesi • Güncelleme durum alarmları • Siber olay alarmları • Performans ve kapasite göstergeleri kurum tarafından kontrol edilmelidir. **Tedbir No. 3.2.7.2:** Kurumların kendi özel sistemleri veya yurt içinde yerleşik kurum kontrolündeki hizmet sağlayıcılar hariç olmak üzere **kurumsal kritik verilerin saklanması/depolanması amacıyla bulut depolama hizmetleri kullanılmamalıdır**.
Bilgi Teknolojileri ve İletişim Kurumu	5809 Sayılı Elektronik Haberleşme Kanunu	**Madde 51/6:** Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, **trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir**.
	112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call) Konulu Kurul Kararı[4]	**Madde 3:** 112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sistemin Yerleştirilmesi ile İlgili Tip Onayı Yönetmeliği'ne uygun olarak ülkemizde kullanılmak üzere üretilen veya ithalat yoluyla satılan araçlardaki **e-Call ile birlikte katma değerli hizmet sunumuna imkân sağlayan haberleşme sistemlerinde hizmet verecek sunucuların** başta 5809 sayılı Elektronik Haberleşme Kanununda belirtilen milli güvenlik ve kamu düzenine ilişkin hükümler ile ilgili diğer mevzuata uygun olarak **ülkemizde bulundurulması ve sistemdeki kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına çıkartılmaması** kararlaştırılmıştır.

	Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik	**Madde 18/1:** Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), **kendi imza oluşturma ve doğrulama verileri ile sertifikasını Türkiye Cumhuriyeti sınırları içerisinde oluşturur ve imza oluşturma verisini hiçbir şekilde bu sınırların dışına çıkaramaz.**
	Uzaktan Programlanabilir SIM Teknolojileri (eSIM) Konulu Kurul Kararı[5]	**1.** Ülkemizde kullanılmak üzere imal edilen veya yolcu beraberinde getirilen ya da ithalat yolu ile piyasaya arz edilen cihazlardaki Uzaktan Programlanabilir SIM (eUICC, eSIM/embedded SIM vb.) teknolojilerinin ülkemiz sınırları içerisinde kullanılması durumunda, bu kapsamdaki modüllerin sadece ülkemizdeki mobil işletmeciler tarafından kontrol edilebilecek şekilde programlanabilir olması ve sadece ülkemizdeki mobil işletmeci profillerinin yüklenebilmesi, yabancı şirketlere ait SIM profillerinin ise ancak yurt dışı çıkışlarında gümrük hattı dışında yüklenebilmesine imkân sağlanması, **2.** Uzaktan Programlanabilir SIM teknolojilerine yönelik olarak; eSIM abonelik yönetimi (GSMA-SM –GSMA Subscription Manager) süreci ile ilgili olan profil verisi hazırlama ve güvenli yönlendirme sunucuları (SM-DP (Subscription Manager Data Preparation), SM-SR (Subscription Manager Secure Routing), SM-DP+, SM-DS (Subscription Manager Discovery Server), Veri Merkezi ve süreç içerisinde GSMA tarafından belirlenebilecek benzeri fonksiyonlara sahip sistem bileşenleri) ve yazılımlar (SM-DP, SM-SR, SM-DP+, SM-DS, Veri Merkezi ve süreç içerisinde GSMA tarafından belirlenebilecek benzeri fonksiyonlara sahip sistem bileşenleri üzerinde çalışan yazılımlar, platformlar, LPA (Local Profile Assistant) de dahil abonelik profili yönetimine ilişkin mobil uygulamalar) ile GSMA standartlarında eSIM platformu ile ilgili öngörülen diğer ekipman ve yazılımlar da dahil tüm yapı, sistem ve depolama birimlerinin, ülkemizde yetkilendirilen işletme tarafından veya tüm sorumluluk işletmeye ait olmak üzere işletmelerin belirleyeceği üçüncü kişiler tarafından ülkemiz sınırları içerisinde tesis edilmesi, birlikte çalışabilirliğinin temin edilmesi, kontrolünün sağlanması, **tüm verinin ülkemiz sınırları içerisinde tutulması,** tüm bu sistemlerin GSMA standartlarına uygun olarak kurulması ve ilgili dokümantasyon ve süreçlerin tamamlanarak sistemlerin 29.02.2020 tarihine kadar Kurumca belirlenecek yerde kurulması,
	Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik	**Madde 5/2:** Milli güvenlik gerekçesiyle **trafik ve konum verilerinin yurt dışına çıkarılmaması esastır.** **Madde 8/1 (e):** Üçüncü tarafın yurt dışında olması halinde verinin aktarılacağı ülkenin adı, şeklindeki bilgiler verilerek ayrıca açık rıza alınır.
	5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla	**Ek Madde 4/5:** Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, **Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alır.**

[4] 2018/DK-YED/27 sayılı Kurul Kararı
[5] 2019/DK-TED/053 sayılı Kurul Kararı

	İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	
	Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar	**Madde 12/1:** Yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, **Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alır.** **Madde 12/2:** Bu maddenin uygulanmasında temel kullanıcı bilgileri ile Kurum tarafından bildirilebilecek hususlara ilişkin **verilerin Türkiye'de barındırılması yönünde gerekli tedbirlerin alınmasına öncelik verilir.** **Madde 12/3:** Bu madde kapsamında alınan tedbirlere ilişkin olarak her raporlama döneminde Kurum tarafından bildirilen hususları da kapsayacak şekilde Kuruma bilgi verilir.
	Kayıtlı Elektronik Posta (KEP) Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik Madde	**Madde 16/1 (ı):** KEP hizmet sağlayıcısı "KEP sistemine ilişkin **ana ve yedek sistemlerini Türkiye Cumhuriyeti sınırları içerisinde bulundurmakla" yükümlüdür.**
Sağlık Bakanlığı	Sağlık Bilgi Sistemleri Uygulamaları Hakkında 2015/17 sayılı Genelge	**Madde 2/7:** Bilgi sistemlerindeki veriler, sağlık tesislerindeki veri kayıt ortamları, Bakanlık merkezi veri kayıt ortamı ya da Genel Müdürlüğün onayladığı veri kayıt ortamları **haricinde hiçbir yere kaydedilemez ve gönderilemez**.
Sermaye Piyasası Kurulu	Sermaye Piyasası Kanunu	**Madde 87/3:** Veri depolama kuruluşları nezdindeki bilgilerin **kamu tüzel kişileri dâhil üçüncü kişiler ile paylaşımı Kurulun onayına tabidir.** Bu fıkranın uygulanmasında kişisel verilerin kullanılmasına ilişkin mevzuata riayet edilir.
	VII-128.9 sayılı Bilgi Sistemleri Yönetim Tebliği	**Madde 26/1:** Kurum, Kuruluş ve Ortaklıkların **birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur**.
	Veri Depolama Kuruluşunun Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik	**Madde 6/1 (a):** VDK'nın görev ve yetkileri şunlardır: Kanunun 87 nci maddesi çerçevesinde, Kurulca belirlenen işlemlere ilişkin kendisine raporlanan verileri Türkiye sınırları içerisinde olmak üzere elektronik ortamda kaydetmek ve saklamak **Madde 16 (2):** VDK nezdindeki bilgilerin kamu tüzel kişileri dâhil üçüncü kişiler ile paylaşımında 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununa ve ilgili diğer mevzuata riayet edilir. **Madde 19 (3):** Yabancı ülke otoritelerinin VDK nezdindeki verilerin paylaşılmasına ilişkin taleplerinin VDK tarafından karşılanması Kurul onayına tabidir.
	Kaydileştirilen Sermaye Piyasası Araçlarına İlişkin Kayıtların Tutulmasının Usul ve Esasları Hakkında Tebliğ	**Madde 33/2:** Hak sahibinin yurt dışında yerleşik kişi olması durumunda, MKK tarafından hak sahibinin yanı sıra bu yatırımcılara yurt dışında saklama hizmeti sunan kuruluşa hak sahipliği bilgilerinin iletilmesi mümkündür. Bunun için, bu müşterilerin yurt dışında saklama hizmeti sunan kuruluşla arasındaki sözleşmede bu kuruluşun müşterilerin hak

		sahipliği bilgilerine erişimine yönelik hüküm olması ve yurt dışında saklama hizmeti sunan kuruluş ile yurt içinde saklamaya yetkili yatırım kuruluşu arasında bu konuya özgü bir sözleşme olması gerekir. Bu fıkra uyarınca MKK tarafından hak sahibi yerine, yurt dışında saklama hizmeti sunan kuruluşa bilgi verilebilmesi için yurt içinde saklamaya yetkili yatırım kuruluşunun MKK'ya başvuru yaparak, bilgi verilecek yurt dışında saklama hizmeti sunan kuruluşun unvanının, bu kuruluşun müşterileri ile arasındaki sözleşmede gerekli hükümlerin bulunduğuna ilişkin beyanının ve ilgili hak sahiplerinin MKK'ya bildirmesi zorunludur. Yurt dışında saklama hizmeti sunan kuruluş aldığı bu bilgilerin gizliliğini korumakla yükümlüdür. Bu bilgiler hukuka aykırı olarak kimseyle paylaşılamaz ve veriliş amaçları dışında kullanılamaz.
Türkiye Cumhuriyeti Merkez Bankası	Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmelik	**Madde 24/6:** **Sistem işleticisinin bilgi sistemleri yurt içinde kurulu olmak zorundadır.** Sistem işleticisinin, faaliyetlerini yürütmede kullandığı bilgi sistemleri kapsamında bir dış hizmet alması halinde, dış hizmet sağlayıcısının bu kapsamdaki faaliyetlerini yürütmede kullandığı bilgi sistemleri ve bunların yedeklerinin de yurt içinde tutulması esastır. **Madde 25/4:** **Yedek merkez, yedek sistemler ve veri yedekleme merkezi yurt içinde bulunmak zorundadır.**
	Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik	**Madde 19:** **Bu madde uyarınca kurulacak iş birliği neticesinde gerçekleştirilecek ödeme işlemlerine ilişkin belge ve kayıtların kuruluş tarafından yurt içinde saklanması zorunludur.** **Madde 62/3:** Ödeme hizmeti sağlayıcıları tarafından ihraç edilmiş ödeme araçlarına ilişkin hassas müşteri verilerinin yurt içinde bulunan işyerleri nezdinde veya sorumluluğunda saklanması durumunda, **bu verilerin yurt içinde tutulması ve saklanması zorunludur.**
	Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri İle Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ	**Madde 16/7:** **Kuruluş her türlü veriyi işlemek, saklamak ve iletmek için bir dış hizmet olarak yurt içinde tesis edilmiş bulut bilişim hizmetlerini kullanabilir**. Ancak hassas müşteri verilerini, rekabete duyarlı verileri, kişisel verileri veya müşteriyle ilintilendirilebilir ve onu belirli ya da belirlenebilir kılan her türlü bilgiyi işleyecek, saklayacak ve iletecek şekilde bulut bilişim hizmetinin alınması, **bu dış hizmetin ancak sadece kuruluşa tahsis edilmiş donanım ve yazılım kaynakları üzerinden sunulduğu özel bulut hizmet modeli ile alınması halinde mümkündür**. Banka tarafından uygun görülen dış hizmet sağlayıcılar tarafından sunulması durumunda kuruluş, sadece ödeme hizmeti sağlayıcılarına veya bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen diğer kredi kuruluşları veya finansal kuruluşlara tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal olarak her ödeme hizmeti sağlayıcısına özgü ayrı kaynağın atandığı **topluluk bulutu hizmet modeliyle dış hizmet alabilir. Topluluk bulutu hizmetinin, kuruluşun ana ortağı, iştiraki veya ana ortağının iştiraki olan ve bilgi sistemlerine ilişkin faaliyetleri ilgili mevzuat çerçevesinde yetkili bir otorite tarafından düzenlenen ve denetlenen bir kredi kuruluşu veya**

