BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

TELEKOMÜNİKASYON VERİSİ ÖRNEKLEMİNDE VERİ LOKALİZASYONU POLİTİKALARININ KARŞILAŞTIRMALI OLARAK İNCELENMESİ VE ÜLKEMİZ MEVZUATI İÇİN ÇÖZÜM ÖNERİLERİ

Fatmanur BEYTEKİN

Bilişim Uzmanlığı Tezi

Aralık 2025

Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

TELEKOMÜNİKASYON VERİSİ ÖRNEKLEMİNDE VERİ LOKALİZASYONU POLİTİKALARININ KARŞILAŞTIRMALI OLARAK İNCELENMESİ VE ÜLKEMİZ MEVZUATI İÇİN ÇÖZÜM ÖNERİLERİ

Fatmanur BEYTEKİN

Bilişim Uzmanlığı Tezi

Aralık 2025

Ankara

Fatmanur BEYTEKİN tarafından hazırlanan "TELEKOMÜNİKASYON VERİSİ ÖRNEKLEMİNDE VERİ LOKALİZASYONU POLİTİKALARININ KARŞILAŞTIRMALI OLARAK İNCELENMESİ VE ÜLKEMİZ MEVZUATI İÇİN ÇÖZÜM ÖNERİLERİ" adlı bu tezin Bilişim Uzmanlığı Tezi olarak uygun olduğunu onaylarım.

Teknik Uzman, Mustafa Tahir ALAK
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı Tezi olarak kabul edilmiştir.

Başkan : Ömer Abdullah KARAGÖZOĞLU

Üye : Mustafa ÖZSERT

Üye : Mustafa Tahir ALAK

Üye : Aysel Deniz ÇAYCI

Üye : Abdulaziz BUDAK

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Telekomünikasyon Verisi Örnekleminde Veri Lokalizasyonu Politikalarının Karşılaştırmalı Olarak İncelenmesi ve Ülkemiz Mevzuatı İçin Öneriler
Türü	Bilişim Uzmanlığı Tezi
Yazar	Fatmanur BEYTEKİN
Teslim Tarihi	2.12.2025
Anahtar Kelimeler	Kişisel Veri, Telekomünikasyon Verisi, Veri Lokalizasyonu, Veri Yerelleştirme, Mahremiyet
Tez danışmanı	Mustafa Tahir ALAK
Sayfa Adedi	v+186

Bireylerin mahremiyetinin ve kişisel verilerinin korunması, kritik altyapıların güvenliğinin sağlanması, kolluk ve istihbarat faaliyetlerinin verimli bir şekilde sürdürülmesi ve yabancı istihbarat faaliyetlerinin engellenmesi gibi sebeplerle devletler, verilerin yurt içinde muhafaza edilmesini teşvik eden veri lokalizasyonu politikalarına yönelmiştir. Katı, yumuşak, karma ve zorlaştırılmış veri aktarımı olmak üzere farklı çeşitleri olan veri lokalizasyonu politikalarının; temel hak ve hürriyetler, ekonomi, siber güvenlik ve kolluk faaliyetleri başta olmak üzere vatandaşlar ile devletler bakımından birçok önemli sonucu bulunmaktadır. Veri lokalizasyonu politikalarının gerekliliğine karar vermeden önce orantılılık ve gereklilik gibi testler uygulanmalı ve bu kurallarla hedeflenen fayda ile vatandaşların temel hak ve hürriyetleri dengelenmelidir. Bu tez çalışması ile; özellikle telekomünikasyon verisi bağlamında, kişisel veri lokalizasyonu politikalarının gerekçe ve sonuçlarının değerlendirilmesi amaçlanmaktadır. Çalışma kapsamında ülkemiz mevzuatındaki veri lokalizasyonu kuralları detaylıca incelenecek ve diğer ülke regülasyonlarına yer verilerek karşılaştırmalı olarak değerlendirilecektir. Tez çalışmasının sonuç ve öneriler kısmında ise veri lokalizasyonu kuralları açısından ülkemiz mevzuatına yönelik öneriler sunulacaktır.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	Comparative Analysis of Data Localization Policies in Telecommunication Data Sample and Suggestions for Turkish Legislation
Type	ICT Expertise Thesis
Author	Fatmanur BEYTEKİN
Submission Date	2.12.2025
Keywords	Personal Data, Telecommunication Data, Data Localisation, Data Residency, Privacy
Advisor	Mustafa Tahir ALAK
Total Page	v+186

For reasons such as protecting the privacy and personal data of individuals, ensuring the security of critical infrastructures, maintaining law enforcement and intelligence activities efficiently, and preventing foreign intelligence activities, states have turned to data localisation policies that encourage data to be kept domestically. Data localisation policies, which have different types such as hard, soft, mixed and hardened data transfer, have many important consequences for citizens and states, especially fundamental rights and freedoms, economy, cyber security and law enforcement activities. Before deciding on the necessity of data localisation policies, tests such as proportionality and necessity should be applied and the benefit targeted by these rules should be balanced with the fundamental rights and freedoms of citizens. This thesis aims to evaluate the justification and consequences of personal data localisation policies, especially in the context of telecommunication data. Within the scope of the study, the data localisation rules in the legislation of our country will be examined in detail and will be evaluated comparatively by including the regulations of other countries. In the conclusion and recommendations section of the thesis, recommendations will be presented for the legislation of our country in terms of data localisation rules.

TEŞEKKÜR

Tez çalışmam boyunca bilgi, tecrübe ve fikirlerini paylaşarak yardım ve katkılarını sunan tez danışmanım Sayın Mustafa Tahir ALAK'a, desteğini hiçbir zaman esirgemeyen Bölge Müdürüm Mustafa ÖZSERT'e, I. Hukuk Müşaviri İlkay ERDOĞAN DAŞDEMİR'e, tüm çalışma arkadaşlarıma, bu süreçte maddi ve manevi olarak her zaman yanımda olan eşim Enes Furkan BEYTEKİN, annem ve babam başta olmak üzere tüm aileme teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
EHK	5809 sayılı Elektronik Haberleşme Kanunu
GVKT	Genel Veri Koruma Tüzüğü
KEP	Kayıtlı Elektronik Posta
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
MKK	Merkezi Kayıt Kuruluşu
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü
SPK	Sermaye Piyasası Kanunu
SOME	Siber Olaylara Müdahale Ekibi
TCK	Türk Ceza Kanunu
TMK	Türk Medeni Kanunu
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VDK	Veri Depolama Kuruluşları

1. GİRİŞ

Teknolojinin büyük bir hızla ilerlemesi ve bireylerin gelişen teknolojiyi kullanma şekillerinin de geçmişe nazaran çok başka bir boyuta ulaşması, mevcut regülasyonların insanların mahremiyetinin ve kişisel verilerinin korunması konusunda yetersiz kalmasına neden olmuştur. Günümüzde bireyler gündelik aktivitelerinin her adımında aralıksız bir şekilde veri üretmekte ve bu veriler çeşitli teknolojiler aracılığıyla devamlı olarak birçok alıcıya ulaştırılmaktadır. İletişimin vazgeçilmez bir parçası olan cep telefonlarından çeşitli amaçlarla kullanılan bilgisayarlara, akıllı saatlerden çamaşır makinelerine kadar birçok cihaz tarafından işlenen veriler büyük veri yığınları oluşturmakta; bu veriler veri madenciliği ve makine öğrenmesi gibi teknolojiler aracılığıyla işlenmektedir.[1] Bu işleme faaliyetlerinin sonucunda birbiriyle alakasız görünen verilerden anlamlı ve kritik bilgiler üretilmekte; bu da bireyler hakkında davranış örüntülerinin açıkça ortaya konulmasından çevrim içi reklam hedeflemesine maruz kalmalarına kadar birçok olumsuz sonuç doğurabilmektedir.

Devletlerin, bireylerin mahremiyeti ve kişisel verilerinin korunmasının yanında; kamu düzeninin ve milli güvenliğin sağlanması ve vatandaşlara huzur ve güven ortamının sunulması gibi birçok sorumluluğu bulunmaktadır. Bu çerçevede devletler; terörizmin engellenmesi, suçların önlenmesi ve soruşturulması gibi amaçlarla kolluk ve istihbarat faaliyetleri yürütmektedir. Tüm bunlar, bireylerin mahremiyet ve kişisel verilerin korunması haklarına karşı meşru müdahale olarak tanımlanabilecek veri işleme faaliyetlerini gerektirebilmektedir.[2] Ancak gelişen teknoloji ile, mahremiyet hakkına meşru gerekçelerle müdahale edilmesi de zorlaşmıştır. Şöyle ki, suçlular; delil olarak tespit edilebilecek birtakım verileri ve bilgileri ülkeden çıkartabilmekte ve dolayısıyla kolluk kuvvetleri, yargı makamları ve ilgili kamu kurum ile kuruluşlarının milli

[1] Aylin Erdoğdu, "Bankacılık Sektöründe Kişisel Verilerin Korunması ve Müşteri İlişkileri Yönetimi" *Kişisel Verileri Koruma Dergisi* 1, sy.2 (Aralık 2019): 89.
[2] Turan Atlı, "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi" *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* 2, sy.1 (Haziran 2019): 11.

güvenliğin sağlanması ve suçların önlenmesi gibi meşru amaçlarla ihtiyaç duyacakları bilgilere erişememesine sebep olabilmektedir.[3]

Tüm bunların yanında; bazı kritik sektörlerce işlenen verilerin korunması, kişisel veri olmasından veya suçların önlenmesiyle ilgili erişilmesi gereken bir veri olup olmamasından bağımsız olarak ayrıca önem arz etmektedir. Devletler, işledikleri bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, milli güvenlik çıkarlarına veya kamu düzeninin bozulmasına yol açabilen bilişim sistemlerini barındıran kritik altyapıların korunması konusunda çalışmalar yürütmektedir.[4] Bu kritik altyapılardan biri olarak kabul edilen elektronik haberleşmeye ilişkin veriler de, başka bir deyişle telekomünikasyon verileri, bu çerçevede belirli düzenlemelere tabi tutulmaktadır.[5]

Zaman içerisinde mevcut koruma mekanizmalarının yetersiz kalmasıyla devletler yukarıdaki gerekçelerle kişisel veriler ve telekomünikasyon verileri üzerindeki kontrolün sağlanması ile ilgili ilave düzenlemeler yapmıştır. Ekonomik, siyasi ve stratejik nedenlerin de etkili olduğu bu süreçte mahremiyetin korunması, milli güvenliğin ve kamu düzeninin sağlanması gibi sebeplerle bazı veri gruplarının yurt içinde saklanması veya yurt dışına aktarımının zorlaştırılması zorunlu tutulmaya başlanmıştır.[6] Veri lokalizasyonu kuralları olarak adlandırılan bu politikalar; uygulamaya göre katı veri lokalizasyonu, yumuşak veri lokalizasyonu, karma veri lokalizasyonu ve zorlaştırılmış veri aktarımı olmak üzere farklı çeşitlerde görülebilmektedir.[7]

---

[3] Nilay Pratap Singh, *A dissertation submitted in partial fulfillment of the requirements for the Degree of Master's in Public Policy (MPP)* (Yüksek lisans tezi, National Law School of India University, 2021), 53, http://oldopac.nls.ac.in:8081/xmlui/bitstream/handle/123456789/968/MPP217.pdf?sequence=1&isAllowed=y (06.07.2024).