		finansal kuruluş tarafından verilmesi, sadece ana ortak, iştirakleri ve ana ortağın iştiraklerine tahsis edilmiş donanım ve yazılım kaynaklarının fiziksel olarak paylaşıldığı ancak mantıksal ayrıma gidilerek kuruluşa özgü ayrı bir kaynak atanması koşuluyla bu fıkra hükümlerine aykırılık teşkil etmez. Kuruluşun müşteri verisi içermeyen test ve geliştirme ortamları ve sistemleri için gerekli güvenlik tedbirlerini alarak bulut bilişim hizmeti alması halinde bu fıkra hükmü uygulanmaz. **Madde 21/1:** **Kuruluşların birincil ve ikincil sistemleri ile veri yedekleme merkezlerini yurt içinde bulundurmaları zorunludur.** Bu maddenin uygulanmasında, Yönetmeliğin 19 uncu maddesinin on üçüncü fıkrası hükümleri saklıdır. **Madde 21/2:** Aynı kuruluşun müşterileri ya da farklı kuruluşların müşterileri arasındaki ödeme işlemlerinin yürütülmesinde kullanılan **tüm bilgi sistemleri ve bunların yedeklerinin yurt içinde bulunması esastır**. Bu kapsamda **dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de yurt içinde tutulur.**
Bankacılık Düzenleme ve Denetleme Kurumu	5411 Sayılı Bankacılık Kanunu	**Madde 73:** Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve **6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz**. Kurul ekonomik güvenliğe ilişkin yapacağı değerlendirme neticesinde, müşteri sırrı ya da banka sırrı niteliğinde olan **her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkilidir.**
	Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik	**Madde 11/4:** **Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur**.
	6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunu	**Madde 23/1:** Sistem işleticisi, ödeme kuruluşu ve elektronik para kuruluşu bu Kanunda yer alan hususlar ile ilgili belgeleri ve kayıtları en az on yıl süreyle güvenli ve **istenildiği an erişime imkân sağlayacak şekilde yurt içinde saklar**. **Sistem işleticisinin faaliyetlerini yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de yurt içinde tutulur.**
	Banka Kartları ve Kredi Kartları Hakkında Yönetmelik	**Madde 26/B/5:** Beklenmedik durumlar nedeniyle mevcut verilerin kaybının önlenmesi amacıyla bir veri yedekleme merkezi oluşturulur.) **Bilgi alışverişi kuruluşları veri yedekleme merkezinin yerini, yurt içinde olmak kaydıyla** veriye yetkisiz erişim risklerini de dikkate alarak acil ve beklenmedik durumların etki alanı dışında kalacak şekilde belirlerler.

	Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik	**Madde 11/4:** **Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.**
	Bilgi Alışverişi, Takas, Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler İle İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ	**Madde 5/2:** **Kuruluşun birincil ve ikincil sistemlerini yurt içinde bulundurması zorunludur**.
	Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik	**Madde 10/1:** Banka, müşterinin kendisinden gelen ve yazılı şekilde ya da kalıcı veri saklayıcısı yoluyla kanıtlanabilir nitelikte olan bir müşteri talebi olmaksızın, faaliyetlerinin ifası sırasında ve her türlü dış hizmet alımlarında bilgi sistemleri aracılığıyla edindiği, sakladığı veya işlediği müşteri sırrı niteliğindeki bilgileri, Kanunda yer alan istisnai haller haricinde **yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşamaz ve bunlara aktaramaz.** **Madde 25/1:** **Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.** **Madde 25/2:** Birincil sistemlerin kaçıncı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve birinci fıkra hükmüne tabidir. **Madde 25/3:** Bankacılık faaliyetlerinin yürütülmesi veya Kanun ve mevzuatta tanımlanan sorumlulukların yerine getirilmesi amacını taşımayan banka içi mesajlaşma sistemleri, piyasa izleme platformları gibi sistemler birincil sistemler kapsamında değildir. Bankanın kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için sistem veya uygulama üzerinden herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da sır kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir. **Madde 25/4:** İşlemlerin doğası gereği yurt dışı ile etkileşimin gerekli olduğu ödeme veya mesajlaşma sistemleri gibi bankacılık işlemleri hariç olmak üzere, bankanın yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bankacılık işlemlerini gerçekleştirebilmesi ve yurt dışı iletişim ağlarıyla bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmesi esastır. **Madde 25/5:** **Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının sunduğu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamında ele alınır ve yurt içinde bulundurulur.**

	Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu	**Madde 17/2:** Kurum; şirket, şirket ortakları, şirketin kontrol ettiği ortaklıklar ile bunların şubeleri ve ilgili diğer gerçek ve tüzel kişilerden bu Kanun hükümleri ile ilgili görecekleri bütün bilgileri gizli dahi olsa istemeye, bunların vergiyle ilgili kayıtları dâhil olmak üzere tüm defter, kayıt ve belgelerini incelemeye yetkili olup, bilgi istenenler de istenilen bilgileri vermekle, defter, kayıt ve belgeleri incelemeye hazır bulundurmakla, tüm bilgi işlem sistemini denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, verilerin güvenliğini sağlamakla ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle yükümlüdür.
	Faktoring ve Finansman – Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ	**Madde 15/2:** **Şirket birincil ve ikincil sistemlerini yurt içinde bulundurur**. Bu kapsamda dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı **bilgi sistemleri ve bunların tüm yedekleri de yurt içinde tutulur.**
Hazine ve Maliye Bakanlığı (Gelir İdaresi Başkanlığı)	E-belge uygulamalarına ilişkin düzenleme getiren Vergi Usul Kanunu Genel Tebliği Sıra No: 509	**V.1.2 (7):** Mükellefin, e-Belge gönderip alma işlemini özel entegrasyon izni alan mükelleflere ait bilgi işlem sistemi vasıtasıyla gerçekleştirmesi, muhafaza ve ibraz ödevlerini ortadan kaldırmaz. e-Belge gönderip alma işleminde kullanılan **bilgi işlem sistemi yazılım ve donanım alt yapısının Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde bulunması zorunludur.** **VI (4):** Mükelleflere ait e-Belgelerin yine mükelleflere ait bilgi işlem sistemlerinde saklanması esas olup üçüncü kişiler nezdinde de elektronik saklama yapılabilecektir. Başka mükelleflerden (Başkanlıktan izin alan saklamacı kuruluşlar dâhil) elektronik saklama hizmetinin alınması mükelleflerin e-Belgelerinin muhafaza ve ibraza ilişkin asli sorumluluğunu ortadan kaldırmaz. e-Belgelerin muhafazasının **Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde yapılması zorunludur.** Bu zorunluluk yurt dışında ikincil bir arşivleme yapılmasına engel teşkil etmez.
	Elektronik Defter, Kayıt ve Belgelerle İlgili Düzenleme Getiren 431 No.Lu Vergi Usul Kanunu Genel Tebliği	**Madde 7/3:** **Muhafaza ve ibraz işleminin Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde yapılması zorunludur**. Elektronik ortamda oluşturulan kayıtların muhafazası, mükelleflere ait bilgi işlem sistemlerinde gerçekleştirilir.
	1 Sıra No.lu Elektronik Defter Genel Tebliği	**Madde 4/1 (d):** Elektronik defterler ve beratların elektronik defter izni verilenlerin kendilerine ait bilgi işlem sistemlerinde muhafaza edilmesi mecburi olup, üçüncü kişiler nezdinde ya da yurt dışında muhafaza işlemi Başkanlık ve Genel Müdürlük açısından herhangi bir hüküm ifade etmemektedir. **Muhafaza yükümlülüğünün Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde yerine getirilmesi zorunludur.**

Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu	Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik	**Madde 16/5:** **Kuruluşların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.** Ancak, elektronik posta hizmetleri, telekonferans veya video konferans gibi hizmetler birincil ve ikincil sistemlerin yurt içinde bulundurulma zorunluluğundan istisnadır.
Ulaştırma ve Altyapı Bakanlığı	İnternet Alan Adları Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik	**Madde 8 (k):** **TRABİS'e entegre olan sistemlerini ve yedeklerini Türkiye Cumhuriyeti sınırları içinde bulundurmakla yükümlüdür.**
	Elektrikli Skuter Yönetmeliği	**Madde 8/1/c:** Gerçekleştirecekleri faaliyetlere ilişkin **verilerin tutulacağı veri tabanının saklanacağı sunucuların Türkiye Cumhuriyeti sınırları içerisinde barındırılması** ve İdarenin erişimine açık olması,
İçişleri Bakanlığı	Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği	**Madde 20/1:** KDHS, EKDS'ye ilişkin **imza oluşturma ve doğrulama verileri ile sertifikasını Türkiye Cumhuriyeti sınırları dışına çıkaramaz.**

3. Veri Yerelleştirmesi Hükümleri İçeren Mevzuat Konusunda Kamu Kurumlarının, Özel Sektör İşletmelerinin ve Sivil Toplum Kuruluşlarının Görüşleri

Bu raporun hazırlanmasına yardımcı olmak üzere sivil toplum kuruluşlarının ve özel sektör işletmelerinin görüşlerinin alınması amacıyla ayrı ayrı toplantılar düzenlenmiş, söz konusu toplantılara ilgili kamu kurumlarından da katılım sağlanmıştır. Bu kapsamda, sivil toplum kuruluşlarından Türk Sanayicileri ve İşinsanları Derneği (TÜSİAD), Uluslararası Yatırımcılar Derneği (YASED), Bilişim Sanayicileri Derneği (TÜBİSAD), Türkiye Odalar ve Borsalar Birliği (TOBB), Otomotiv Sanayii Derneği (OSD), Otomotiv Distribütörleri Derneği (ODD), Müstakil Sanayici ve İşadamları Derneği (MÜSİAD) ve Türkiye Bilişim Derneği (TBD); farklı sektörlerde faaliyet gösteren özel sektör işletmelerinden Ford Otosan, Vodafone İletişim, Figopara, Sefamerve, HSBC, Vestel Sağlık Grubu Hayriya Bilişim ve Sağlık Teknolojileri, BP ve Bosch tarafından görüş ve katkı alınmıştır.

3.1. Özel Sektör İşletmelerinin ve Sivil Toplum Kuruluşlarının Genel Görüş ve Değerlendirmeleri

Ticaretin bu kadar yoğun yaşandığı bir dönemde yurt dışına veri aktarımı kaçınılmazdır. Veri yerelleştirmesine yönelik düzenlemeler, işletmelerin ticari ve operasyonel faaliyetleri ile bunların sürdürülebilirliğini doğrudan, uluslararası rekabet koşullarını ise dolaylı olarak etkilemekte ve işletmeler yönünden etkin olmayan bir ekosisteme yol açmaktadır. **İşletmeler için mevcut yatırımların korunması ve yeni yatırım kararları için yurt dışına veri aktarımı yapılabilmesi kritik öneme sahiptir.**

Genel olarak birçok ülkede birçok işletme her gün yurt dışına veri aktarmakta, özellikle çok uluslu işletmeler genel merkezlerinde kurulu olan bilgi sistemlerini ve teknoloji araçlarını kullanmaktadır. Bu işletmeler faaliyetlerini yürütürken veriden değer üretmek için ana ortakları ile birlikte entegre bir şekilde bulut bilişim çözümlerinden ve veri analitiği servislerinden yararlanmaktadır. Ülkemizde faaliyet gösteren bazı çok uluslu işletmeler ise ilgili sektördeki veri yerelleştirmesi hükümleri içeren düzenlemeler sebebiyle farklı ülkelerdeki operasyonlarının tek merkezden yürütüldüğü yurt dışındaki sistemlere entegre olamamakta, bu bağlamda veri analitiği servislerinden yararlanamamakta ve dolayısıyla rekabetçiliklerini destekleyecek veriye dayalı üretim ve ürün geliştirme, raporlama ve işlem senkronizasyonu olanaklarından yoksun kalmaktadır.