[4] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*, 9. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf (03.10.2024).

[5] Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, *Sektörel SOME Kurulum ve Yönetim Rehberi,* Kasım 2014, 7. https://dsy.usom.gov.tr/usom/19/02/190211090404_Sektorel%20SOME%20Rehberi.pdf (03.10.2024).

[6] Anupam Chander ve Uyên P. Lê, "Data Nationalism" *Emory Law Journal* 64, sy.3 (2015): 680.

[7] Erol Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies*, Temmuz 2021, https://www.csis.org/analysis/real-national-security-concerns-over-data-localization (06.08.2024).

Veri lokalizasyonu politikaları; vatandaşların mahremiyetinin ve kişisel verilerinin korunması, kolluk ve istihbarat faaliyetlerinin güçlendirilmesi, yabancı ülke istihbarat faaliyetlerinin engellenmesi ve yerel ekonominin geliştirilmesi gibi farklı gerekçelerle uygulamaya konulabilmektedir.[8] Literatürde bu gerekçeleri destekleyen yazarlar bulunduğu gibi, bu politikaların yukarıda sayılan amaçların karşılanmasında ölçülü ve orantılı olmadığını, bu amaçların veri lokalizasyonu politikaları ile sağlanamayacağını, aksine bu politikaların temel hak ve hürriyetler bakımından olumsuz sonuçlara sebep olacağını savunan görüşler de mevcuttur.[9] Ülkemiz mevzuatında da veri lokalizasyonu alanındaki gelişmeler son yıllarda hız kazanmasına rağmen bu konuda literatürümüzde detaylı bir çalışma yer almamaktadır.

Bu tez ile; özellikle telekomünikasyon verileri bağlamında kişisel veri lokalizasyonu politikalarının çeşitli ülke düzenlemeleri ile karşılaştırılarak incelenmesi ve ülkemiz mevzuatı için öneriler sunulması amaçlanmaktadır. Tezin ilk bölümünde mahremiyet kavramına yer verilecek ve mahremiyet hakkı ile kişisel verilerin korunması hakkının tarihsel gelişimi detaylı biçimde incelenecektir. Bu kapsamda, hukuki korumaların genişlemesi ve uluslararası insan hakları düzenlemelerinin mahremiyetin şekillenmesindeki rolü ele alınacaktır. Ardından, gelişen teknolojilerin mahremiyet üzerindeki etkileri ve bu teknolojilerin bireylerin mahremiyetini koruma ihtiyacını nasıl artırdığı değerlendirilecek; mahremiyetin korunmasının bireysel özgürlükler, demokratik toplum düzeni ve milli güvenlik bakımından taşıdığı önem üzerinde durulacaktır. Sonrasında ise, kişisel verilerin korunması alanında uluslararası düzenlemeler ile ve Türkiye'deki mevzuatın ortaya koyduğu standart ve yükümlülükler kapsamlı bir şekilde aktarılacaktır.

Tezin ikinci bölümünde; kişisel veri ve telekomünikasyon verisi kavramı detaylı biçimde incelenecek, kişisel verinin unsurları ile telekomünikasyon verisinin niteliği ve kapsamı değerlendirilecektir. Bu çerçevede, kişisel verilerin korunmasına ilişkin temel kavramlar tanımlanacak ve veri lokalizasyon süreçlerinin değerlendirilmesine ilişkin kavramsal bir altyapı oluşturulacaktır. Ayrıca, telekomünikasyon alanında

[8] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*
[9] Chander ve Lê, "Data Nationalism": 718.

işlenen verilerin diğer veri kategorilerinden farklılaşan yönleri ele alınarak sonraki bölümlerde yapılacak değerlendirmelere zemin hazırlanacaktır.

Üçüncü bölümde ise telekomünikasyon verileri ile kişisel verilerin işlenmesine ilişkin temel ilkeler ele alınacak ve işleme faaliyetleri sırasında dayanılması gereken hukuki sebepler değerlendirilecektir. Bu kapsamda, genel ve özel nitelikli kişisel verilerin işlenme şartları incelenecek; veri aktarımı, veri güvenliği ve telekomünikasyon verilerinin kritik altyapı niteliği çerçevesinde taşıdığı önem de ortaya konulacaktır.

Dördüncü bölümde, ülkemiz mevzuatı çerçevesinde kişisel verilerin ve telekomünikasyon verilerinin korunmasına yönelik düzenlenmiş koruma mekanizmalarına yer verilecektir. Bu bağlamda, genel veri koruma yükümlülükleri ile telekomünikasyon sektörüne özgü güvenlik, bilgilendirme, erişim sınırlandırma ve aktarım düzenlemeleri incelenecek; veri sorumlularının ve hizmet sağlayıcıların yükümlülükleri aktarılacaktır. Böylece, kişisel veri güvenliğinin sağlanmasına ilişkin hukuki altyapının telekomünikasyon alanındaki yansımaları bütüncül bir bakış açısıyla ortaya konulacaktır.

Tezin beşinci bölümünde veri lokalizasyonu kavramı ve türleri incelenecektir. Bu çerçevede, veri lokalizasyonu politikalarının dayandığı hukuki, ekonomik ve güvenlik temelli gerekçeler detaylı olarak tartışılacak; söz konusu politikaların mahremiyet, veri güvenliği ve milli güvenlik açısından doğurduğu etkiler değerlendirilecektir. Ardından, Türkiye'deki düzenlemeler ile çeşitli ülkelerde uygulanan veri lokalizasyonu yaklaşımları karşılaştırmalı olarak ele alınarak küresel eğilimlere ilişkin bütüncül bir perspektif sunulacaktır.

Tezin son bölümünde ise yapılan çalışma özetlenecek, ulaşılan bulgular ışığında genel değerlendirmeler sunulacak ve veri lokalizasyonu politikalarının düzenlenmesine yönelik olarak ülkemiz mevzuatına ilişkin çözüm önerileri ortaya konulacaktır. Bu kapsamda, daha etkin, dengeli ve sürdürülebilir bir veri lokalizasyonu yapısının tesisine katkı sağlayabilecek mevzuat geliştirme önerileri sunulacaktır.

2. MAHREMİYETİN KORUNMASI

2.1.Mahremiyet Kavramı

Mahremiyet, Türk Dil Kurumunun internet sayfasında yer alan Güncel Türkçe Sözlük'e göre "gizlilik" [1] olarak tanımlanmaktadır.

Başka bir deyişle mahremiyet, gizli tutulması gereken veya kişiye özel olan hususlar olarak adlandırılabilir. Ancak hukuki değerlendirmeler kapsamında bu tanımlama yetersiz kalacağından daha detaylı bir incelemeye ihtiyaç bulunmaktadır. Kaliforniya Üniversitesi Mahremiyet ve Bilgi Güvenliği Yönlendirme Komitesi Raporu'na göre mahremiyet; özerklik ve bilgi mahremiyeti kavramlarının iç içe geçmesiyle oluşmuş bir terimdir.[1] Buna göre özerklik, insanların gözetlenmeksizin veya gözetlenme endişesi hissetmeksizin eylemlerini yürütebilmesi; bilgi mahremiyeti ise, insanlar hakkındaki bilgilerin uygun bir şekilde korunmasıdır.[2] Bir diğer tanıma göre ise mahremiyet, insanların özerkliklerinin ve onurlarının korunması için gerekli olan en temel haktır.[3] Başka bir deyişle mahremiyet; bir insanın özünü ve kim olduğunun temelini oluşturur.

Özellikle hukuk dünyasında "mahremiyet" kavramı zaman içerisinde oldukça tartışılmış, bu süreçte boyut değiştirmiş ve adeta yeni bir anlam kazanmıştır. Yukarıdaki bilgilerden özetle anlaşılması gereken husus, bir insanın mahremiyetinin hukuken koruma altında tutulması gerektiğidir. Hukuk; mahremiyeti, bir insanın mahremi veya özelini diğer insanların müdahalesinden koruyarak ve burada efektif bir sınır belirleyerek sağlar.[4] Gelişen teknoloji, internet kullanımının yaygınlaşması, globalleşme ve insanların yaşam şeklinin değişmesi gibi hususlar buradaki sınırın konumlandırılması konusunda tartışmalara yol açmıştır. Örneğin; mahremiyet hakkı uzun bir süre boyunca bir evin içerisine izinsiz girilememesi gibi insan hayatına yapılan fiziksel müdahaleler ve genellikle somut kavramlar üzerinden sınırlı olarak

---

[1] Türk Dil Kurumu, "Mahremiyet" *Güncel Türkçe Sözlük*, https://sozluk.gov.tr, (03.07.2024).
[1] The University of California, *Privacy and Information Security Initiative Steering Committee Report to the President*, Ocak 2013, 9. https://www.ucop.edu/privacy-initiative/uc-privacy-and-information-security-steering-committee-final-report.pdf, (03.07.2024).
[2] The University of California, Privacy and Information Security…, 9.
[3] Privacy International, *What is Privacy?*, Ekim 2017. https://privacyinternational.org/explainer/56/what-privacy (03.07.2024).
[4] Samuel D. Warren ve Louis Brandeis, "The Right to Privacy", *Harvard Law Review* 4, sy. 5 (Aralık 1890): 196.

değerlendirilmiştir. Ancak zamanla bu anlayış değişmiş ve mahremiyetin sağlanması kişiye ait bilgilerin korunması gibi soyut kavramları da içerir hale gelmiştir.[5] Aslında burada değişen husus, tanımın kendisi değil; zaman içerisinde tanımın kapsamının genişlemesidir. Lessig, mahremiyete yönelik müdahaleleri, izleme ve arama olmak üzere iki ayrı boyutta incelemiştir.[6] Detaylandırmak gerekirse; bir insanın hayatı, izlenebilen ve aranabilen olmak üzere iki ayrı boyuta sahiptir. İzlenebilen kısmı, bireylerin başkaları tarafından rahatlıkla görülebilen ve fark edilebilen günlük davranışlarından oluşur. Örneğin, bir insanın sokakta yürümesi izlenebilen hayatın izlenebilen kısmına ilişkin bir davranıştır. Aranabilen kısmı ise kayıt altına alınabilen ve tabiri caizse arkada delil bırakılan davranışlardır. Bir günlük yazmak, evde yer alan eşyalar veya bir mobil uygulama aracılığıyla ses kaydı göndermek bu kısma dahil edilebilecek örneklerdendir. Bir davranışın yalnızca izlenebilen olması, kolaylıkla anlaşılacaktır ki, mahremiyet açısından daha az risk oluşturur. Yukarıdaki örnek ile devam edilecek olursa, bir bireyin sokakta yürüdüğü; ancak bu yürüme davranışını görenlerin bulunması ve bunu gören kişilerin sorgulanması ile kayıt altına alınabilir. Dolayısıyla tek başına izlenebilen davranışlar bir insanın mahremiyetinin ihlali hususunda daha az tehlikelidir. Ne var ki, teknoloji bu iki ayrım arasındaki dengeyi bozmuş ve hatta yok etmiştir. Teknolojik gelişmeler, neredeyse her davranışı izlenebilir kılmakla kalmamış, "aranabilir" de kılmıştır.[7] Bu durum insanların her davranışının başkaları tarafından bilinebilmesine yol açmış ve dolayısıyla bireylerin diğer insanların müdahalesi ya da hiç değilse farkındalığı olmaksızın yaşaması epeyce zorlaşmıştır. Bunun iki farklı sonucunun olduğu söylenebilecektir. İlk olarak, eskiden mahrem olarak nitelendirilmeyen birçok eylem artık bu kapsamda değerlendirildiğinden hukukun koruması gereken davranış ve durumların şaşırtıcı düzeyde arttığı ve hukukun temas etmesi gereken alanın genişlediği rahatlıkla görülebilmektedir. İkinci sonucunun ise genişleyen bu mahremiyeti korumanın öneminin ve zorluğunun da aynı şekilde artması olduğu söylenebilecektir.

[5] Avrupa İnsan Hakları Mahkemesi Kararı, 25 Nisan 1978 tarihli, 5856/72 başvuru nolu Tyrer/Birleşik Krallık kararı.
[6] Lawrence Lessig, *CODE Version 2.0* (New York, Basic Books, 2006), 202.
[7] Lessig, *CODE Version 2.0*, 205.

Mahremiyetin genişlemesi, ihlal edilebilir alanın ve dolayısıyla korunması gereken alanın da büyümesi anlamına gelecektir.

2.2.Mahremiyeti Korumanın Tarihçesi

2.2.1. Hukuki korumaların genişlemesi

Bilindiği üzere hukuk, ilk çağlardan beri iki temel görevi üstlenmektedir: Adaletin sağlanması ve düzenin korunması. Bu görevlerini yerine getirirken hukuk, temelde insanı korumayı amaçlamaktadır. Yukarıda da bahsedildiği gibi, hukukun bu iki temel misyonu sabit kalsa da zaman içerisinde koruma ve müdahale alanları oldukça genişlemiştir. İnsanı korumak ilk zamanlarda fiziksel güvenliğinin sağlanması ve mülkiyetinin korunması ile mümkünken; ekonominin gelişmesi, ilerleyen teknoloji ve küreselleşme gibi sebeplerle bu korumalar yetersiz kalmaya başlamıştır.[8] Örnek vermek gerekirse, hukukun temel görevi insanın yaşam hakkını sağlamak, fiziksel bütünlüğünü korumak ve arazisi ile hayvanlarını korumak ile sınırlıyken; bu koruma alanları gün geçtikçe genişlemiştir. Bu gelişmeleri kişinin itibarı ile aile hayatının da korunmaya başlanması takip etmiş ve nihayet, insanların gündelik hayatın zorlukları karşısında yalnız kalmaya haklarının olduğu ve mahremiyetlerinin korunması gerektiği ifade edilmiştir.[9] Bu gereksinimlerin ortaya çıkmasıyla doğal olarak hukukun tanımış olduğu temel insan hak ve özgürlükleri genişlemiş ve bunların korunması adına hazırlanan uluslararası ve yerel düzenlemeler gittikçe artmıştır.

2.2.2. Mahremiyet hakkı (Özel ve aile hayatına saygı hakkı)

İnsanların yalnız kalma hakkının olduğunun ve mahremiyetlerinin korunması gerektiğinin kabulü hukuk dünyasında yeni tanımlara yol açmıştır. Bu hak, yukarıda da bahsedildiği gibi 1890 yılında Warren ve Brandeis'in "Mahremiyet hakkı" (Right to Privacy) adlı makalesiyle ilk kez isimlendirilmiştir. Bu hakkın uluslararası alanda ilk kez tanınması ise 1948 yılında Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi (Beyanname) ile olmuştur. Beyanname'nin 12'nci maddesi;

[8] Warren ve Brandeis, "The Right to Privacy": 194.
[9] Warren ve Brandeis, "The Right to Privacy": 195.

"*Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır."* hükmünü haizdir.

Maddeden açıkça görülebileceği gibi; insanların özel hayatları, aile hayatları, meskenleri ve yazışmaları insanların mahremi olarak kabul edilmiştir. Buradaki yazışma hususu, aşağıda daha detaylı incelenmek üzere, iletişim anlamıyla geniş yorumlanmalıdır. Bu Beyanname ile insanların mahremiyet hakkı ilk kez uluslararası anlamda tanınmakta ve devletlerin bireylerin mahremiyetlerini kanun ile korumasının gerektiği öngörülmektedir. Beyanname ayrıca insanların mahremiyetine keyfi bir şekilde müdahale edilmesini de açıkça yasaklamaktadır.

1950 yılında imzalanan ve 1953 yılında yürürlüğe giren ve Avrupa İnsan Hakları Sözleşmesi (AİHS), mahremiyet hakkını tanıyan ikinci uluslararası düzenlemedir. AİHS'in 8'inci maddesinde;

"*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir." hükmü yer almaktadır.

Başka bir deyişle, AİHS ile her bir bireyin başkalarının müdahale etmesinin yasak olduğu özel alanlarının olduğu ve bu alanların korunması gerektiği kesin bir dille düzenlenmiştir.[10] Gizli haberleşme hakkı ve kişisel verilerin korunmasını isteme hakkı da AİHS'in 8'inci maddesi altında tanınmış olup bu tezin konusu bakımından önem arz ettiklerinden aşağıda ayrıca incelenecektir.

Her ne kadar bağlayıcı olmasa da mahremiyet alanında uluslararası bir mevzuat oluşturmanın ilk çalışması olması sebebiyle Ekonomik İşbirliği ve Kalkınma Örgütünün (OECD) 1980 yılında yayımlamış olduğu Özel Yaşamın Korunması ve

[10] Lessig, *CODE Version 2.0*, 207.

Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri önem arz etmektedir.[11] Bu Rehber daha çok kişisel verilerin korunmasını isteme hakkı ile ilgili olduğu için bu başlık altında incelenmeyecektir.

Son olarak, bu başlık altında Avrupa Birliği Temel Haklar Bildirgesi'ne (Charter of Fundamental Rights of the European Union) de değinilmesi yerinde olacaktır. 2000 yılında yürürlüğe giren Avrupa Birliği Temel Haklar Bildirgesi, 7'nci maddesiyle herkesin özel hayatına, aile hayatına, konutuna ve iletişimine saygı hakkı olduğunu düzenlemektedir. AİHS'ten farklı olarak Avrupa Birliği Temel Haklar Bildirgesi 8'inci maddesiyle kişisel verilerin korunması hakkını ayrı bir hak olarak düzenlemiştir.

Mahremiyet hakkının tanınmasıyla insanların özel hayatları koruma altına alınmış, ancak özel hayat kavramı üzerindeki tartışmalar sürmeye devam etmiştir. Daha önce de açıklandığı gibi, 1950'li yıllara kadar mahremiyet kavramının odağını insan hayatına ilişkin fiziksel müdahaleler oluşturmaktaydı. Bilgi mahremiyeti ise herhangi bir korumaya sahip değildi. Avrupa İnsan Hakları Mahkemesi (AİHM) 1978 yılında Tryer kararıyla, gelişen teknoloji ve endüstri gibi unsurlarla tamamen değişen yaşam koşullarının da etkisiyle bilgi mahremiyetinin de mahremiyet hakkı kapsamında değerlendirilmesi gerektiğine hükmetmiştir.[12] Yine bu karar ile AİHS'in "yaşayan bir enstrüman" (living instrument) olduğu ve dünyadaki gelişmeler doğrultusunda gelişen bir yorumlama metoduyla değerlendirilmesi gerektiğini belirtti.

Bu noktada mahremiyet hakkı, haberleşmenin gizliliği hakkı ve kişisel verilerin korunmasını isteme hakkı bakımından son derece önemli olması sebebiyle "bilgi" kavramına da değinilmesi gerekmektedir. Hukuk dünyasında meydana gelen bu gelişmelerle bilgilerin de korunması gerektiği anlaşılmıştır. Ancak hukuk, burada bahsedilen bu üç temel hak bağlamında bilgiyi korumamakta, aslında bilginin bireyin "müdahale edilemez kişiliği" ile olan ilişkisini korumaktadır.[13] Başka bir deyişle bilgi,

---

[11] Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Eylül 1980, https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1729547405&id=id&accname=guest&checksum=3A723BC9D5AE35CECCD8825DD8AECD63, (01.07.2024).

[12] Avrupa İnsan Hakları Mahkemesi Kararı, 25 Nisan 1978 tarihli, 5856/72 başvuru nolu Tyrer/Birleşik Krallık kararı.

[13] Warren ve Brandeis, "The Right to Privacy": 195.

bir insanın mahremiyetiyle ilişkili olduğu zaman bu üç temel hakkın koruma alanına girmektedir. Ne var ki, Purtova'nın da ifadesiyle, günümüz dünyasında her şey ya bilgidir ya da en azından bilgi içerir.[14] Aşağıda daha detaylı inceleneceği gibi, neredeyse her bilgi bireylerin kişiliği ile ilişkilendirilebileceği için artık bu ayrımın bir işlevinin kalmadığı, dolayısıyla neredeyse her türlü bilginin korunması gerektiği söylenebilecektir.

2.2.3. Haberleşmenin gizliliği hakkı

Haberleşme veya iletişim, insanların gündelik hayatta kendilerini ifade etme yöntemlerini ve etkileşim kurmalarını ifade eder. Başka bir ifadeyle iletişim, karşılıklı bilgi paylaşımı olarak da açıklanabilir.

Haberleşmenin gizliliği hakkını incelemeden önce bu hakka temel oluşturması sebebiyle ifade özgürlüğü üzerinde durmak gerekmektedir. İfade özgürlüğü, AİHS'in 10'uncu maddesiyle düzenlenmektedir. Söz konusu madde; "*Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü kapsar.*" şeklindedir. Madde metninden de anlaşılacağı gibi, ifade özgürlüğü; bireylerin birbirleriyle haberleşmesini ve görüş alıp vermesini de kapsar. Diğer bir deyişle, bu hak ile insanların herhangi bir baskı altında kalmadan birbirleriyle bilgi alışverişi yapabilmeleri sağlanmaktadır. Bu kapsamda ifade özgürlüğü ile insanların birbiriyle kuracağı iletişimin de korunduğu rahatlıkla söylenebilir. İletişimin mahremiyeti ise yine AİHS'in 8'inci maddesi ile koruma altındadır.