Veri yerelleştirmesi sebebiyle yurt dışından verilen bulut bilişim hizmetlerinin kullanılamaması yeni hizmetler geliştirilirken verimlilik, maliyet, rekabet, gelişim, ürünün pazara girişi, sürdürülebilirlik ve ölçeklendirme gibi konularda büyük dezavantajlara sebebiyet vermekte ve bu dezavantajlar sonucunda **işletmeler tarafından, rekabet edilebilirliğin ve sürdürülebilirliğin sağlanması için ek maliyetlere katlanılmak durumunda kalınmaktadır. Katlanılan maliyetler nedeniyle müşteriye inovasyon olarak sunulabilecek**

katma değerli hizmetlerin/gelişmiş çözümlerin sunumu gecikmekte veya bu imkân tamamen ortadan kalkmaktadır.

Veri yerelleştirmesine ilişkin düzenlemeler, işletmeleri bulut bilişim alanında hizmet alımı için ülkemizdeki veri merkezlerine yönlendirse de ülkemizdeki veri merkezi işletmeleri tarafından sunulan hâlihazırdaki **bulut bilişim hizmetleri, her zaman tam olarak işletmelerin beklentilerini karşılayamamakta, hiper ölçekli bulut bilişim hizmeti sunan sağlayıcıların hizmetlerine nazaran bu nitelikteki hizmetler ülkemizde yeterli çeşitlilik ve olgunluk seviyesinde sağlanamayabilmektedir.**

İlgili düzenleyici ve denetleyici kurumların denetim yapabilmesi amacıyla oluşturulan **birincil, ikincil ve yedek bilgi sistemlerinin yurt içinde tutulması gibi veri yerelleştirmesi hükümleri içeren mevzuat sebebiyle işletmeler ya genel merkezlerinin kurduğu benzer yapıları ülkemizde ayrıca kurmak ve bunları işletmek için yüksek ve mükerrer maliyetlere katlanmak ya da Türkiye'deki hizmetlerini sonlandırmak durumu ile karşı karşıya kalmaktadır. Ayrıca bu durum, potansiyel yabancı yatırımcılar için Türk pazarının cazibesini azaltmaktadır.**

3.2. Özel Sektör İşletmeleri ve Sivil Toplum Kuruluşları Tarafından Sunulan Sektör ve Mevzuat Bazında Örnekler

Finans, ödeme sistemleri ve bankacılık sektöründeki veri yerelleştirmesi içeren mevzuatta[6] yer verilen **birincil ve ikincil bilgi sistemlerinin ve hatta bazı mevzuatla sistem yedeklerinin dahi yurt içinde bulundurulması, müşteri sırrı ya da örneğin banka sırrı niteliğinde olan her türlü verinin yurt dışındaki üçüncü kişilerle paylaşılmaması ya da bunlara aktarılmamasına ilişkin şartlar;** öncelikle yurt dışından verilen bulut bilişim hizmetlerinin işletmeler tarafından kullanılamamasına ve bulut bilişimin sağlayacağı faydalardan mahrum kalınmasına sebebiyet vermektedir. Öte yandan bu şartlar, Türkiye'de yerleşik olmayan ancak ülkemizde faaliyet yürüten yabancı işletmeler için Türkiye pazarına yatırım yapma konusunda çekinceler yaratmaktadır.

Küresel finans kuruluşları, gerek ölçek ekonomisinden yararlanarak maliyetleri kontrol edebilmek, gerekse uygulamalarda standardizasyon ve kalite seviyesini muhafaza edebilmek

[6] Sermaye Piyasası Kanunu, VII-128.9 sayılı Bilgi Sistemleri Yönetim Tebliği, Veri Depolama Kuruluşunun Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik, Kaydileştirilen Sermaye Piyasası Araçlarına İlişkin Kayıtların Tutulmasının Usul ve Esasları Hakkında Tebliğ, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanunu, Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmelik, Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ, 5411 Sayılı Bankacılık Kanunu, Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, Banka Kartları ve Kredi Kartları Hakkında Yönetmelik, Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, Bilgi Alışverişi, Takas, Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler İle İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu, Faktoring ve Finansman – Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ, E-belge uygulamalarına ilişkin düzenleme getiren Vergi Usul Kanunu Genel Tebliği Sıra No: 509, Elektronik Defter, Kayıt ve Belgelerle İlgili Düzenleme Getiren 431 No.Lu Vergi Usul Kanunu Genel Tebliği, 1 Sıra No.Lu Elektronik Defter Genel Tebliği, Dijital Hizmet Vergisi ile Bazı Kanunlarda ve 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun,

amacıyla, genellikle düşük maliyetli ülkelerde, tüm iştiraklerine farklı alanlarda hizmet veren "küresel hizmet merkezleri" (global service centers / centers of excellence) kurmakta ve işletmektedir. Bu hizmet merkezlerinden yararlanabilmek için ilgili verilerin yurtdışına çıkarılması zorunlu olmaktadır. Birincil ve ikincil bilgi sistemlerinin ve sistem yedeklerinin yurt içinde bulundurulması şartı işletmeler için milyonlarca dolar harcayıp tek merkezden yürüttükleri sistemlerin benzerlerinin ülkemizde kurulmasını ve işletilmesini gerektirdiği için işletmeleri, "Bu yüksek maliyete katlanılmalı mı, hizmet sunmayı sonlandırmalı mı?" soruları ile baş başa bırakmaktadır. Nitekim dünya çapında faaliyet gösteren finansal ödeme aracı işletmesi olan PayPal bu şartları yerine getirmeyerek 2016 yılı Haziran ayı itibariyle ülkemizden ayrılma kararı almıştır. Paypal'ın hizmet sunumunu sonlandırması yalnızca yatırım ortamını değil, düşük maliyetli finansal hizmetlerden ciddi anlamda fayda elde edebilecek küçük, orta ve büyük işletmeleri de etkilemiştir. Örneğin, 120 ülkeye ihracat yapan bir işletme olan Sefamerve, PayPal gibi finansal ödeme hizmetlerini müşterilerine kullandıramamaktan ötürü uluslararası rekabette ciddi dezavantajlar yaşadığını ifade etmektedir.

Benzer şekilde, söz konusu sektörleri etkileyen bir başka mevzuatta[7] yer verilen dış hizmet alınması durumunda dahi (örn. e-posta ve müşteri ilişkileri yönetimi (MİY/CRM) gibi hizmetler) dış hizmet sağlayıcısının söz konusu hizmete ilişkin faaliyetlerini yürütmede kullandığı bilgi sistemlerinin ve yedeklerinin yurt içinde tutulması şartı ise ya ihtiyaç duyulan hizmetin alınamamasına ya da dış hizmet sağlayıcıların sistemlerini ülkemize getirmesi sebebiyle yüksek uyum maliyetlerinin ortaya çıkmasına sebebiyet vermektedir. Kaldı ki, büyük ölçekli işletmelerin kullanmakta oldukları e-posta ve MİY/CRM gibi hizmetleri alabilecekleri dünya genelinde belli başlı sağlayıcılar bulunmakta, bu hizmet sağlayıcıların ise sunucuları genellikle tek merkezde olup ülkemiz içerisinde barındırılmamaktadır. Bu sebeple bu şarta uygunluk sağlanması ödeme hizmetleri alanında faaliyette bulunan işletmelerin yurt içi çalışma koşullarının zorlaştırılması sonucunu doğurmaktadır. Özellikle ana ortağı yurtdışında yerleşik olan Türkiye'deki iştiraklerin, küresel sistemleri kullanabilmesi, uluslararası yatırımcı konumundaki ana ortağın tabi olduğu yasal yükümlülükler çerçevesinde risk iştahını yönetebilmesi, iştiraklerini kontrol edebilmesi ve ülkeye olan güveni açısından da önem taşımaktadır.

Bahse konu sektörlerdeki düzenlemelerde geniş/muğlak kapsamların kullanılmasının yanı sıra **doğrudan bankacılık/ödeme hizmetleri/finans faaliyetleriyle ilgili olan ve yurt içinde tutulması gereken veriler ile dış hizmet alımında hizmet bazında doğrudan bankacılık/ödeme hizmetleri/finans faaliyetleriyle ilgili olmayan ve yurt dışına aktarılabilecek veriler belirlenip bu doğrultuda sınıflandırılma yapılmaması,** pratik işleyişte güçlüklere sebebiyet vermektedir.

[7] Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ

Telekomünikasyon sektörü açısından bakıldığında, bu sektörde veri yerelleştirmesi yönünde hükümler içeren bir Kurul Kararında[8] yer verilen e-Call ile birlikte katma değerli hizmet sunumuna imkân sağlayan haberleşme sistemlerinde hizmet verecek sunucuların ülkemizde bulundurulması şartı otomotiv sektörünü ciddi anlamda etkilemekte, sunucuları yurt dışında bulunan tüm üreticilerin büyük uyum maliyetlerine katlanarak sunucularını Türkiye'de de kurup işletmesi ya da tüm ilgili hizmetlerini sonlandırması sonuçlarına yol açmaktadır. Bir otomotiv işletmesi olan Honda bu düzenlemeden oldukça etkilendiklerini çeşitli platformlarda ifade etmiştir. Düzenlemenin tüketiciye etkisi ise araçların bağlanılırlık ve katma değerli hizmet özelliklerinin kullanım dışı bırakılması suretiyle tüketici faydasının azalması yönünde olmuştur. Ayrıca, bağlantılı araçlar ile otomotiv şirketleri tüketici faydasını artırmanın yanı sıra araç güvenliğini de iyileştirmeyi hedeflemektedir. Bahsi geçen küresel sistemlerin tamamında, araç içerisinde yer alan ve bağlanabilirlik özelliklerini sağlayan donanım modülleri, sadece yurt dışında bulunan bu küresel sistemler ile çalışabilecek şekilde tasarlanmış ve üretilmiş durumdadır. Buradaki amaç, özellikle araçlar üzerindeki donanım modülleri ile küresel sistemler arasındaki haberleşme mekanizmalarının güvenliğidir. Bu amaçla, araçlardaki donanım modülleri ile küresel sistemler arasında, sadece bu iki unsurun bilebildiği / tanıyabildiği ve üçüncü tarafların araya giremediği ve şifrelenmiş veriyi göremediği özel güvenlik mekanizmaları kullanılmaktadır.

Son dönemde Türkiye'nin de TOGG ile birlikte önemli bir katkı sağlayacağı şüphesiz olan elektrikli araçlar sektörü için de bağlantılı araç sistemlerinin kullanılması önemli bir gerekliliktir. Tüketici en yakın şarj istasyonunu; mevcut şarj ile ne kadar mesafe gidebileceğini, ne kadar sürede şarjının dolabileceğini bu sistemler sayesinde öğrenebilecektir. Araçların tüm bilgisi "bağlantılı veri" ile önem kazanacaktır. Şarj istasyonları için de bu sistemler kaçınılmaz olacaktır.

Bağlantılı araçlar ve otonom araçlar gibi teknolojilerin geliştirilmesi ve kullanılması için bulut bilişim teknolojisi ve veri analitiği kritik önemdedir. Bulut bilişim hizmetlerinden ve entegre akıllı üretim yöntemlerinden faydalanılamaması, ilerleyen yıllarda bu alanda ülkemizin küresel rekabetçiliğini azaltabilecektir. Mevcut regülasyon kısıtlamalarının sürmesi halinde bağlanabilirlik hizmetlerinin verilemeyecek olması nedeniyle otonom sürüş yetenekleri gibi özellikler de sağlanamayabilecektir. Local Hazard Information (LHI) Services gibi Avrupa'da hâlihazırda devreye girmek üzere olan sürüş güvenliğine önemli katkı sağlayacak sistemler de bu durumda sağlanamayacaktır. Bu durum Türk tüketicilerinin gelişen teknolojilerden ve güvenlik sistemlerinden mahrum kalmasının yanında, Türk mühendislerine know-how transferinin önünde de engel oluşturacaktır. Ayrıca, söz konusu bağlantılı araçların uygulamalarının ürettiği verilerden hangilerinin kişisel veri olarak kabul edileceği noktasında da belirsizlik bulunmakta ve kişisel veri ile araç verisinin tanımını net olarak ortaya koyan bir rehber bulunmamaktadır.