Yukarıda da belirtildiği gibi, AİHS, 8'inci maddesiyle insanların yazışmalarının da özel hayat kapsamına girdiğine, dolayısıyla mahremiyet hakkı ile korunduğuna hükmetmektedir. Bu koruma Avrupa Birliği Temel Haklar Bildirgesi'nin yine mahremiyet hakkını düzenleyen 7'nci maddesindeki "iletişim" ifadesiyle sağlanmaktadır. Daha önce de açıklandığı üzere, AİHM, AİHS'in "yaşayan bir enstrüman" olduğunu ve güncel yaşam koşullarıyla yorumlanması gerektiğini belirtmektedir. Buradaki "yazışma" ifadesi AİHM'in Barbulescu (2017) kararından da

[14] Nadezhda Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" *Law, Innovation and Technology* 10, sy.1 (Mart 2018): 33.

görülebileceği gibi, aynı yöntem ve anlayışla geniş yorumlanmakta ve her türlü iletişimi içerecek şekilde değerlendirilmektedir.[15] Daha açık bir ifadeyle, buradaki iletişim ifadesi insanların birbiriyle yaptığı sözlü konuşmalardan anlık mesajlaşma uygulamalarıyla gerçekleştirdiği yazışmalara kadar her türlü etkileşimi kapsamaktadır.

2.2.4. Kişisel verilerin korunmasını isteme hakkı

Yukarıda da açıklandığı gibi, mahremiyet hakkı bireylerin özel hayatı ve "ihlal edilemez kişiliği" ile ilgili bilgiler için koruma sağlamaktadır. Ancak bu hak, bireylerle ilgili olmasına rağmen özel hayat kapsamına girmeyen veya bir bireyle ilgili özel olarak nitelendirilemeyen bilgileri kapsamamaktadır.[16] Bununla bağlantılı olarak AİHM de Rotaru/Romanya (2000) kararıyla kişisel verilerin özel hayat kapsamında değerlendirilebileceğine, ancak yalnızca bilgilerin sistematik toplanma ve saklanma şartının sağlanması gerektiğine hükmetmiştir.[17] Kokott ve Sobotta'ya göre bir bilgi özel olarak nitelendirilmese dahi, tanımlanabilir bir gerçek kişiyle ilişkilendirilebiliyorsa yine korunmayı hak eder.[18] Bu düşünceyle, mahremiyet hakkı yıllar içinde birtakım bilgilerin korunması hususunda yetersiz kalmış ve bu noktada kişisel verilerin korunmasını isteme hakkı devreye girmiştir. Kişisel verilerin korunması mevzuatına aşağıda ayrıntılarıyla değinileceğinden burada detaylı inceleme yapılmayacaktır.

Elbette ki bu üç temel hak da insanlar ve mahremiyetleri açısından sınırsız bir koruma sağlamamaktadır. İlgili sözleşme ve mevzuat maddelerinden de görülebileceği gibi belli şartlar dahilinde bu haklara müdahale söz konusu olabilmektedir. Bu husus aşağıda detaylıca incelenecektir.

2.3.Gelişen Teknoloji ve Mahremiyete Etkisi

2.3.1. Veri teknolojileri

Mahremiyetin korunması adına birçok yasal düzenleme ve bunlarla uyumlu olarak teknik ve idari korumalar geliştirilmiştir. Ancak; günümüz teknolojisi ve insanların bu

[15] Avrupa İnsan Hakları Mahkemesi Kararı, 5 Eylül 2017 tarihli, 61496/08 başvuru nolu Bărbulescu/Romanya kararı.
[16] Juliane Kokott ve Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" *International Data Privacy Law* 3, sy.4 (Eylül 2013): 226.
[17] Avrupa İnsan Hakları Mahkemesi Kararı, 4 Mayıs 2000 tarihli, 28341/95 başvuru nolu Rotaru/Romanya kararı.
[18] Kokott ve Sobotta, "The distinction between privacy…": 224.

teknolojiyi kullanma şekilleri, mahremiyetin korunmasını oldukça zorlaştırmış, hatta neredeyse imkânsız hale getirmiştir. Zuboff'un da ifadesiyle; günümüz dünyası kâr amacıyla davranışları değiştirmeyi ve metalaştırmayı hedefleyen, ödüller ve cezalar üreten yeni bir küresel veri toplama ve analiz mimarisinden oluşmaktadır. Bu durum aşağıda bir kısmı açıklanan teknolojiler aracılığıyla oluşturulmaktadır.[19]

2.3.1.1. Büyük veri (Big data)

Şeker'in (2013) ifadesiyle veri, *"tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan, ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgi"* olarak ifade edilebilir.[20] Günümüzde birçok sektör veri teknolojileri üzerine odaklanmış, veri ekonomisi ve verinin değeri tahmin edilemez bir şekilde büyümüştür. Bu çerçevede veri, sıklıkla "yeni petrol" olarak adlandırılmaktadır.[21] Ancak verinin defalarca yeniden kullanılabilmesi, paylaşılabilmesi, kopyalanabilmesi ve en önemlisi de asla tükenmemesi gerekçeleriyle petrolden çok daha değerli olduğu söylenebilir.

Büyük veri birçok farklı kaynaktan toplanan geniş veri yığınlarının geleneksel saklama, yönetme ve işleme yöntemlerinin ötesinde bir şekilde toplanması olarak tanımlanabilir.[22] Diğer bir deyişle; kullanılan farklı sosyal medya hesapları, kredi kartı kullanımları, arama motoru araştırmaları, eğitim bilgileri, ailevi bilgiler, sağlık bilgileri gibi sayısız türde bilginin sayısız kaynaktan elde edilmesi ve bu heterojen verilerden anlamlı bilgiler üretilmesi amacıyla verilerin işlenmesi olarak ifade edilebilir. Büyük veri; verileri toplayanlar, verileri üretenler ve verileri kullananlar olmak üzere farklı paydaşlardan oluşur.[23] Bu teknoloji özellikle ekonomik ve yenilikçi gelişmeler açısından oldukça önemli avantajlar sağlasa da mahremiyet ve bilgi güvenliği bakımından büyük problemleri de beraberinde getirmektedir. Örneğin, bireyler ile ilgili birçok farklı kaynaktan birçok verinin toplanması; mağduriyetlerin

---

[19] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Londra: İngiltere, Profile Books, 2019), 23.
[20] Şadi Evren Şeker, *İş Zekası ve Veri Madenciliği* (İstanbul: Cinius, 2013), 37.
[21] Dennis D. Hirsch, "The Glass House Effect: Big Data, The New Oil, and The Power of Analogy" *Maine Law Review 66*, sy. 2 (Haziran 2014): 374.
[22] Korcan Doğan ve Sacit Arslantekin, "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum" *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi* 56, sy. 1 (Ocak 2016): 21.
[23] Ali Özcan, "Büyük Veri: Fırsatlar ve Tehditler" *TRT Akademi* 6, sy. 11 (Ocak 2021): 14.

yaşanmasına sebep olabilecek önemli bilgilerin açığa çıkmasına zemin hazırlayabilecektir.

2.3.1.2. Veri madenciliği (Data mining)

Birçok farklı kaynaktan bu derecede büyük miktardaki veri elbette ki yalnızca depolama amacıyla toplanmamaktadır. Veriye böylesi bir ekonomik değer kazandıran unsur, karmaşık yığınlardan anlamlı ve değerli bilgiler üretilebilmesi özelliğidir. Tam da bu noktada veri madenciliği (data mining) kavramı devreye girmektedir. Büyük miktarda heterojen veri yığınından çözümleme yapılarak anlamlı bilgiler üretilmesi yöntemi veri madenciliği olarak adlandırılır.[24] Veri madenciliği tabiatıyla basit sorgulamalar aracılığıyla gerçekleştirilen bir yöntem olmaktan çok uzaktır. Aksine, birçok farklı örüntü ve model kullanılarak ortaya çıkarılması güç bilgilerin keşfedilmesini sağlar.[25] Her ne kadar insanlara imkânsız gibi gelse de, birbirleriyle hiçbir ilgisi olmayan iki veri grubundan oldukça değerli ve anlamlı bilgiler üretilebilmekte ve bu bilgiler reklamcılık, sağlık ve telekomünikasyon gibi çeşitli sektörlerde farklı amaçlarla kullanılabilmektedir. Basit bir örnekle anlatılacak olursa, konum verisi ile ilgisiz görünen türde birkaç verinin birleştirilmesiyle etnik köken bilgisine ulaşılabilir. Bu teknolojinin gittikçe gelişmesiyle elde edilen bilgilerin doğruluk oranı da gittikçe artmaktadır.[26] Bu durum da teknolojinin mahremiyet açısından oluşturduğu riskleri gözler önüne sermektedir.

2.3.1.3. Makine öğrenmesi (Machine learning)

Aslında veri madenciliği gibi teknolojiler yeni geliştirilmiş yöntemler değildir. 1960'lardan beri uygulanan bu yöntemler, beraberinde gelişen teknolojiler ile daha doğru sonuçlara daha kolay bir şekilde ulaşma kabiliyeti kazanmıştır. Büyük veri ve veri madenciliği gibi yöntemlerin insanlar tarafından değil de yapay zekâ tarafından gerçekleştirilmesi, sürece oldukça büyük bir hız kazandırmakta; dahası daha doğru sonuçlara ulaşılmasını sağlamaktadır. Makine öğrenmesi (machine learning) olarak adlandırılan bu yöntem, bir problemin doğrudan o problemin verilerine göre bilgisayar

---

[24] Eda Coşlu, "Veri Madenciliği" *Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri*, (Antalya: Akdeniz Üniversitesi, Ocak 2013): 616.
[25] Selim Tüzüntürk, "Veri Madenciliği ve İstatistik" *Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 29, sy. 1 (2010): 66.
[26] Coşlu, "Veri Madenciliği": 617.

tarafından modellenmesini sağlayan algoritma olarak tanımlanabilir.[27] Başka bir deyişle makine öğrenmesi, ulaşılmak istenen sonuca bir insanın açık talimat ve yönergelerine ihtiyaç duyulmadan algoritmanın modellemesiyle ulaşılmasıdır. Bu yöntem, duygu analizinden[28] diyabet hastalığının sınıflandırılmasına[29] akademik başarının tahmin edilmesinden[30] ormancılığa[31] kadar çok geniş bir sektör ve alan spektrumunda kullanılmaktadır. Dolayısıyla makine öğrenmesinin bireylerin sağlık bilgilerinden akademik başarılarına kadar her konuda oldukça başarılı tahminler yapılmasını sağlayan bir teknoloji olduğu kolaylıkla söylenebilir.

2.3.1.4. Derin öğrenme (Deep learning)

Makine öğrenmesinin insanların açık talimatlarına gerek kalmaksızın algoritma aracılığıyla problemlerin sonuçlandırılmasını sağlayan bir yöntem olduğundan yukarıda bahsedilmişti. Derin öğrenme, makine öğrenmesinin bir kolu olarak değerlendirilse de bu yöntemin daha gelişmiş hali olarak nitelendirilmesi yanlış olmaz. Zira derin öğrenme, makine öğrenmesinin bir alt dalı olarak, algoritmaların önceden programlanmış komutlarla değil, alana özgü veriler kullanılarak otomatik bir şekilde eğitilmesini sağlayan öğrenme yöntemlerini ifade eder.[32] Derin öğrenmenin geliştirilmesinin arkasında yatan amaç, insan beyninin öğrenme ve bir sonuca ulaşma metodunun makineye adapte edilmesidir.[33] Özetle, derin öğrenmeyi makine öğrenmesindeki insan etkileşimi ihtiyacını azaltan bir çözüm algoritması olarak düşünmek mümkündür. Derin öğrenme, yapılandırılmamış verilerin anlamlandırılması konusunda daha iyi çözümler sunmaktadır.[34] Yeni tedavi

---

[27] Muhammet Atalay ve Enes Çelik, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları" *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 9, s.22 (Aralık 2017): 161.

[28] Oğuz Kaynar vd., "Makine Öğrenmesi Yöntemleri ile Duygu Analizi" *International Artificial Intelligence and Data Processing Symposium (IDAP'16)*, (Malatya: İnönü Üniversitesi, Eylül, 2016): 235.

[29] Bilge Özlüer Başer vd., "Makine Öğrenmesi Teknikleriyle Diyabet Hastalığının Sınıflandırılması" *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 25, sy.1 (2021): 113.

[30] Murat Gök, "Makine Öğrenmesi Yöntemleri ile Akademik Başarının Tahmin Edilmesi" *Gazi Üniversitesi Fen Bilimleri Dergisi* 5, sy. 3 (2017): 140.

[31] Remzi Eker vd., "Ormancılıkta Makine Öğrenmesi Kullanımı" *Türkiye Ormancılık Dergisi* 24, sy.2 (Haziran 2023): 152.

[32] Dilek Küçük ve Fazlı Can, "Hukuki Metinlerin Otomatik İşlenmesinde Yapay Zeka Teknolojilerinin Kullanımı" *Bilişim Hukuku Dergisi 6,* sy.1 (Haziran 2024): 4.

[33] Ferdi Doğan ve İbrahim Türkoğlu, "Derin Öğrenme Modelleri ve Uygulama Alanlarına İlişkin Bir Derleme" *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi* 10, s.2 (Haziran 2019): 411.

[34] Küçük ve Can: 4.

yöntemlerinin geliştirilmesi ve yapay zekâ teknolojileri gibi alanlarda oldukça avantajlı olanaklar sunsa da, mahremiyetin ihlali noktasında ciddi düzeyde risk oluşturduğundan tüm bu veri teknolojilerinin sınırlarının belirlenmesi hususunda hukukçulara büyük görevler düşmektedir.

2.3.1.5. Bulut bilişim (Cloud computing)

Bulut bilişim, kolaylıkla atanan ve yönetilebilen kaynakların ortak ve her an kullanılabildiği sanal bir bilgi deposu olarak tanımlanabilir.[35] Günümüzde birçok farklı amaçla kullanılan bulut teknolojisi ile birden fazla kullanıcı her türlü bilgi ve belgeyi sanal bir ortamda saklayabilmekte ve kullanabilmektedir. Bulut bilişim, özellikle ortak çalışma ihtiyacı bulunan alanlarda oldukça kullanışlı bir teknoloji olsa da gizlilik, bütünlük, ulaşılabilirlik ve erişilebilirlik gibi konularda birtakım mahremiyet endişelerine sebep olmaktadır.[36] Bunun yanında verilerin uluslararası aktarımına ilişkin kurallar ve veri yerelleştirme düzenlemeleri, bulut bilişimin kullanımını oldukça zorlaştırmaktadır.

2.3.1.6. Nesnelerin interneti (Internet of things)

Türkçeye "Nesnelerin İnterneti" olarak çevrilen "Internet of Things", çağımızın en hızlı gelişen teknolojilerinden birisidir. Nesnelerin interneti, sayısız nesne ve cihazın internete bağlanabilmesi ve bu sayede birbirleriyle veri ve bilgi alışverişinde bulunabilmesi durumunu anlatmak için kullanılır.[37] Başka bir deyişle, nesnelerin interneti, nesnelerin birbirine bağlanabilmesini ifade eder. Akıllı saatler ve bağlantılı araçlardan beyaz eşya ve tartılara kadar her nesne artık internete bağlanabilmektedir. Bu sayede cihazlar birbirleriyle veri akışı sağlayabilmekte ve entegre olabilmektedir. Örneğin; bir akıllı saat aracılığıyla günlük harcanan kalori miktarı bilgisi ve bir akıllı tartıdan da haftalık kilo kaybı bilgisi cep telefonunda birleştirilerek analiz edilebilir. Nesnelerin interneti sayesinde büyük veri ve veri analitiği gibi teknolojiler tahmin

---

[35] Cemal Elitaş ve Serkan Özdemir, "Bulut Bilişim ve Muhasebede Kullanımı" *Muhasebe Bilim Dünyası Dergisi* 16, s.2 (2014): 95.

[36] Z. Xiao ve Y. Xiao, "Security and Privacy in Cloud Computing" *IEEE Communications Surveys & Tutorials* 15, sy. 2 (2013): 851.

[37] United Nations Conference on Trade and Development, *Data protection regulations and international data flows: Implications for trade and development*, 2016, 88. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (03.10.2024).

edilemeyecek düzeyde ilerlemiştir.[38] Sayısız nesne ve cihazdan elde edilen bilgilerin niteliği ile niceliği ve bu bilgilerin kullanılması sonucunda oluşacak mahremiyet riskleri de hukuk dünyasını endişelendirmektedir.

2.3.2. Teknolojinin kullanımı

1960'lı yıllara kadar bir insan ile ilgili oluşabilecek mahremiyet riskleri oldukça kısıtlıydı. Yukarıda da bahsedildiği gibi, bireyler hakkında bilgi edinebilmek için fiziksel takip ile komşuların ve/veya yakınların bilgisine başvurulması gibi yöntemler gerekmekteydi. Ancak bu gibi yöntemlerin tümünün kullanılması halinde bile elde edilebilecek bilgi sınırlıydı ve bu bilgilerin analitik bir şekilde incelenip bunlardan anlamlı başka bilgiler çıkarma imkânı da kısıtlıydı.

Görülebileceği gibi veri teknolojileri, hem toplanan bilgilerin çeşitliliği hem de farklı veri yığınları içerisinden kritik ve anlamlı bilgiler çıkarılması bakımından oldukça elverişli yöntemler sunmaktadır. Bu teknolojiler sayesinde nereden geldiği bile belli olmayan birçok farklı türde bilgi bir arada tutulmakta ve analiz edilmektedir. Bu yöntemlerle kişilerin ortaya çıkarma niyetinin olmadığı ve paylaşmadığı bilgilerin de öğrenilmesi pekâlâ mümkündür.

Tüm bu veri teknolojilerinin yanında yıllar içerisinde insanların teknolojiyi kullanım şekilleri de değişmiştir. İnsanlar; mobil uygulamaları kullanarak, bir arama motorunda arama yaparak ve hatta yalnızca internete bağlanabilen bir cihazı yanında taşıyarak dahi neredeyse her hareketiyle veri üretmekte, üretilen bu veriler yukarıda bahsedilen teknolojiler sayesinde devamlı olarak anlamlı ve değerli bilgilere dönüştürülmektedir. Eskiden yalnızca günlük yazılarak aranabilir hale gelen bilgiler, şu anda yalnızca adım atılmasıyla dahi bu konuma gelebilmektedir. Sonuç olarak veri teknolojilerinin yanında teknolojinin günümüzdeki kullanım şeklinin de mahremiyet açısından risk oluşturduğu kolaylıkla söylenebilecektir.

2.4.Mahremiyeti Korumak

2.4.1. Mahremiyetin korunmasının önemi

Tüm bu teknolojiler ve teknolojilerin kullanım şekilleri beraberinde birçok yeni kazanç kapısı sağlamakta ve birçok yeni iş kolu oluşturmaktadır. Örneğin; bağlantılı

[38] United Nations Conference on Trade and Development, *Data protection regulations and* …, 90.

araç verilerinin analiziyle trafik kazalarını neredeyse ortadan kaldırabilecek yöntemler geliştirilebilir.[39] Bir aracın sürüş esnasında yolda karşılaştığı bir çukurun bilgisi konum verisiyle birleştirilerek kendiliğinden Karayolları Genel Müdürlüğü veya ilgili belediye kapsamında kurulacak bir sisteme aktarılabilir ve bu şekilde yollarda büyük bir tehlike oluşturan çukurlara hızlıca müdahale edilebilir.[40] Ayrıca verilerin birleştirilmesi ve analiziyle enerji tasarrufu çalışmaları çok başka bir seviyeye getirilebilir ve de yeni iş alanları üretilerek istihdam sağlanabilir.

Bu durum bireyler için birçok avantaj sağladığı kadar, temel hak ve hürriyetler açısından da birçok riski beraberinde getirmektedir. Günümüzde verilerin sayısız anonim tarafça öğrenilmesi ve işlenebilmesi riski bulunmaktadır.[41] Bu da elbette ki veri sahiplerinin bilgileri üzerindeki kontrol kabiliyetlerini kaybetmelerine yol açmaktadır. Bunun yanında yukarıda da değinildiği gibi tüm bu teknolojiler sayesinde insanların paylaşmak veya açıklamak istemediği bilgiler de kolaylıkla ortaya çıkabilmekte ve davranış örüntüleri kolaylıkla ortaya çıkarılabilmektedir. Bu durum ciddi düzeyde mahremiyet riski barındırmakla beraber, insanların özgürce karar verme yeteneklerinin dahi ortadan kaybolmasına sebep olabilmektedir.[42] İnsanların tüm davranış örüntülerinin açıkça anlaşılabilmesi, doğal olarak bu kişilerin zafiyetlerinin ve iradelerinin etkilenebileceği noktaların tespitini de kolaylaştırmaktadır. Elde edilen bu bilgilerle bir insanın bir sözleşmeyi imzalaması için dahi o insanın zafiyetlerini kullanan ve o insana özgü yöntemlerle geliştirilmiş sömürücü sözleşmeler (exploative contracts) geliştirilebilmekte ve bu yöntemlerle insanların kendileri dahi farkında olmadan ve özgürce imzaladıklarını düşünmelerine rağmen aslında sakatlanmış iradeyle bu tür sözleşmeleri imzalaması sağlanabilmektedir.[43]

---

[39] Araz Taeihagh ve Hazel Si Min Lim, "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks" *Transport Reviews* 39, s.1 (2018): 110.
[40] Kun Xie vd., "Use of Real-World Connected Vehicle Data in Identifying High-Risk Locations Based on a New Surrogate Safety Measure" *Accident Analysis and Prevention* 125 (2019): 316.
[41] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), *Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale*, Şubat 2019, 8. https://www.datenschutzzentrum.de/uploads/projekte/ULD_Location-Service-Tracking.pdf (02.10.2024).
[42] Philipp Hacker, "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things" *International Data Privacy Law* 7, sy.4 (Eylül 2017): 274.
[43] Hacker, "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things": 276.