[8] 112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call) Konulu Kurul Kararı

Otonom araç sayısının hızlı bir şekilde arttığı günümüzde, **bulut bilişim hizmetlerinin kullanılmasına imkân vermeyen bahse konu düzenlemeler araçların birbirleri ile haberleşmesi ve sürüş güvenliği hizmetlerinin sağlanması yönünden otomotiv sektörünün faaliyetlerini zorlaştırmaktadır.**

İncelemeye telekomünikasyon sektörü üzerinden devam edildiğinde, ilgili Kanunda[9]; **kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verilerinin ancak ilgili kişilerin açık rızalarının alınması koşuluyla yurt dışına aktarılabileceği şartı** getirilmiştir. Aralık 2020 tarihinde yürürlüğe giren bir Yönetmelikle[10] ise **milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmamasının esas olacağı, ancak üçüncü tarafın yurt dışında olması halinde aktarılacak verinin kapsamı, aktarılacak tarafın adı ve açık adresi, aktarma amacı ve süresi, verinin aktarılacağı ülkenin adı bilgileri verilerek ayrıca açık rıza alınması şartı** getirilmiştir. Söz konusu yönetmelik kapsamında, açık rıza koşullarının ilgili kanuna nazaran ağırlaştırıldığı görülmektedir. Ülkemizde faaliyet gösteren ve hâlihazırda yetkilendirilmiş işletmeler elektronik haberleşme sektöründeki kişisel verileri yurt dışına aktarımı yönünden yürürlükteki mevzuat kapsamında bazı şartlara tabi tutulmuştur. Oysaki ülkemizde faaliyet gösteren ancak yerleşik olmayan/temsilcisi bulunmayan yetkilendirilmemiş işletmeler hâlihazırda elektronik haberleşme sektöründeki kişisel verileri herhangi bir şarta tabi olmadan yurt dışına kolayca aktarabilmektedir. Bu durum rekabet dezavantajı oluşturmaktadır. **Özellikle trafik ve konum verisinin tanımının tam olarak netleştirilmemesi ve açık rıza koşullarının yanı sıra açık rıza dışındaki mekanizmaların/alternatif koşulların da yurtdışına veri aktarımı kapsamında kullanılmaması düzenlemelerin olduğundan daha ağır bir şekilde uygulanmasına sebebiyet vermektedir.**

Telekomünikasyon sektöründeki diğer ilgili düzenlemeler[11] ile **kullanıcı bilgilerinin, imza oluşturma ve doğrulama verilerine ilişkin birincil, ikincil ve yedek sistemlerinin ülkemizde tutulmasına yönelik** çeşitli veri yerelleştirme şartları getirildiği görülmektedir. Bu düzenlemeler tıpkı diğer sektörlerdeki gibi yurt dışındaki bulut bilişim teknolojilerinin kullanılamamasına neden olmakta ve potansiyel faydalardan yararlanmayı engellemektedir.

Ulaştırma sektörü açısından bakıldığında, Elektrikli Skuter Yönetmeliği'nde **gerçekleştirilen faaliyetlere ilişkin verilerin tutulacağı veri tabanının saklanacağı sunucuların ülkemiz sınırları içerisinde barındırılması ve İdarenin erişimine açık olması şartı**, sağlık sektörü incelendiğinde Sağlık Bilgi Sistemleri Uygulamaları Hakkında 2015/17 sayılı Genelgede **bilgi sistemlerindeki veriler, sağlık tesislerindeki veri kayıt ortamları, Bakanlık merkezi veri kayıt ortamı ya da Genel Müdürlüğün onayladığı veri kayıt ortamları haricinde hiçbir**

[9] 5809 Sayılı Elektronik Haberleşme Kanunu
[10] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönetmeliği
[11] Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Uzaktan Programlanabilir SIM Teknolojileri (eSIM) Konulu Kurul Kararı, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar, Kayıtlı Elektronik Posta (KEP) Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, İnternet Alan Adları Yönetmeliği

yere kaydedilemez ve gönderilemez şartı ile Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği'nde ise **kimlik doğrulama hizmet sağlayıcısı, elektronik kimlik doğrulama sistemine ilişkin imza oluşturma ve doğrulama verileri ile sertifikasını ülke sınırları dışına çıkaramaz şartı** da veri yerelleştirmesine örnek olarak gösterilebilir. Bu veri yerelleştirmesi hükümleri de yukarıda ayrıntılarına değinildiği üzere bulut bilişimin hiç kullanılamamasına veya uyum maliyetlerine sebebiyet vermektedir.

3.3. Kamu Kurumlarının Genel Görüş ve Değerlendirmeleri

Ülkemizde kamu kurumları tarafından veri yerelleştirmesi düzenlemelerinin başlangıçta kritik sektörler için uygulanması eğilimi, giderek artan bir şekilde diğer sektörlere de uygulanması şeklinde değişmiştir. Bu durum, işbu raporun ikinci bölümünde ayrıntılı bir şekilde değinildiği üzere bankacılık, telekomünikasyon, ulaşım, sağlık, finans, ödeme hizmetleri ve sigortacılık gibi farklı sektörlerin birincil ve ikincil mevzuatı incelendiğinde açıkça görülmektedir.

Bir kamu kurumu tarafından veri yerelleştirmesi hükümleri içeren bir düzenleme, her ne kadar spesifik bir amaca hizmet etmek için oluşturulsa da son zamanlarda kamu kurumları tarafından yaygın bir şekilde tercih edilen bahse konu düzenlemelerin temel gerekçelerinin aşağıda belirtilen ana hususlar altında toplanabileceği değerlendirilmektedir.

- **Milli güvenlik kaygıları,**
- **Yönetim ilkeleri çerçevesinde işletmeler üzerinde denetim ve inceleme mekanizmalarının etkin bir şekilde kullanılabilmesi yönünden bilgi ve belgelere hızlı ve kolay erişim (availability),**
- **Veri gizliliğinin (confidentiality) sağlanması,**
- **Verilerin ülke içerisinde kalmasının sağlanarak veriyle ilgili operasyonlara ilişkin yerli katma değerin artırılması.**

Kamu kurumları tarafından özellikle sistemlerin ve verilerin yurt içinde tutulması sonucunda; ülkenin kritik verilerinin yurtdışına aktarılarak veri işleme, anlamlandırma, yapay zekâ uygulamaları ve istihbarat faaliyetlerinde kullanılmamasının sağlanması, ölçek ekonomisinin verdiği avantajla küresel firmaların yerli firmalara karşı haksız rekabet içinde bulunmaları engellenerek yerli firmaların gelişimlerinin desteklenmesi ve yurtiçinde akredite edilmiş veri merkezleri kurulumlarının yapılması ve nitelikli insan kaynağının yetiştirilmesi gibi faydaların da ülkemize kazandırılacağı ifade edilmektedir.

Diğer taraftan, veri yerelleştirmesi içeren mevzuat incelendiğinde, **aynı sektörde, aynı amaç doğrultusunda ve aynı temel gerekçe ile oluşan mevzuatın uygulanmasında kamu kurumları tarafından farklı yaklaşımlar sergilenebilmektedir.** Örneğin, yerinde denetim ve inceleme yükümlüğü bulunan finans, ödeme sistemleri ve bankacılık sektörlerinde ilgili kamu kurumları tarafından yapılacak olan inceleme ve denetimlerde gerekli bilgi, belgelere ve sunuculara hızlı ve kolay erişimin sağlanması gerekçesiyle veri yerelleştirmesi düzenlemelerine

gidilerek bilgi sistemlerinin yurt içinde barındırılması zorunlu tutulmaktadır. Bir kamu kurumun sistem yerelleştirmesine ilişkin ilgili mevzuatında birincil, ikincil ve yedek sistemlerin yurtiçinde barındırılması şartı bulunurken; başka bir kamu kurumunun ilgili mevzuatında birincil ve ikincil sistemlerinin yurtiçinde barındırılması şartı getirilmesine rağmen yedek sistemlerin yurt dışında barındırılamayacağına ilişkin herhangi bir şart getirilmemektedir. Nihayetinde bu durum, **aynı amaç doğrultusunda ve aynı temel gerekçe ile oluşan mevzuatın uygulanmasında kimi kamu kurumlarının daha katı bir veri yerelleştirme anlayışı benimsediğini kimi kamu kurumlarının ise daha esnek bir veri yerelleştirme anlayışı benimsediğini açıkça göstermektedir.**

Her ne kadar aynı sektörde, aynı amaç doğrultusunda ve aynı temel gerekçe ile oluşturulan mevzuatın uygulanmasında kamu kurumları tarafından farklı yaklaşımlar gösterilse de bazı kamu kurumları tarafından önceden benimsenmiş katı veri yerelleştirmesi anlayışlarının güncel teknolojideki ve iş modellerinde değişimler ile giderek esnekleşmeye başlandığı örnekler de son zamanlarda gündeme gelmektedir. **Örneğin, 1 Aralık 2021 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren "Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik"in 19 uncu maddesi uyarınca PayPal gibi yurt dışında yerleşik ödeme hizmeti sağlayıcıların yurt içinde yerleşik ödeme hizmeti sağlayıcılar ile birlikte ödeme hizmeti sunabilmeleri mümkün kılınmıştır.** Söz konusu madde kapsamındaki iş birliği, ödeme hizmeti sağlayıcısının Kanun kapsamına giren ödeme hizmetlerini yurt içinde yerleşik müşterilerine yurt dışında yerleşik tüzel kişi ile birlikte sunması şeklindedir ve sadece gönderen veya alıcıdan en az birisinin yurt dışında bulunduğu ödeme hizmetleri ile sınırlı olacak şekilde yapılabilir. **Kurulacak iş birliği neticesinde sunulacak hizmete ilişkin tüm işlemlerin yurtiçinde yerleşik ödeme hizmeti sağlayıcısının bilgi sistemleri üzerinden geçmesi ve denetim izinlerinin yurtiçinde yerleşik ödeme hizmeti sağlayıcısı tarafından tutulması durumunda, iş birliği yapılacak yurt dışında yerleşik tüzel kişinin bilgi sistemlerinin Türkiye'de bulunma zorunluluğu aranmamaktadır.**

4. Uluslararası Kuruluşların Çalışmaları ve Yaklaşımları

Günümüzde veriye atfedilen değer arttıkça verilerin yurtdışına aktarımı hususu da giderek önem kazanmış, verinin serbest dolaşımı konusunda AB, OECD, G20, G7 ve Dünya Ekonomik Forumu gibi uluslararası kuruluşlar tarafından çalışmalar başlatılmıştır. Söz konusu kuruluşlarda temsil edilen ülkelerin bu hususstaki pozisyonları temelde büyük ölçekli teknoloji işletmelerini ne ölçüde kontrol edebildiklerine göre şekillenmektedir. ABD ve Japonya gibi bazı gelişmiş ülkeler yurt dışına veri aktarımlarının mümkün olduğunca kolaylaştırılması ve mümkün olduğunca veri yerelleştirme uygulamalarına gidilmemesi yönünde pozisyon alırken kimi AB ülkeleri gibi gelişmiş bazı ülkeler ile gelişmekte olan ülkelerin çoğu ise bu hususta veri mahremiyeti ve güvenliği ile ticari hayatın gereklilikleri arasında denge gözetmeyi amaçlayan bir politika benimsemektedir. Bu çekişmenin uluslararası ticareti aksatabileceği endişesiyle uluslararası kuruluşlar ülkelerin güvenlik çekincelerini mümkün mertebe ortadan kaldırabilecek güvenli ve adil veri aktarımının sağlanmasını teşvik edici politikalar ve düzenlemeler yapılması yönünde çalışmalar yürütmektedir. Bu bölümde AB, OECD, G20, G7 ve Dünya Ekonomi Forumu'nun konuya ilişkin çalışma ve yaklaşımlarına yer verilmektedir.