Bu noktada Cambridge Analytica skandalına değinilmesi de oldukça yerinde olacaktır. Cambridge Analytica, veri teknolojilerini kullanarak Brexit ve ABD başkanlık seçimi gibi birçok seçim süreci için siyasi kampanya danışmanlığı hizmeti veren bir şirketti.[44] Guardian gazetesinde yayımlanmış haber ile, Cambridge Analytica şirketinin yaklaşık 87 milyon Facebook kullanıcısının verilerini topladığı ve bu verileri insanların seçim sürecinde iradelerini etkilemek için kullandığı ortaya çıktı.[45] Birçok farklı kategoride verinin kullanıldığı skandalda, ağırlıklı olarak kullanıcıların psikolojik verilerinin tercih edildiği tespit edildi.[46] Yaklaşık 87 milyon Facebook kullanıcısının yalnızca yaklaşık 270 bininin bilgilerini paylaşmak için rıza gösterdiği, kullanıcıların oldukça büyük bir kısmının bilgilerinin ise veri güvenliği açığı nedeniyle ele geçirilebildiği ortaya çıktı.[47] Seçmenlerin konumları, psikolojik durumları ve genel tercihleri gibi bilgilerin toplandığı skandalda, toplanan bu bilgiler veri teknolojileri aracılığıyla anlaşmalı olunan adaya oy verilmesi yönünde bireylerin iradelerinin yönlendirilmesi amacıyla kullanıldı. Bu durum kişisel verilerin korunması başta olmak üzere mahremiyetin sağlanması ve sürdürülmesinin önemini açık bir şekilde ortaya koymaktadır. Sonuç olarak, mahremiyetin ihlali yalnızca insanların öğrenilmesini istemediği bilgilerin ortaya çıkması gibi ilk akla gelen sonuçları oluşturmamakta, daha da önemlisi, insanların karar verme mekanizmalarının ihlal edilmesine kadar oldukça kritik problemlere sebebiyet verebilmektedir. Bunun gibi birçok örnek, günümüzde mahremiyetin korunmasının önemini gözler önüne sermektedir.

2.4.2. Milli güvenliğin sağlanması

Yukarıda bahsedilenlerden özetle; mahremiyet, gizli iletişim ve kişisel verilerin korunmasının bireylerin en temel haklarından olduğu ve devletlerin bu hakların korunmasını sağlamakla yükümlü olduğu söylenebilir. Ancak, devletlerin tek

---

[44] Ikhlaq ur Rehman, "Facebook-Cambridge Analytica data harvesting: What you need to know" *Library Philosophy and Practice (e-journal)*, 2497, (2019): 5.
[45] Carole Cadwalladr ve Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" *The Guardian*, 17 Mart 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, (27.06.2024).
[46] Cecilia Kang ve Sheera Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users" *The New York Times*, 4 Nisan 2018, https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html , (27.06.2024).
[47] Kang ve Frenkel, "Facebook Says Cambridge Analytica…".

yükümlülüğü elbette ki bu hakları sağlamak ve korumak değildir. AİHS'in 1'inci maddesiyle devletlerin kendi yetki alanları içinde bulunan herkesin AİHS'te yer alan hak ve özgürlüklerden faydalanmasını sağlama yükümlülüğü düzenlenmektedir. Örneğin, AİHS'in 2'nci maddesinde yaşam hakkı ve 5'inci maddesinde özgürlük ve güvenlik hakkı yer almaktadır. Bazı durumlarda bu hakların korunması, milli güvenliğin sağlanması veya kamu düzeninin korunması gibi sebeplerle mahremiyet hakkına müdahale edilebilecektir. Örneğin, 5271 sayılı Ceza Muhakemesi Kanunu'nun 135'inci maddesiyle iletişimin tespiti, dinlenmesi ve kayda alınması hususu düzenlenmektedir. Söz konusu maddenin birinci fıkrası "*Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir.*" şeklinde olup, aynı maddenin 8'inci fıkrasında ise dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümlerin uygulanabileceği suçlar belirtilmiştir. Örneğin, kasten insan öldürme veya işkence suçları dolayısıyla yapılan bir soruşturmada, kuvvetli şüphenin bulunması ve başka bir şekilde delil elde etme imkanının bulunmaması durumunda hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı kararıyla şüphelinin iletişimi dinlenebilecek ve kayda alınabilecektir. Bu durum şüphesiz mahremiyet hakkına bir müdahaledir. Ancak, aşağıda daha detaylı incelemek üzere, mahremiyet hakkının sınırsız olmadığı ve belirli şartlar dahilinde bu hakka müdahale edilmesinin zorunlu olduğu durumların meydana gelebileceği söylenebilecektir.

Daha önce de belirtildiği gibi özel ve aile hayatına saygı hakkı, başka bir deyişle mahremiyet hakkı, AİHS'in 8'inci maddesiyle düzenlenmektedir. Bu maddenin ikinci fıkrasında *"2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."* ifadelerine yer verilmiştir. Bu

doğrultuda mahremiyet hakkının sınırsız olmadığı; hukuka uygun olması, demokratik bir toplumda gerekli olması ve meşru bir amaca sahip olması şartlarının tümünün sağlanmasıyla bu hakka bir kamu makamı tarafından müdahale edilebileceği söylenebilecektir.

Ancak gelişen teknoloji, mahremiyet hakkının korunması açısından oluşturduğu risklerin yanında; mahremiyet hakkına meşru gerekçelerle müdahale edilmesini de oldukça zorlaştırmıştır. Örneğin; haberleşme aracılığıyla kullanılan anlık mesajlaşma uygulamaları uçtan uca şifreleme yöntemi kullanmaya başlamış ve bu durum haberleşmeyi daha güvenli hale getirmiştir.[48] Aynı şekilde hem şirketler hem de bireyler verilerini dünyanın birçok yerinde güvenli buldukları veri merkezlerinde depolayabilmeye başlamış ve bu noktada internet ile teknolojinin getirdiği imkanlar sayesinde bilgiler daha güvenli bir şekilde muhafaza edilebilmeye başlamıştır.[49] Ne var ki bu durum, suçların önlenmesi ve milli güvenliğin sağlanması açısından dünya genelinde çeşitli problemlere yol açmıştır. Kolluk kuvvetleri, yargı makamları ve ilgili kamu kurum ile kuruluşları milli güvenliğin sağlanması ve suçların önlenmesi gibi meşru amaçlar için ihtiyaç duyulan bilgilere erişememeye başlamıştır.[50] Her ne kadar devletlerin mahremiyet hakkına müdahalesi sınırsız olmasa da yukarıda açıklanan şartların sağlanmasıyla ve kamu düzeninin sağlanması ve suçların önlenmesi gibi meşru amaçlar dahilinde devletlerin birtakım bilgilere erişme çabası oldukça doğaldır. Teknolojinin bu duruma engel oluşturacak şekilde sunduğu imkânlar bakımından ise devletler, çeşitli çözüm yöntemlerine yönelmiştir. Burada önemli olan hak ve özgürlükler ile meşru menfaatlerin adil bir şekilde dengelenmesi ve mahremiyet hakkına yapılacak müdahalelerin doğru bir şekilde gerekçelendirilebilmesidir.[51] Bu bölüme ilişkin detaylı açıklamalara tezin ilerleyen kısımlarında yer verilecektir.

---

[48] Digital Europe, *Encryption: finding the balance between privacy, security and lawful data access*, 16 Mart 2020. https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/, (21.10.2024).
[49] Chander ve Lê, "Data Nationalism": 721.
[50] Office of the Inspector General U.S. Department of Justice, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*, Mart 2018. https://oig.justice.gov/reports/2018/o1803.pdf, (06.10.2024).
[51] Chris Reed, *Internet Law* (London: Cambridge University Press, 2012), 122.

2.5.Kişisel Verilerin Korunması Mevzuatı

Günümüz şartlarıyla karşılanması daha da zorlaşan mahremiyeti koruma gereksinimini sağlamak adına birçok mevzuat düzenlenmiş ve bununla birlikte birçok da koruma mekanizması geliştirilmiştir. Bu tez kapsamında kişisel verilerin korunması ve telekomünikasyon verisi bağlamında veri lokalizasyonu politikaları inceleneceğinden, kişisel verilerin korunması mevzuatının detaylıca incelenmesi büyük bir önem arz etmektedir. Aşağıda kişisel verilerin korunması alanında öncelikle uluslararası düzenlemelere yer verilecek, sonrasında ise ülkemiz mevzuatı incelenecektir.

2.5.1. Uluslararası düzenlemeler

2.5.1.1. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

1948 yılında yayımlanan Beyanname'nin 12'nci maddesiyle mahremiyet hakkı ilk kez uluslararası alanda tanınmıştır. Yukarıda bu düzenleme incelenmiş olduğundan ilave açıklama yapılmayacaktır.

2.5.1.2. Avrupa İnsan Hakları Sözleşmesi

1950 yılında imzalanan ve 1953 yılında yürürlüğe giren AİHS, 8'inci maddesiyle, mahremiyet hakkını tanıyan ikinci uluslararası düzenlemedir. Yukarıda da açıklandığı gibi; AİHM, yıllar içinde kişisel verilerin de bu hak kapsamında korunması gerektiğine hükmetmiş ve kararlarını da bu doğrultuda almaya başlamıştır.

2.5.1.3. Ekonomik İşbirliği ve Kalkınma Örgütü, Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri

OECD'nin 1980 yılında yayımlamış olduğu Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri (Rehber İlkeler), kişisel verilerin korunması alanında uluslararası bir mevzuat oluşturma çabasının ilk ürünü olması sebebiyle büyük önem arz etmektedir. Bu Rehber İlkeleri, ülkeler için bağlayıcı olmamakla birlikte rehber niteliği taşımaktadır. Rehber İlkeler ile veri sorumlusu, kişisel veri ve sınırlar arası kişisel veri transferi ifadeleri tanımlanmış; veri minimizasyonu, veri kalitesi, belirli amaçla sınırlılık, kullanımın sınırlandırılması, veri güvenliğinin sağlanması, işleme faaliyetinin şeffaflığı ve hesap verilebilirlik gibi ilkeler düzenlenmiştir. Sonrasında oluşturulan Avrupa Birliği veri koruma

düzenlemelerine temel oluşturması sebebiyle bu Rehber İlkeleri, veri koruma hukuku açısından bir referans noktası olarak değerlendirilebilir.

2.5.1.4. 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Avrupa Konseyi önderliğinde 28 Ocak 1981 yılında imzaya sunulan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, kişisel verilerin korunması konusunda bağlayıcı ilk uluslararası sözleşme olarak tarihe geçmiştir. 28 Ocak 1981 yılında sözleşmeyi imzalayan Türkiye Cumhuriyeti, ilk imzacı devletlerden birisi olmuştur.[52] Sözleşme, 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanarak iç hukuka dahil edilmiştir. Bu Sözleşme ile; uyruğu ve ikamet ettiği ülke fark etmeksizin her ülkedeki vatandaşın otomatik yollarla gerçekleştirilen kişisel veri işleme faaliyetlerine karşı hak ve özgürlüklerinin korunması amaçlanmaktadır.

2.5.1.5. Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri

14 Aralık 1990 yılında yayımlanan Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri ile kişisel verilerin korunması alanında uluslararası alanda asgari koşulların belirlenmesi ve her devletin tam bağımsızlık prensibiyle görevlerini uygulayacak denetleyici otorite kurmasının sağlanması amaçlanmaktadır.