OECD, birçok ülkenin dikkate aldığı politika, tavsiye kararı ve rehber hazırlayan bir uluslararası kuruluş olması statüsüyle, dijital veri kapsamındaki küresel politikaların seyrinde önemli bir yere sahiptir. OECD tarafından verinin ekonomik değeri ve küresel ticarete etkisi erken dönemde incelenmeye başlanmış, bünyesinde dijital veri çalışmaları kapsamında Dijital Ekonomi Politikaları Komitesi (The Committee on Digital Economy Policy - CDEP) ve bu komitenin altında Veri Yönetişimi ve Gizliliği Çalışma Grubu (Working Party Data Governance and Privacy-WPDGP) oluşturulmuş ve ülkelere veri aktarımı hususunda yön verebilecek birçok tavsiye kararı[12] yayımlanmıştır.

OECD tarafından erken dönemde yurt dışına veri aktarımının ehemmiyeti anlaşılarak **uluslararası veri aktarımını kolaylaştırıcı düzenlemelere yön vermek adına**, Dijital Ekonomi Politikası Komitesi, Bilimsel ve Teknolojik Politika Komitesi (The Committee for Scientific and Technological Policy - CSTP) ve Kamu Yönetimi Komitesi (The Public Governance Committee - PGC) tarafından ortaklaşa olarak geliştirilen "**Verilere Erişimin ve Paylaşımın Geliştirilmesine İlişkin Konsey Tavsiyesi**[13]" kararı Ekim 2021 tarihinde alınmıştır. Bu tavsiye kararında hükümetlerin, bireylerin ve kuruluşların haklarını koruyup aynı zamanda meşru çıkar ve hedeflerini göz önünde bulundurarak, dijital verilere erişim ve verilerin paylaşımı düzenlemelerinden nasıl maksimum fayda sağlanabileceğine ilişkin genel ilkeler ve politikalar belirlenmiştir. Söz konusu tavsiye kararındaki önemli hususlar aşağıda sunulmaktadır;

[12] Kamu Sektörü Bilgilerinin Geliştirilmiş Erişimi ve Daha Etkili Kullanımı için Konsey Tavsiyesi, OECD Konseyi'nin Kamu Mali Kaynaklarından Araştırma Verilerine Erişime İlişkin Tavsiyesi, Dijital Yönetim Stratejileri Konseyi'nin Tavsiyesi, Sağlık Veri Yönetimine İlişkin Tavsiye, Açık Yönetim Konseyi'nin Tavsiyesi, Verilere Erişimi ve Veri Paylaşımını Geliştirmeye İlişkin Taslak Öneri

[13] Recommendation of the Council on Enhancing Access to and Sharing of Data

- **Veri Ekosisteminde Güvenin Güçlendirilmesi**
  - İlgili tüm paydaşların güçlendirilmesi ve veri ekosisteminin güvenilirliğini artırma çabalarına proaktif olarak katılımlarının desteklenmesi,
  - **Veri erişimine ve paylaşımına yönelik stratejik bir hükümet yaklaşımının benimsenmesi,**
  - Birey ve kuruluşların haklarını koruyup aynı zamanda veri yönetişimi sorumluluğu kültürünü teşvik etmek ve mümkün kılmak doğrultusunda meşru çıkar ve hedefleri göz önünde bulundurarak **veri erişiminin ve paylaşımının maksimuma çıkarılması**,

- **Veriye Yatırımın Teşvik Edilmesi ve Veriye Erişimin ve Paylaşımın Teşvik Edilmesi**
  - **Veri erişimi ve paylaşımı için sürdürülebilir iş modellerinin ve pazarlarının geliştirilmesi ve benimsenmesi için gerekli koşulların ve tutarlı teşvik mekanizmalarının sağlanması,**

- **Toplum Genelinde Etkili ve Sorumlu Veri Erişiminin, Paylaşımının ve Kullanımının Geliştirilmesi**
  - **Sınır ötesi veri erişimi ve güvenli veri paylaşımı için koşulların iyileştirilmesi**,
  - Kamu ve özel sektörde, kuruluşların birbirleri arasında verilerin bulunabilirliğinin, erişilebilirliğinin, birlikte çalışabilirliğinin ve yeniden kullanılabilirliğinin teşvik edilmesi,
  - Verileri etkin ve veri döngüsü içerisinde sorumlu bir şekilde kullanmak için tüm paydaşların kapasitesinin artırılması.

"OECD Veri Yerelleştirme Eğilimleri ve Zorlukları (Data Localization Trends and Challanges: Considirations for the review of the Privacy Guidelines)'' adlı raporda da veri gizliliği yasalarının, sınır ötesi veri akışına ilişkin getirdiği etkinin, veri yerelleştirmesini gerektirip gerektirmediği konusunun ayrıca ele alınıp değerlendirilmesi önerilmiştir. Veri yerelleştirme, bazı durumlarda veri gizliliğini korurken bazı durumlarda ise veri gizliliğine zarar verebileceğinden, **herhangi bir veri yerelleştirmesinin veri gizliliği üzerindeki etkisinin değerlendirilmesinin bütünsel ve bağlama özel yapılması gerekliliği değerlendirilmiştir**.[14] G20 tarafında ise ekonomik büyümenin, kalkınmanın ve sosyal refahın sağlayıcısı olarak verilerin etkin kullanımının kritik rol oynadığı[15] konusunda hemfikir olan liderler tarafından, özellikle dijitalleşmenin herkesin yararına kullanılması için verinin güvenli serbest dolaşımına (Digitalization, Data Free Flow With Trust) ilişkin çalışmalar yürütülmektedir. Bu çalışma kapsamında aşağıda sunulan hususlar üzerinde durulmuştur;

- Yurt dışına veri aktarımının beraberinde getirdiği gizlilik, verilerin korunması, fikri mülkiyet hakları ve güvenlik gibi zorluklar ile mücadele edilmesi,

[14] Data localisation trends and challenges : Considerations for the review of the Privacy Guidelines | OECD Digital Economy Papers | OECD iLibrary (oecd-ilibrary.org)
[15] https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

- Verinin serbest akışını desteklemek için tüketici ve işletmeler arasında güvenin güçlendirilmesi,
- Ulusal ve uluslararası yasal çerçevelere saygı gösterilmesi, yasal çerçevelerin birlikte çalışılabilirliğini teşvik etmek için iş birliğinin teşvik edilmesi,
- Yenilikçi, çevik, esnek ve etkili düzenleyici yaklaşımların ve çerçevelerin dijital çağa uyarlanması.

Dünya Ekonomik Forumu tarafından konu kapsamında düzenli olarak çeşitli raporların yayımlanmasının yanı sıra "Teknoloji Yönetişiminin Geleceğini Şekillendirmek: Veri Politikası (Shaping the Future of Technology Governance: Data Policy[16])" isimli bir platform kurulmuştur. Bu platform; kullanıcıları veri ekonomisiyle ilişkili risklerden korurken topluma fayda sağlamak için veri kullanımını en üst düzeye çıkarmaya odaklanmaktadır. Platformun amacı ise inovasyonu teşvik etmek ve verilerin sorumlu kullanımını hızlandırmak için ileriye dönük, birlikte çalışabilir ve güvenilir veri politikalarının tasarlanması, denenmesi ve ölçeklendirilmesidir.

Ayrıca Dünya Ekonomi Forumu tarafından "Uluslararası Veri Akışında Yol Haritası: Dijital Ekonomide Rekabetçiliği Yakalamak (A Roadmap for CrossBorder Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy[17])" adlı bir rapor hazırlanarak uluslararası veri aktarımının dijital ekonomideki durumuna yer verilmiştir. Aşağıdaki tabloda yer aldığı üzere bu raporda uluslararası veri akışında etkinliğin sağlanması için başarıya giden bir yol haritası oluşturmuştur.

Tablo 2: Dünya Ekonomi Forumu -Uluslararası Veri Akışında Yol Haritası

1. Güvenin yeniden inşası	• Veri akışını serbest bırak. • Veriyi korumaya al. • Siber güvenliği sağla.
2. Ülkelerarası işbirliğinin teşviki	• Ülkeler arasında hesap verebilirliği sağlamlaştır. • Bağlantı kalitesini, ülkelerarası işlerliği, veri taşınabilirliğini ve bütünlüğü koru. • Bağlantı kalitesi (Bağlantısallık, 5G politikaları ve yüksek performanslı bilgi işlem) • Teknik uyumluluk • Veri taşınabilirliği • Veri bütünlüğü

[16] https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-data-policy
[17] https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy

3. **Veri paylaşımı politikalarının düzenlenmesi**	• Politikaları geleceğe uyumlu hale getir. • Federe öğrenme teknolojisi. • Veri birlikleri.

G7 tarafından ise veriden sağlanacak potansiyel faydalardan yararlanabilmek için birlikte çalışmanın önem taşıdığını gösteren bir çalışma olan "Roadmap for Cooperation on Data Free Flow with Trust[18]" ve G20 Liderlerinin Riyadh Deklarasyonu yayımlanmıştır.

G7 ülkelerinin anılan çalışmaları ile **verinin güvenli serbest akışının faydalarından yararlanmasına yönelik somut ilerleme sağlamak için bir yol haritası çizilmiştir.** Bu yol haritasına göre G7 ülkeleri, aşağıdaki dört ortak eylem adımını ortaya koymaktadır;

- **Veri Yerelleştirme:** Veri yerelleştirme önlemlerinin etkilerine ilişkin **kanıt temelli yaklaşımlar** ve bu yaklaşımlara **karşı alternatif politikalar** oluşturulacaktır.
- **Mevzuata Yönelik İşbirlikleri:** The G7 Digital and Tech yetkilileri, sınır ötesi veri aktarımına yönelik düzenleyici yaklaşımlardaki ortak noktaları belirleyecek, düzenleyici uygulamalar ve ülkeler arasındaki işbirliğini sağlayacaktır.
- **Devletin Verilere Erişimi:** Mâkul ilkeler ölçüsünde veri erişimini kolaylaştıran yasal düzenlemeleri sürdürmeye kararlılıkla devam edilecektir. Bu konuda OECD'nin "Özel sektör tarafından tutulan kişisel verilere devlet tarafından güvenilir erişim" üzerinde çalışan grubun amaç ve hedefleri desteklenecektir.
- **Öncelikli Sektörler için Veri Paylaşımı**: Üzerinde anlaşmaya varılan öncelikli sektörlerde karşılıklı olarak kabul edilebilir veri paylaşımı uygulamalarının geliştirilmesi hızlandırılacaktır.

Öte yandan, dijital çağda ekonominin giderek daha fazla veriye bağlı olduğunu gören Avrupa Parlamentosu ve AB Konseyince, farklı AB ülkeleri ve bu ülkelerdeki bilişim sistemleri arasındaki kişisel olmayan verilerin serbest dolaşımına yönelik engellerin kaldırılması amacıyla, 2019 yılında "Kişisel Olmayan Verilerin Serbest Akışına İlişkin Düzenleme[19]" (Regulation On A Framework For The Free Flow Of Non-Personal Data In The EU) yayımlanmıştır. Sürekli geliştirilen bu çalışmalar doğrultusunda, ayrıca ek bir kılavuz ortaya konulmuştur. Bahse konu düzenleme ve kılavuzda değinilen ana hususlara aşağıda yer verilmektedir;

- **Kişisel Olmayan Verilerin Sınırlar Arasında Serbest Dolaşımı**: Her kuruluş, AB ülkeleri içerisinde herhangi bir yerde verileri depolayabilmeli ve işleyebilmelidir.