2.5.1.6. 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol, 08 Kasım 2001 tarihinde 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne ek olarak hazırlanmıştır. Türkiye Cumhuriyeti'nin 08 Kasım 2001 tarihinde imzaladığı ve 05 Mayıs 2016 tarihli

[52] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*, 3. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/3a7934b6-406e-4911-a94d-795293aa0e3d.pdf, (20.10.2024).

ve 29703 sayılı Resmî Gazete'de yayımlanarak iç hukuka dahil edilen Protokol ile taraf devletlerin her biri, kişisel verilerin korunması alanında tam bağımsızlık prensibiyle görevlerini uygulayacak denetleyici otorite kurmayı taahhüt etmiştir. Ayrıca bu protokol ile kişisel verilere ilişkin yeterli korumayı sağlamayan ülkelere kişisel veri transferi yasaklanmıştır.

2.5.1.7. 108+ Sözleşmesi

108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (108 sayılı Sözleşme) üzerinden çok zaman geçmesi ve bu Sözleşme'nin gelişen teknoloji karşısında ihtiyaçları karşılayamaz hale gelmesi üzerine 18 Mayıs 2018 tarihinde 108+ Sözleşmesi kabul edilmiştir. Bu sözleşme ile 108 sayılı Sözleşme'ye nazaran kişisel verilerin korunmasına ilişkin daha etkin bir koruma mekanizması öngörülmüş ve özel nitelikli kişisel verilerin kapsamı genişletilmiştir.

2.5.2. Avrupa Birliği mevzuatı

2.5.2.1. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi

Avrupa Birliği mahremiyet ve veri koruma hukukunun temeli olarak değerlendirilebilecek olan 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi (Direktif), 13 Aralık 1995 yılında yürürlüğe girmiş ve Avrupa Birliği üyesi olan tüm devletlerin bu Direktif'te yer alan ilgili hükümleri 24 Ekim 1998 tarihine kadar kendi ulusal mevzuatında yürürlüğe koymaları gerekliliğini düzenlemiştir. Direktif'in temel amacının Avrupa Birliği genelinde kişisel verilerin korunması başta olmak üzere mahremiyet hakkının korunmasını sağlamak, Avrupa Birliği genelinde kişisel verilerin serbest dolaşımını sağlamak ve kişisel verilerin korunmasına yönelik düzenlemelerin Avrupa Birliği genelinde birbiriyle uyumlu olmasını sağlamak olduğu söylenebilir. Bu çerçevede Avrupa Birliği ülkeleri kendi iç mevzuatlarını bu Direktif doğrultusunda oluşturmuştur. 6698 sayılı Kişisel Verilerin Korunması Kanunu da bu Direktif esas alınarak düzenlenmiştir.

Direktif'in 29'uncu maddesiyle kişisel verilerin işlenmesine dair bireylerin korunması hakkında danışma statüsüne sahip ve bağımsız olarak hareket edecek bir çalışma grubu kurulması öngörülmüştür. Madde 29 Çalışma Grubu (Article 29 Working Party) olarak adlandırılan bu çalışma grubunun görevleri ise Direktif'in 30'uncu maddesiyle belirlenmiştir. Örnek vermek gerekirse, kişisel verilerin korunmasına ilişkin tavsiyeler ve rehberler yayımlamak ve belirlenen konularda raporlar hazırlamak Çalışma Grubu'nun görevlerindendir. Direktifin 2016/679 sayılı Genel Veri Koruma Tüzüğü ile yürürlükten kaldırılmasıyla Çalışma Grubu'nun yerini Avrupa Veri Koruma Kurulu (European Data Protection Board) almıştır.

2.5.2.2. 97/66/EC sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Direktif

97/66/EC sayılı Direktif, telekomünikasyon alanında kişisel verilerin ve mahremiyetin korunmasına yönelik temel Avrupa Birliği düzenlemelerinden biridir. Direktif, abonelerin kişisel verilerinin gizliliğinin sağlanmasını ve telekomünikasyon hizmetleri sırasında verilerin korunmasını amaçlamaktadır. Bu düzenleme, telekomünikasyon sektörü için özel kurallar ve veri işleme sınırlamaları getirmiştir ve 2002/58/AT sayılı Direktif ile güncellenerek telekomünikasyon ve elektronik iletişim alanındaki gelişmelere uyum sağlamıştır.

2.5.2.3. 2002/58/EC sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Direktif

2002/58/AT Direktifi, elektronik iletişim hizmetlerinde kişisel verilerin korunmasını düzenleyen özel bir Avrupa Birliği direktifidir. Direktif, telekomünikasyon ve internet servis sağlayıcıları tarafından işlenen kişisel verilerin gizliliğini güvence altına almayı, çerezler ve diğer takip teknolojilerini düzenlemeyi ve kullanıcı rızasına dayalı veri işleme esaslarını belirlemeyi amaçlar. Böylece 97/66/EC sayılı Direktif'in kapsamını genişleterek güncel teknolojik gelişmelere uyum sağlamıştır.

2.5.2.4. Avrupa Birliği Temel Haklar Bildirgesi

7 Aralık 2000 tarihinde imzalanan Avrupa Birliği Temel Haklar Bildirgesi ile Avrupa Birliği bünyesinde temel hak ve özgürlüklerin bir araya getirilmesi amaçlanmıştır. Bu bildirgenin 7'nci maddesindeki "*Herkes, özel ve aile yaşamına, konutuna ve*

haberleşmesine saygı gösterilmesini isteme hakkına sahiptir." hükmüyle, AİHS'in 8'inci maddesi ile düzenlenen özel ve aile hayatına saygı hakkı tanınmıştır. Bildirgenin 8'inci maddesindeki;

"*1. Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir.*

2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir." hükmüyle kişisel verilerin korunması hakkı düzenlenmiştir. AİHS'den farklı olarak Avrupa Birliği Temel Haklar Bildirgesi'nin 8'inci maddesiyle kişisel verilerin korunması ayrı bir hak olarak düzenlenmiştir. Ayrıca, kişisel verilerin korunmasına ilişkin kuralların denetiminin bağımsız bir makam tarafından yapılması gerekliliğinin de temel hak düzenlemesinin içerisinde yer alması, bu hakkın etkili bir şekilde korunabilmesine verilen önemi yansıtmaktadır.

2.5.2.5. 2016/679 sayılı Genel Veri Koruma Tüzüğü

Gelişen teknoloji ile kişisel verilerin korunması alanında Direktif'in ve bu çerçevede Avrupa Birliği üyesi ülkelerin geliştirmiş olduğu ulusal düzenlemelerin yetersiz kalması sebebiyle Avrupa Birliği içerisinde yeni bir düzenleme ihtiyacı hasıl olmuş ve Genel Veri Koruma Tüzüğü (GVKT), 24 Mayıs 2016 tarihinde, 25 Mayıs 2018'de yürürlüğe girecek şekilde kabul edilmiştir. GVKT ile kişisel veri tanımının genişletilmesi, yeni hakların tanımlanması ve mevcut hakların geliştirilmesi ile yeni koruma mekanizmalarının düzenlenmesi gibi birçok yenilik getirilmiştir.

GVKT, 1'inci maddesinde belirtildiği üzere gerçek kişilerin kişisel verilerinin korunmasını ve Avrupa Birliği içerisinde serbestçe dolaşımının sağlanmasını amaçlar. 3'üncü maddesinde ise GVKT'nin bölgesel kapsamı düzenlenmiştir. Buna göre bir kişisel veri işleme faaliyeti; Avrupa Birliği içerisindeki bir veri sorumlusu veya veri işleyenin faaliyetleri bağlamında ise, işleme faaliyetinin nerede gerçekleştiğine bakılmaksızın GVKT'ye tabi olacaktır. Ayrıca bir kişisel veri işleme faaliyeti; Avrupa Birliği içerisindeki kişilere mal veya hizmet sunulması veya davranışlarının izlenmesi

ile ilgili ise, veri sorumlusu veya veri işleyen Avrupa Birliği içerisinde olmasa dahi bu veri işlemenin GVKT'ye tabi olacağı düzenlenmiştir. Bu düzenlemeden GVKT'nin etkisinin yalnızca Avrupa Birliği ile sınırlı olmadığı ve AB vatandaşlarının verilerini işleyen tüm veri sorumlularının bu düzenlemeye tabi hale geldiği kolaylıkla anlaşılmaktadır. Yalnızca bu durum dahi GVKT'nin ne derece öneme sahip olduğunu gözler önüne sermektedir. Ayrıca, Kişisel Verileri Koruma Kurulunun da verdiği kararlarda GVKT'ye atıf yapması, bu düzenlemenin ülkemiz mevzuatı için de önemli olduğunu göstermektedir.[53]

2.5.2.6. 2016/680 sayılı Direktif

GVKT'nin 2'nci maddesiyle bazı işleme faaliyetleri GVKT'nin kapsamı dışında tutulmuştur. Bunlardan birisi de GVKT'nin 2'nci maddesinin (d) fıkrasıyla düzenlenen, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi amacıyla yetkili makamlar tarafından kişisel verilerin işlenmesidir. Bu fıkrada sayılanlardan birisi amaçlanarak gerçekleştirilen işleme faaliyetlerinde GVKT değil, Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ya da Cezaların İnfazı Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı ile ilgili, 2008/977/JHA Sayılı Konsey Çerçeve Kararı Yerine Geçen 27 Nisan 2016 Tarihli (EU) 2016/680 Sayılı Avrupa Parlamentosu ve Konsey Direktifi gündeme gelecektir.

2.5.3. Yerel mevzuat

2.5.3.1. Türkiye Cumhuriyeti Anayasası

Türkiye Cumhuriyeti Anayasası'nın (Anayasa) 20'nci maddesiyle özel hayatın gizliliği düzenlenmektedir. 07 Mayıs 2010 tarihli ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun'un 2'nci maddesiyle Anayasa'nın 20'nci maddesine yeni bir fıkra eklenmiş ve kişisel verilerin korunması hususu ülkemizde anayasal güvence altına alınmıştır. Bu maddede;

[53] Kişisel Verileri Koruma Kurulu Kararı, 03/08/2023 tarihli ve 2023/1310 sayılı "Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi" konulu karar.

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." ifadelerine yer verilmiştir. Bu düzenleme çerçevesinde kişisel verilerin korunmasını isteme hakkının ülkemizde anayasal bir insan hakkı olarak düzenlendiği söylenebilecektir.

2.5.3.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu

Ülkemizde kişisel verilerin korunması ile ilgili temel düzenleme 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur (KVKK). KVKK'nin 1'inci maddesi ile Kanunun amacı; *"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 düzenlemek*" olarak ifade edilmiştir. KVKK'nin 2'nci maddesi uyarınca ise kişisel verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında bu Kanunun uygulanacağı düzenlenmektedir.

KVKK'nin 19'uncu maddesi ile aynı Kanun ile verilen görevleri yerine getirmek üzere idari ve mali özerkliğe sahip Kişisel Verileri Koruma Kurumu kurulmuş ve bu Kurumun karar organı Kişisel Verileri Koruma Kurulu olarak belirlenmiştir. Kişisel Verileri Koruma Kurulu; kararları, ilke kararları, rehberleri ve çeşitli yayınları ile kişisel veri koruma mevzuatını geliştirmeye devam etmektedir.