[18] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf

[19] https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)495&lang=en

- **Veri Yerelleştirme Kısıtlamalarını Önleme**: Üye devletler, planlanmakta olan herhangi bir veri yerelleştirme kısıtlaması **varsa bu kısıtlamaların değerlendirilmesi için Komisyona bildirmek zorundadır.**
- **Karışık Veri Kümeleri İçin Kurallar:** Karma bir veri kümesi olması durumunda, kişisel verilerin serbest akışını garanti eden Avrupa Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerle ilgili olan veri seti kısmına uygulanırken kişisel olmayan verilerin serbest dolaşımı ile ilgili düzenlemeler de kişisel olmayan veri seti için uygulanır.
- **Bulut Hizmeti Sağlayıcıları Arasında Daha Kolay Geçiş**: Servis sağlayıcılar, çeşitli bulut servis sağlayıcıları arasında geçiş yapılabilmesinin kolaylaştırılması amacı taşıyan bir bulut servisleri rehberi hazırlamaları konusunda teşvik edilecektir. Bu durum, bulut hizmetleri için piyasayı daha esnek hale getirirken aynı zamanda AB içerisindeki veri içeren servisleri daha ekonomik hale getirecektir.
- **Düzenleyici Kontrol İçin Veriye Erişim**: Yetkili kamu otoriteleri, verinin AB içerisinde saklandığı ve işlendiği her yere inceleme ve denetleme amacıyla erişebilecektir. Üye devletler, yetkili makamın başka bir üye devlette saklanan verilerine erişim talebine cevap vermeyen kullanıcılara ise yaptırım uygulayabileceklerdir.
- **Siber Güvenliğin Sağlanması:** İlgili siber güvenlik düzenlemelerini içeren paket ile tam tutarlılığın sağlanması amaçlanarak, işletmelerin hâlihazırda geçerli olan veri depolama ve veri işleme ile ilgili güvenlik gereksinimleri AB sınırları içerisinde veya bulutta verileri depoladıkları ya da işledikleri aynı şekliyle devam ettirilecektir.

Görüldüğü üzere, verilerin serbest dolaşımı sadece ülkemizin değil, uluslararası kuruluşların da gündeminde yoğun şekilde yer almaktadır. Veriye dayalı yenilikçiliğin odağında yer alan etkin veri paylaşımı, küresel değer zincirlerine katılım sağlamak isteyen ülkeler için stratejik önemi haizdir. Bu değer zincirlerinin bir parçası olmak ve veri temelli ekonominin her yönüyle gelişimini sağlamak için doğru, ticari yaşamın akışını olumsuz etkilemeyecek hukuki düzenleme ve süreçler tasarlamanın yanı sıra mevcuttakiler de iyileştirilmedir.

5. Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi İçin Öneriler

5.1. Genel Değerlendirme

Özellikle son 10 yılda hızlanan dijitalleşme sürecinin sonucu olarak, hem yerel hem de küresel ölçekte üretkenliği ve rekabet gücünü artırmak üzere, mevcut değer zincirleri yeniden yapılanmakta ve yeni değer zincirleri ortaya çıkmaktadır. Birçok durumda söz konusu değer zincirleri, farklı ülkelerde bulunan veya farklı ülkelerin mevzuatına tabi paydaşların (bireyler, firmalar, devlet kurumları vb.) dahliyle oluşturulmakta, doğal olarak bu değer zincirlerinin etkin şekilde işlemesi de bahse konu paydaşlara ait veya onların kontrolündeki dijital verilerin değer zincirinde yer alan diğer paydaşlarla paylaşılmasını gerektirmektedir. Her ne kadar sınır aşan nitelikteki bu veri transferleri küresel değer zincirlerine eklemlenmek ve hem işletme hem de ülke ölçeğinde üretkenlik ve rekabet gücünü artırmak açısından son derece önemli olsa da, bahse konu dijital verilerin diğer ülkelerdeki paydaşlarla paylaşımının ülkeler açısından mahremiyet ve ekonomik çıkar ile siber ve ulusal güvenlik boyutları olan çeşitli çekinceleri ortaya çıkardığı da gözlenmektedir. Diğer bir ifadeyle, ülkeler açısından sınır aşan veri transferlerinin sağlayabileceği ekonomik fayda ile ortaya çıkardığı güvenlik ve mahremiyet çekincelerini dengeleyebilecek mekanizmalar geliştirilmesi gerekmektedir. Nitekim bu dokümanın dördüncü bölümünde de açıklandığı üzere, birçok uluslararası kuruluş bu dengeleme mekanizmalarının oluşturulmasına yönelik temel ilke, politika ve düzenlemeleri geliştirme konusunda yoğun çaba sarf etmektedir.

Her ne kadar sınır aşan veri transferlerine yönelik uluslararası politikalar ve düzenleyici çerçeveler tam anlamıyla olgunlaşmış olmasa da, yukarıda bahsi geçen çalışmalar dikkate alındığında, sınır aşan veri transferlerine yönelik ilke, politika ve düzenlemelerin temelde iki unsuru benimsediği görülmektedir. Bunlardan ilki, bahse konu verilerin yaşam döngüsünün yönetimi (verilerin hangi şartlarda ve ne şekilde işlenip üçüncü taraflarla paylaşılacağı, devlet kurumlarının verilere hangi şartlarda erişeceği, verilerin güvenliğini temin etmeye dönük alınması gereken teknik ve idari tedbirler, verilerin hangi sıklıkla güncelleneceği ve hangi şartlar altında silineceği, verilere ilişkin fikri mülkiyet ve telif haklarının sahipliği vb.) açısından ilgili ülkelerin üzerinde mutabık kaldığı ve tüm bu ülkelerde aynı şekilde uygulanacak ortak kuralların belirlenmesi suretiyle farklı ülkelerin ve bu ülkelerdeki paydaşların veri paylaşım ekosistemine güven duymasının temin edilmesidir. Böylesi **bir güven ortamının oluşturulması ve korunması, sınır aşan veri paylaşımı ekosisteminde yer alan paydaşların mahremiyet ve güvenlik çekincelerine sebep olan farklı risk unsurlarından oluşan "toplam riski" azaltarak veri paylaşımı ile bu paylaşımın sağlayacağı üretkenlik ve rekabet gücü artışlarını gerçekleştirmeyi kolaylaştırmaktadır.** Örneğin, AB'nin GDPR düzenlemesinin amaçlarından biri de, kişisel veriler açısından böylesi bir "güvenilir veri paylaşım ekosistemi" oluşturmaktır.

Diğer taraftan, "**toplam riski"** azaltmaya yönelik uluslararası kural ve mekanizmalar geliştirilse de, bu kural ve mekanizmaların yeterli ve etkin şekilde karşılayamadığı mahremiyet ve güvenlik çekinceleri kalmaya devam edecektir. Diğer bir ifadeyle, "**toplam risk"** azaltılmış

olsa bile hala ekosistemdeki bazı ülkeler veya paydaşlar açısından kabul edilebilir riskin üzerinde olabilir. Bu nedenle, birçok ülkenin, diğer ülkelerden bağımsız şekilde, sınır aşan veri transferleri için kendi risk algısını ve değerlendirmesini yansıtan özel tedbirler aldığı da görülmektedir. Örneğin, hâlihazırda birçok ülkede benimsenen çeşitli sektörel veri yerelleştirme uygulamaları bu kapsamdadır.

Verinin "**bağlamsal doğası"** nedeniyle, sınır aşan veri paylaşımı ekosisteminde yer alan tüm paydaşların üzerinde mutabık kalacağı ve her bir paydaşın risk değerlendirmesini tam olarak karşılayıp uygulayabileceği ortak kurallar belirlemek oldukça zordur. Bu nedenle, **veri yerelleştirmesi kısıtlamalarına yönelik olarak, öngörülen kısıtlamaya temel teşkil eden çekinceye konu duruma ve şartlara özel, etraflı ve sağlıklı bir risk değerlendirmesine ve fayda-maliyet analizine dayanan mâkul ve orantılı tedbirlerin ilgili ülkelerce alınabileceği uluslararası kuruluşlarca da genellikle kabul gören bir yaklaşımdır.** Bu da yukarıda bahsi geçen ilke, politika ve düzenlemelerin ikinci unsurudur. Örneğin, G7 veri yerelleştirme önlemlerinin etkilerine yönelik kanıt temelli yaklaşımlar benimsenmesini önermektedir. Benzer şekilde AB de, kişisel olmayan veriler açısından üye ülkelerin veri yerelleştirme yönünde alacakları tedbirlere ilişkin, Komisyon'un kapsam ve gerekçeye yönelik olarak önceden bilgilendirilmesini talep etmektedir.

Konu Türkiye açısından değerlendirildiğinde; ülkemizde veri yerelleştirmesine yönelik çeşitli sektörel düzenlemelerin bulunduğu görülmekte, ilgili sektörlerde faaliyet gösteren özellikle çok uluslu işletmelerin Türkiye'deki birimleri ve/veya ortaklıkları ile yurtdışındaki işletmelerle yoğun ticari ilişkileri olan Türk işletmelerinin bu düzenlemelerden ciddi anlamda olumsuz etkilendiği anlaşılmaktadır. Ayrıca, sektörel veri yerelleştirme düzenlemelerinden ayrı olarak, KVKK'nın, AB'nin GDPR düzenlemesine tam uyumunun temin edilmemiş olması ve Türkiye'nin AB tarafından güvenli ülke olarak kabul edilmemesi nedeniyle, Türkiye'de faaliyet gösteren çok uluslu firmalar ile yerli şirketlerin yoğun ticari ilişkilerimiz olan AB ülkelerindeki paydaşlarıyla kişisel veri paylaşımı noktasında birçok sorun yaşadığı da ilgili sektör temsilcilerince ifade edilmektedir.

Ülkemizde sektörel veri yerelleştirme düzenlemelerinin oluşturulma aşaması için işleyen mevcut sürecin aksine; bu sürecin ilgili kamu kurumlarınca, yapılacak düzenlemenin tüm boyutlarıyla ve ilgili olabilecek tüm paydaşlar üzerindeki olumlu ve olumsuz etkileri hassasiyetle değerlendirilerek ve söz konusu paydaşların görüş ve çekinceleri dikkate alınarak işletilmesi elzemdir. Ancak, söz konusu düzenlemelerin genellikle, ilgili sektörel verilerin hassasiyet seviyesi ve güvenlik ihtiyaçlarının (gizlilik, bütünlük, erişilebilirlik) birbirlerinden farklı olmasına ve alınacak tedbirlerin de bu ihtiyaçlar doğrultusunda belirlenmesi gereğine rağmen, mâkul güvenlik hassasiyetlerinin en etkin şekilde karşılanabilmesine imkân veren alternatif tedbirleri değerlendirme yoluna gitmeksizin, toptancı bir yaklaşımla ilgili tüm veriler için yurtdışına veri aktarımını yasaklayacak şekilde yapıldığı görülmektedir. Bu durumun bahse konu düzenlemelerin etkilediği sektörlerde iş ortamındaki belirsizliği artırdığı, iş yapmayı güçleştirdiği, yatırım ortamını bozduğu ve ülkemiz açısından ekonomik kayıplara yol açtığı

birçok sektör profesyonelinin ortak görüşüdür. Bunun yanı sıra, veri yerelleştirme düzenlemeleri nedeniyle bulut bilişim hizmetlerinden yararlanamayan kuruluşların bilgi ve iletişim teknolojisi maliyetlerinde artışlar gözlemlenmekte, bu kuruluşlar bulut bilişimin sağlayacağı kolay e düşük maliyetli ölçeklendirme imkânından yararlanamamakta, piyasalara erişimde zorluklar yaşanmaktadır.

Diğer taraftan, ülkemizdeki kamu kurumlarının ve politika yapıcıların, ilgili sektörlerdeki sınır aşan veri transferlerinden kaynaklı mahremiyet, ekonomik çıkar veya ulusal güvenlik endişeleri ile bu tür veri transferlerinin ilgili kamu otoritelerinin görev ve sorumluluklarını etkin şekilde yerine getirebilmesi açısından aksaklık oluşturabilecek olmasından kaynaklı çekincelerinin bulunması ve bu çekinceleri azaltmaya veya ortadan kaldırmaya yönelik tedbirler alması son derece doğaldır. Bununla birlikte, hem uluslararası kuruluşların dikkat çektiği hem de ülkemiz tecrübesinin işaret ettiği üzere, sınır aşan veri transferlerini kısıtlamaya yönelik olarak alınacak tedbirlerin bir takım sosyoekonomik maliyetleri olabilmektedir. Bu nedenle, **bu nitelikteki tedbirlerden mümkün olan en yüksek faydayı sağlamak ve tedbirlerin sosyoekonomik maliyetini ve olumsuz etkilerini en aza indirmek için söz konusu tedbirlerin etraflı risk ve fayda-maliyet analizine dayalı olarak, mâkul ve orantılı biçimde kurgulanması gerekmektedir**. Böyle bir kurgunun sağlıklı şekilde oluşturulması ise;

- yukarıda bahsi geçen çekincelere temel teşkil eden tehdidin ve tehdit arz eden aktörler ile bunların motivasyonlarının tanımlanması,
- tehdit aktörlerinin elindeki araçlar ve imkanlar ile motivasyonları birlikte değerlendirilerek tehdidin gerçekleşme olasılığının ne olduğunun öngörülmesi,
- tehdidin gerçekleşmesi durumunda ortaya çıkacak sorun veya maliyet doğrultusunda riskin belirlenmesi,
- riski azaltmak üzere, riskin unsurlarını ve doğasını dikkate alarak, hedeflenen risk azaltımını sağlayabilecek en düşük maliyetli ve en etkin hukuki, idari ve/veya teknik tedbirlerin tanımlanması,
- belirlenen bu tedbirlerin maliyetinin, tedbirin hayata geçirilmesiyle sağlanacak risk azaltımıyla tutarlı ve mâkul olup olmadığının analiz edilmesi

adımlarını kapsayan bir sürecin işletilmesini gerektirir.

Yukarıda bahsi geçen analiz ve değerlendirmelerin etkin şekilde yapılabilmesi, hem ilgili düzenlemeden etkilenebilecek sektörlerin doğası ve işleyişi hem de alınacak tedbirlerin olası etki, fayda ve maliyetleri konusunda etraflı bilgi sahibi olunmasını gerektirir. Dolayısıyla, **bu tür bir risk değerlendirmesinin ve fayda-maliyet analizinin sağlıklı şekilde yapılabilmesi için bahsi geçen hususlarda bilgi, uzmanlık ve tecrübe sahibi farklı paydaşların ortak çalışması kaçınılmaz bir ihtiyaçtır. Bu nedenle, veri yerelleştirmesine yönelik tedbirlerin katılımcı ve sorgulayıcı bir müzakere sürecinde şekillendirilmesi gerekli görülmektedir.**

Sınır aşan veri transferlerine yönelik yukarıda açıklanan iki yönlü yaklaşımın Türkiye için de uygulanabilir ve faydalı olacağı değerlendirilmektedir. Aşağıdaki kısımda bu hususstaki somut politika önerileri açıklanmıştır.

5.2. Öneriler

5.2.1. Kişisel Verilerin Korunması Kanunu'nun GDPR ile Uyumlaştırılması

Her ne kadar bu raporda KVKK kapsam dışında bırakılmış olsa da, yapılan toplantılar ve konuya ilişkin yurt dışı araştırmaları sonucunda, verilerin aktarımının ticareti destekleyici bir çerçeveye dönüştürülmesi için bütüncül bir yaklaşımın sergilenerek kişisel verilerin yurt dışına aktarımının da kolaylaştırılması gerektiği görülmektedir. Özelikle kişisel verilerin sınır aşan aktarımı açısından ülkemizdeki mevcut mevzuatın öngördüğü mekanizmaların çeşitli sektörlerde ciddi sorunlar yarattığı ve bu nedenle acil düzenleme ihtiyacı olduğu göz önünde bulundurulduğunda, öncelikle KVKK'nin veri aktarımını düzenleyen dokuzuncu maddesinin GDPR ile uyumuna yönelik yasal düzenlemenin hızlıca yapılmasının, bunun akabinde de GDPR'nin geneline yönelik uyumu hedefleyen daha detaylı bir yasa çalışmasının yürütülmesinin yerinde olacağı değerlendirilmektedir.

5.2.2. Veri Yerelleştirmesine İlişkin Hükümler İçeren Mevzuatın Risk Değerlendirmesinin Yapılmasına Yönelik Yönetişim Mekanizması Oluşturulması

Dördüncü bölümde detaylandırıldığı üzere, birçok uluslararası kuruluş sınır aşan veri transferlerinin sağladığı ekonomik fayda ile ortaya çıkardığı güvenlik ve mahremiyet çekincelerini dengeleyebilecek mekanizmaların geliştirilmesi gerektiği yönünde temel ilke, politika ve düzenlemeler oluşturulması konusunda yoğun çaba sarf etmektedir. Sınır aşan veri transferlerinin küresel değer zincirlerine eklemlenme ve dijital ekonomide ortaya çıkan yeni fırsatlardan faydalanma açısından artan önemi dikkate alındığında da, bu tür mekanizmaların oluşturulmasının Türkiye'nin üretkenliğinin ve uluslararası rekabet gücünün artırılarak ekonomik gelişmesinin hızlandırılması açısından önemli bir ihtiyaç olduğu düşünülmektedir.

Sektörel boyuttaki sınır aşan veri transferlerinin bütünüyle engellenmesi veya tümüyle serbest bırakılmasının mâkul olmadığı dikkate alındığında, bu tür veri transferlerinin düzenlenmesi noktasında temelde iki yaklaşım benimsenebileceği değerlendirilmektedir;

i. Sınır aşan veri transferlerinin "varsayılan" olarak engellenmesi, ancak mevzuatla belirlenen istisnalar çerçevesinde bu tür veri transferlerine izin verilmesi.
ii. Sınır aşan veri transferlerine "varsayılan" olarak izin verilmesi, ancak mevzuatla belirlenen durumlar için bu tür veri transferlerinin kısıtlanması.

Tüm sektörlerde yaygınlaşan dijitalleşmenin sonucu olarak artan veri çeşitliliği ve bu verilerin farklı iş süreçleri ve karar alma mekanizmalarında çok çeşitli ve önceden her boyutuyla öngörülmesi kolay olmayan dinamik yöntemlerle kullanılıyor olması, veriye dayalı yenilikçilik ile bundan kaynaklı üretkenlik ve rekabet gücü artışlarının temelini oluşturmaktadır. Diğer

taraftan, etraflı risk değerlendirmesi ve fayda-maliyet analizleri yapılmaksızın, sınır aşan veri transferlerinin çeşitli riskleri beraberinde getirebileceği düşüncesine dayalı olarak, herhangi bir sektörde bu tür veri transferlerinin "varsayılan" olarak kısıtlanması durumunda, yukarıda bahsi geçen ve son derece dinamik şekilde işleyen veriye dayalı süreçlerin aksatılması ve bu faydaların ortaya çıkmasının engellemesi oldukça yüksek bir olasılıktır. Zira söz konusu kısıtlamaların ilgili sektördeki olumsuz sonuçlarının net olarak anlaşılıp bunların ortadan kaldırılmasına yönelik olarak mevzuatta istisnalar tanımlanmasına kadar geçecek sürede, ilgili sektörde yenilikçilik ve üretkenlik artışı getirebilecek birçok uygulamanın ve iş modelinin önünün kesilmesi ve bunun sonucunda ekonomik kayıpların ortaya çıkması ihtimali son derece yüksektir. Böyle bir durumun, özellikle Türkiye gibi dijitalleşmeyle ortaya çıkan veya yeniden şekillenen küresel değer zincirlerine daha güçlü şekilde eklemlenmeye çalışan bir ülke için ciddi ekonomik kayıpları ve fırsat maliyetlerini ortaya çıkarması kaçınılmazdır. Bu nedenle, yukarıda bahsi geçen ilk yaklaşımın benimsenmesinin Türkiye açısından mâkul olmadığı değerlendirilmektedir. Diğer taraftan, ilgili sektörlerdeki aktörlerin veriden faydalanması açısından doğal olarak var olan belirsizlik ve dinamizm nedeniyle, somut sorun tespitleri ile bunlara yönelik risk ve fayda-maliyet analizlerinin yapılmadığı durumlar için sınır aşan veri transferlerinin kısıtlanmaması, ancak bahse konu tespit ve analizler sağlıklı şekilde yapıldıktan sonra ve bu analizler doğrultusunda ihtiyaç olduğu belirlenirse bu tür kısıtlamaların yapılması şeklindeki yaklaşımın, sınır aşan veri transferlerine yönelik kısıtlamaların faydalarının ve maliyetlerinin dengelenebilmesi noktasında Türkiye açısından daha etkin bir yaklaşım olacağı düşünülmektedir.

Yukarıda açıklanan gerekçelerle, uluslararası kuruluşların dikkate aldığı fayda-maliyet dengeleme yaklaşımları da göz önünde bulundurularak, Türkiye için (KVKK hükümleri saklı kalmak kaydıyla) sınır aşan veri transferlerinde serbestliğin esas olması, kısıtlamaların ise etraflı risk ve fayda-maliyet analizlerine dayalı olarak yapılması gerektiği düşünülmektedir (yukarıdaki ikinci yaklaşım).

Söz konusu kısıtlamalara ilişkin düzenlemelerin ise, yukarıda açıklandığı üzere çok paydaşlı ve çok boyutlu risk değerlendirmelerine dayalı şekilde yapılması gereklidir. Bu nedenle, hem bu alandaki mevcut mevzuatın risk değerlendirmesinin yapılarak ihtiyaç tespit edilirse söz konusu mevzuata yönelik değişiklik önerilerinin oluşturulup uygulamaya konması sürecini yönlendirmek, hem de yeni hazırlanacak benzer nitelikteki mevzuat için risk değerlendirmesini yapmak üzere Sınır Aşan Veri Transferleri Mevzuatı Risk Değerlendirme Komisyonu'nun oluşturulabileceği değerlendirilmektedir. Komisyon'un yapısı, işlevleri ve yetkileri açısından;

- Çeşitli bakanlıklar, konu hakkında yetkin bilgiye sahip üniversiteler ve düzenleyici kurumların görev alanına giren hususlarda inceleme yapacak ve karar alacak olması nedeniyle, Komisyon'un başkanlığını Cumhurbaşkanı Yardımcısı'nın yapması,
- Komisyon'un yapacağı incelemelerin gerektirdiği temel uzmanlık alanlarındaki görevleri nedeniyle Ticaret Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Kişisel Verileri Koruma Kurumu, Adalet Bakanlığı ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin

Komisyon'un devamlı üyeleri olması ve Komisyon'un sekretaryasının Ticaret Bakanlığı tarafından yürütülmesi,

- İncelenecek mevzuat veya mevzuat tasarılarının tarafı olan kamu kurumları ile söz konusu mevzuat düzenlemesinden etkilenebilecek diğer kamu kurumlarının ve ilgili sektörlerin temsilcilerinin (STK'lar, firmalar vb.) Kurul toplantılarına katılmaları,
- Sınır aşan veri transferlerini kısıtlayan mevcut mevzuat hükümleri açısından, söz konusu hükümleri uygulamakla sorumlu kamu kurumlarının Ek-1'deki forma göre hazırlayacakları risk değerlendirmelerini Komisyon'a sunmaları, sunulan bu risk değerlendirmelerinin Komisyon tarafından tartışılıp değerlendirilmesi,
- Değerlendirme sonucunda ilgili mevzuatın değiştirilmesine karar verilirse, mevzuata yönelik değişiklik taslağının Komisyon'da kararlaştırılan hususlar çerçevesinde hazırlanıp ilgili sektör paydaşlarının da görüş alındıktan sonra nihai onay için tekrar Komisyon'a sunulmasına yönelik ilgili kuruma görev verilmesi,
- Komisyon'un nihai onayından geçen mevzuat değişikliği taslaklarını, kanun seviyesinde ise yasalaşma sürecini işletmek, ikincil düzenleme seviyesinde ise uygulamaya koymak üzere ilgili kurumun görevlendirilmesi,
- Sınır aşan veri transferlerini kısıtlamak üzere hazırlanan yeni mevzuat taslakları açısından, söz konusu taslağı hazırlayan kamu kurumlarının Ek-1'deki forma göre hazırlayacakları risk değerlendirmelerini Komisyon'a sunmaları, sunulan bu risk değerlendirmelerinin Komisyon tarafından tartışılıp değerlendirilmesi,
- Değerlendirme sonucunda ilgili mevzuat taslağının değiştirilmesine karar verilirse, mevzuata yönelik değişiklik taslağının Komisyon'da kararlaştırılan hususlar çerçevesinde hazırlanıp nihai onay için tekrar Komisyon'a sunulmasına yönelik ilgili kuruma görev verilmesi,
- Komisyon'un nihai onayından geçen mevzuat değişikliği taslaklarını, kanun seviyesinde ise yasalaşma sürecini işletmek, ikincil düzenleme seviyesinde ise uygulamaya koymak üzere ilgili kurumun görevlendirilmesi,
- Kamu kurumlarına, sınır aşan veri transferlerini kısıtlamaya yönelik olarak hazırlayacakları mevzuat taslakları için yukarıdaki usuller çerçevesinde Komisyon'a başvuruda bulunma ve Komisyon'un onayından geçmeyen taslaklar için mevzuatın yürürlüğe konmasına yönelik süreçleri ilerletmeme sorumluluğu getirilmesi

önerilmektedir. Bu çerçevede, Sınır Aşan Veri Transferleri Mevzuatı Risk Değerlendirme Komisyonu'nun yukarıda açıklanan yapı ve yetkilerle oluşturulmasına yönelik bir Cumhurbaşkanlığı Kararnamesi çıkarılabileceği değerlendirilmektedir.

Ek-1: Risk Değerlendirme Formu (3 sayfa)

SINIR AŞAN VERİ TRANSFERLERİ MEVZUATI RİSK DEĞERLENDİRME KOMİSYONU

EK-1 RİSK DEĞERLENDİRME FORMU

1. GENEL DEĞERLENDİRME

Talep Yapan Kurum	(S*ınır aşan veri transferi hususunda birincil ve/veya ikincil mevzuat oluşturma talebi ile Komisyon*[20]*'a başvuracak olan kamu kurumunun adı*)
Talep Tarihi	*(Formun doldurularak Komisyon'a iletileceği tarih)*
Mevzuat Talebi	*(Sınır aşan veri transferi hususunda kamu kurumunun gündeme getireceği birincil ve/veya ikincil mevzuat talebinin ne olduğuna ilişkin açıklama)*
Talep Sonucunda Etkilenen Sektörler ve Aktörler	*(Sınır aşan veri transferi hususunda talep edilen mevzuatın yürürlüğe girmesi durumunda, bu mevzuattan doğrudan veya dolaylı olarak etkilenecek sektörler ile bahse konu sektörlerdeki aktörlere ilişkin açıklama)*
Talep Sonucunda Etkilenen Sektör ve Aktörlerden Görüş Alındı mı?	*(Sınır aşan veri transferi hususunda birincil ve/veya ikincil mevzuat taslağına ilişkin mevzuattan etkilenecek olan sektör ve aktörlerin temsilcilerinden görüş alınıp alınmadığına ilişkin açıklama)*
Mevzuat Talebine İlişkin Benzer Yurtdışı Uygulamalar Var Mı? Varsa Uygulamaya İlişkin Bilgiler	*(Sınır aşan veri transferi hususunda talep edilen birincil ve/veya ikincil mevzuat doğrultusunda diğer ülkelerde benzer yaklaşımların/uygulamaların olup olmadığına ve varsa bahse konu yaklaşımlara/uygulamalara ilişkin gerekçelere vb. bilgilere ilişkin açıklama)*

[20] İşbu formda yer alan Komisyon ifadesi; "Sınır Aşan Veri Transferleri Mevzuatı Risk Değerlendirme Komisyonu" için kullanılmaktadır.

SINIR AŞAN VERİ TRANSFERLERİ MEVZUATI
RİSK DEĞERLENDİRME KOMİSYONU

2. TALEP EDİLEN MEVZUATA İLİŞKİN RİSK DEĞERLENDİRMESİ

Mevzuat Talebine Gerekçe Oluşturan Tehditler Nelerdir? *(Tehdit: İlgili tarafa/taraflara zarar/hasar verebilecek olaylar. Örneğin; hassas bilgilerin yetkisiz tarafların eline geçmesi, kritik sistemlerin çalışmasının aksatılması vb.)*	*(Sınır aşan veri transferi hususunda talep edilen birincil ve/veya ikincil mevzuatın oluşturulmasına sebep olan tehditlerin neler olduğuna/neler olabileceğine ilişkin açıklamalar.)*
Yukarıda Belirtilen Tehdit/Tehditler için Tehdit Aktörleri Nelerdir? *(Tehdit Aktörü: Tehdidi ortaya çıkarabilecek taraflar. Örneğin; yabancı istihbarat kuruluşu, rakip firma, siber saldırgan vb.)*	*(Yukarıda belirtilen tehdit/tehditlerin kim/hangi kurum, organizasyon vb. tarafından gerçekleştirilebileceğine ilişkin açıklamalar.)*
Tehdit Aktörlerinin Motivasyonları ve Bahse Konu Tehdit/Tehditleri Gerçekleştirebilmek için Sahip Oldukları Kaynaklar Nelerdir?	*(Yukarıda belirtilen tehdit aktörlerinin tehdit/tehditleri gerçekleştirmek istemelerinin altında yatan nedenler ve bu tehditleri gerçekleştirebilmek için sahip oldukları teknik, finansal, insan gücü vb. kaynaklarına ve imkânlarına ilişkin açıklamalar.)*
Tehdit Aktörlerinin Sahip Olduğu Motivasyon ve Kaynaklarla, Bahse Konu Tehdit/Tehditleri Gerçekleştirme Olasılığı Nedir?	*(Bu kısımda, tehdit/tehditler için belirlenen gerçekleşme olasılığını destekleyecek ve daha önce yaşanmış benzer olay örnekleri, sektörel ve politik gelişmeler, tehdidin gerçekleşmesini kolaylaştıracak özel durumlar ile diğer durumsal bilgilere ilişkin açıklamalar verilebilir.)* *5: Çok Yüksek (%81-%100)* *4: Yüksek (%61-%80)* *3: Orta (%41-%60) Tehdit ancak belirli durumlarda gerçekleşebilir. Benzer bölüm/süreçlerde belirli durumda gerçekleşti. Ortam gerçekleşmesi için uygun olabilir.* *2: Düşük (%21-%40)* *1: Çok Düşük (%0-%20)*

SINIR AŞAN VERİ TRANSFERLERİ MEVZUATI
RİSK DEĞERLENDİRME KOMİSYONU

<table>
<tr><td>Tehdit Aktörleri Tarafından Tehdit/Tehditlerin Gerçekleştirilmesi Durumunda Oluşacak Zararlar Nelerdir?</td><td>(Bu kısımda finansal kayıplar, ulusal/kurumsal itibar kayıpları, toplum sağlığı sorunları, asayiş sorunları, mahremiyet ihlali, ölçümlenemeyen diğer kayıplar vb. için seçilen zarar skalasına yönelik açıklama yapılmalı ve mümkünse bunlar olay örnekleriyle desteklenmelidir.)
5: Çok Yüksek)
4: Yüksek
3: Orta
2: Düşük
1: Çok Düşük</td></tr>
<tr><td>Bahse Konu Tehditlerin Oluşturduğu Riskin Değerlendirmesi

(Risk Matrisi = Tehdit/Tehditlerin Gerçekleşme Olasılığı x Gerçekleşmesi Durumunda Oluşacak Zarar)</td><td>(Gerekli görüldüğü takdirde tehdidin/tehditlerin gerçekleşmesine ilişkin açıklama)
<table><tr><td>25</td><td>20</td><td>15</td><td>10</td><td>5</td></tr><tr><td>20</td><td>16</td><td>12</td><td>8</td><td>4</td></tr><tr><td>15</td><td>12</td><td>9</td><td>6</td><td>3</td></tr><tr><td>10</td><td>8</td><td>6</td><td>4</td><td>2</td></tr><tr><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr></table>Kırmızı Bölge (15-25 puan): Kabul Edilemez Risk (Acil tedbir gereklidir.)
Sarı Bölge (7-14 puan): Dikkate Değer Risk (Mümkün olduğunca çabuk müdahale edilmelidir.)
Yeşil Bölge (1-6 puan): Kabul Edilebilir Risk (Acil tedbir gerektirmeyebilir.)</td></tr>
<tr><td>Riski Azaltabilecek Olası Hukuki, İdari ve Teknik Tedbirler Nelerdir?</td><td>(Risk değerlendirmesi sonucunda çıkan risk seviyesinin azaltılması için hangi tedbirlerin yapılabileceğine ilişkin açıklamalar. Örneğin; yurtdışına veri transferinin tümüyle yasaklanması, yedek sistemlerin yurtdışında tutulmasına izin verilirken ana sistemlerin ülke içinde bulunmasının zorunlu tutulması, yurtdışında tutulacak bilgi sistemi unsurlarına ilişkin teknik/idari standartlar koyulması vb.)</td></tr>
<tr><td>Belirlenen Tedbirler, Risk Seviyesini Ne Kadar Azaltacak ve Belirlenen Tedbirlerin Etkilerinin Tüm Paydaşlar ile Kamu Kurumu Açısından Fayda ve Maliyeti Ne Olacak?</td><td>(Risk seviyesinin azaltılması adına alınabilecek tedbirlerden etkilenen taraflar için bu tedbirlerin riski ne ölçüde azaltacağı, buna mukabil söz konusu tedbirlerin ne tür/ölçekte maliyetler ortaya çıkaracağına yönelik analizler.</td></tr>
<tr><td>Risk Değerlendirmesi Sonuçları ve Tedbirlere ilişkin Fayda-Maliyet Çerçevesinde Talebe Konu Mevzuatın Oluşturulma Nedenleri?</td><td>(Yukarıdaki tüm analizler çerçevesinde, sınır aşan veri transferi hususunda talep edilen birincil ve/veya ikincil mevzuata konu tedbirin/tedbirlerin, azaltılan risk miktarı ve yüklenilen maliyetler dikkate alındığında, neden en etkin ve kabul edilebilir çözüm olduğuna yönelik gerekçeli açıklamalar.)</td></tr>
</table>