Son olarak, KVKK'nin 28'inci maddesiyle KVKK'nin uygulama alanı bulmadığı kişisel veri işleme faaliyetleri düzenlenmiştir. Buna göre;

"...a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi,

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi…"

hallerinde KVKK uygulama alanı bulmaz.

2.5.3.3. 5237 sayılı Türk Ceza Kanunu

26 Ağustos 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun (TCK) 135'inci ve 140'ıncı maddeleri arasında kişisel verilerin hukuka aykırı olarak işlenmesiyle ilgili suçlar düzenlenmiş ve bu fiiller ağır yaptırımlara bağlanmıştır. Örneğin; TCK'nin 135'inci maddesi ile, hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği ve kişisel verilerin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda ise verilecek cezanın yarı oranında artırılacağı hüküm altına alınmıştır.

Bunun yanında TCK'nin 136'ncı maddesiyle kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi suçu; 137'nci maddesinde, 135 ve 136'ncı maddede tanımlanan suçların nitelikli halleri ve 138'inci maddesinde verileri yok etmeme suçu düzenlenmiştir. 139'uncu maddesiyle ise; kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulmasının şikâyete bağlı olduğu düzenlenmiştir. Başka bir deyişle; 135, 136 ve 138'inci maddeler ile düzenlenen kişisel verilerin korunmasına yönelik suçların işlendiğinin öğrenilmesi halinde, Cumhuriyet Başsavcılığınca şikâyet aranmaksızın re'sen soruşturma

başlatılacaktır. Son olarak, 140'ıncı madde ile, bu suçların tüzel kişilerce işlenmesi halinde bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmektedir.

2.5.3.4. 4721 sayılı Türk Medeni Kanunu

22 Kasım 2001 tarihli ve 4721 sayılı Türk Medeni Kanunu'nun (TMK) 24'üncü maddesi;

"*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.*

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır." hükmünü amirdir. Kişisel verilerin korunması hakkına gerçekleştirilecek bir müdahale de kişilik hakkının zedelenmesi olarak kabul edilecektir.[54] Dolayısıyla kişisel verilerin hukuka aykırı işlenmesi durumunda ilgili kişilerin korunma taleplerinin TMK nezdinde de yer bulduğu söylenebilir.

2.5.3.5. Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

10 Temmuz 2024 tarihli ve 32598 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, KVKK'nin 9'uncu ve 22'nci maddeleri uyarınca ve KVKK'nin yurt dışına veri aktarılmasını düzenleyen 9'uncu maddesinin uygulanmasına ilişkin usul ve esasların belirlenmesi amacıyla hazırlanmıştır. Bu Yönetmelik tezin ilerleyen kısımlarında tartışılacağından bu bölümde detaylıca incelenmeyecektir.

2.5.3.6. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

28 Ekim 2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan ve 01 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, KVKK'nin 7'nci ve 22'nci maddeleri uyarınca hazırlanmıştır. Bu Yönetmelik ile tamamen veya kısmen otomatik olan ya da herhangi

[54] Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, (Beta, 2016), 147.

bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların belirlenmesi amaçlanmaktadır. Yönetmeliğin 5'inci maddesiyle kişisel veri saklama ve imha politikası hazırlama yükümlülüğü düzenlenmiş, 6'ncı maddesiyle de bu politikanın kapsamı belirlenmiştir. Devamında ise kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine yönelik ilkeler ve süreler açıklanmıştır.

2.5.3.7. Veri Sorumluları Sicili Hakkında Yönetmelik

Veri Sorumluları Sicili Hakkında Yönetmelik, 30 Aralık 2017 tarihli ve 30286 sayılı Resmî Gazete'de yayımlanmış ve 01 Ocak 2018 tarihinde yürürlüğe girmiştir. KVKK'nin 16'ncı ve 22'nci maddeleri uyarınca hazırlanan Yönetmelik, kamuya açık olarak tutulacak olan Veri Sorumluları Sicilinin oluşturulması, idaresi ile Veri Sorumluları Siciline yapılması öngörülen kayıtlara ilişkin usul ve esasları belirlemek ve uygulanmasını sağlamak amacıyla düzenlenmiştir.

2.5.3.8. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik

4 Aralık 2020 tarihli ve 31324 sayılı Resmî Gazete'de yayımlanan ve yayımı tarihinden itibaren 6 ay sonra yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik, Bilgi Teknolojileri ve İletişim Kurumu tarafından özel hayatın gizliliği ile kişi temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirlemek amacıyla hazırlanmıştır.

2.5.3.9. Kişisel Sağlık Verileri Hakkında Yönetmelik

21 Haziran 2019 tarihli ve 30808 sayılı Resmî Gazete'de yayımlanan ve yayımı tarihinde yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik, Sağlık Bakanlığı tarafından Sağlık Bakanlığının merkez ve taşra teşkilatı birimleri ile bunlara bağlı olarak faaliyet göstermekte olan sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları tarafından yürütülen süreç ve uygulamalarda uyulacak usul ve esasları düzenlemek amacıyla hazırlanmıştır.

2.5.3.10. Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ

10 Mart 2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan ve yayımı tarihinde yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, veri sorumlusuna başvuru ve işlemin ayrıca bir maliyet gerektirmesi hâlinde alınacak ücret ile ilgili usul ve esasları belirlemek üzere hazırlanmıştır.

2.5.3.11. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ

10 Mart 2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan ve aynı tarihte yürürlüğe giren Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, KVKK'nin 10'uncu maddesi uyarınca veri sorumluları veya yetkilendirdiği kişilerce yerine getirilmesi gereken aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasları belirlemek amacıyla düzenlenmiştir.

3. KİŞİSEL VERİLERİN KORUNMASI VE TELEKOMÜNİKASYON VERİSİ

3.1. Kişisel Veri Kavramı

KVKK'nin 3'üncü maddesi ile kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Benzer şekilde GVKT'nin 4'üncü maddesinin birinci fıkrasıyla kişisel veri, kimliği belirlenmiş veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi olarak ifade edilmiştir. Görülebileceği gibi her iki mevzuatta da kişisel veri, oldukça geniş tanımlanmıştır. Purtova'nın da ifadesiyle kişisel verinin bu kadar geniş tanımlanması ve yorumlanması, çok yakın gelecekte her şeyin kişisel veri olarak veya en azından kişisel veri içerdiğinin kabul edilmesine ve veri koruma hukukunun "her şeyin hukuku"na dönüşmesine sebebiyet verecektir.[1]

Aşağıda detaylıca inceleneceği gibi, bir bilginin kişisel veri olarak kabul edilmesinin sonucunda birçok sorumluluk ve yükümlülük gündeme gelmekte ve gerçekleştirilen işleme faaliyeti birçok kurala tabi olmaktadır. Bu sebeple bir bilginin kişisel veri olup olmadığı ve dolayısıyla kişisel verinin tanımı dikkatlice değerlendirilmelidir. Kişisel veri tanımı, Madde 29 Çalışma Grubu (2007) tarafından dört temel unsur altında incelenmiştir.[2] KVKK'de düzenlenmiş kişisel veri tanımı ile GVKT'deki tanımın benzerliği sebebiyle Türk mevzuatındaki kişisel veri tanımı da aynı şekilde incelenebilir.

3.1.1. Kimliği belirli veya belirlenebilir

Kişisel veri tanımının ilk unsuru, bilginin kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin olmasıdır. KVKK'nin gerekçesinde de belirtildiği gibi "kimliği belirli gerçek kişi" ifadesi; ad, soyadı, doğum tarihi ve doğum yeri gibi bilgilerle kesin olarak teşhis edilmiş gerçek kişileri ifade etmektedir. Dolayısıyla bu tür bilgiler, bir gerçek kişinin kimliğini kesin olarak belirler ve kişisel veri olarak kabul edilirler. Ancak, kişisel veri tanımı yalnızca bu tür bilgilerle sınırlı değildir. Aynı zamanda, bir gerçek kişinin kimliğini kesin olarak belirlememesine rağmen herhangi bir şekilde bir gerçek kişiyle ilişkilendirilebilen bilgiler, o gerçek kişiyi tanımlanabilir hale getirmektedir.

---

[1] Purtova, "The Law of Everything…": 33.

[2] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 20 Haziran 2007, 6. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (10.09.2024).

İşte KVKK ve benzer şekilde GVKT, bir kişiyi bu şekilde tanımlanabilir veya kimliği teşhis edilebilir hale getiren bilgileri de kişisel veri olarak kabul etmektedir. Örneğin bir bilgi; bir gerçek kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi gibi herhangi başka bir bilgiyle ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlaması durumunda kişisel veri tanımı altında değerlendirilmektedir. Bir aracın plakası, bir kişinin sosyal güvenlik numarası ve fotoğrafı gibi bilgiler kişiyi doğrudan tanımlamasa dahi dolaylı olarak belirlenebilir kıldığından kişisel veri olarak kabul edilir.

Bu noktada tabiatıyla bir gerçek kişinin belirlenebilir olup olmadığına nasıl karar verilebileceği tartışma konusu haline gelmektedir. GVKT'nin 26'ncı gerekçe maddesine göre bir bilgi, veri sorumlusu veya başka bir kişi tarafından kullanılması makul ve muhtemel olan tüm olanaklar ile yöntemlerin uygulanması sonucunda gerçek bir kişiyle ilişkilendirilebiliyorsa, belirlenebilir bir gerçek kişiye ilişkin kabul edilir ve dolayısıyla kişisel veri olarak tanımlandırılır. Yine aynı gerekçe maddesi ile bu olanak ve yöntemlerin makul ve muhtemel olup olmadığının tespiti için işleme faaliyetinin gerçekleştirildiği sıradaki mevcut teknoloji ve teknolojik gelişmelerin göz önünde tutulması ve kimliğin belirlenmesi için gerekli süre ve maliyet gibi tüm nesnel faktörlerin dikkate alınması gerektiği belirtilmektedir. Özetle, bir bilginin kişisel veri olup olmadığı değerlendirilirken, o bilginin makul ve muhtemel tüm olanakların kullanılmasıyla gerçek bir kişiyle ilişkilendirilip ilişkilendirilememesine bakılmalıdır. Bu olanaklar tespit edilirken ise mevcut teknoloji, süre ve maliyet gibi tüm nesnel faktörler incelenmelidir.

3.1.2. Gerçek kişi

Bir bilginin kişisel veri olarak kabul edilebilmesi için gerçek bir kişiye ilişkin olması gerekmektedir. 22 Kasım 2001 tarihli ve 4721 sayılı Türk Medeni Kanunu uyarınca kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Dolayısıyla ölmüş kişiler ile henüz doğmamış kişilere ilişkin bilgiler, kişisel veri olarak kabul edilemeyecektir. Ayrıca kişisel veriden söz edebilmek için bir gerçek kişinin belirli veya belirlenebilir olması gerektiğinden, tüzel kişilere ilişkin bilgilerin de kişisel veri tanımı altında değerlendirilmediğini söylemek gerekmektedir. Ancak, bir tüzel kişiye ait bilgiler kişisel veri olarak kabul edilmese de tüzel kişinin

temsilcileri veya çalışanları gerçek kişi olduğundan onlara ait bilgiler yine kişisel veri hükmündedir. Örnek vermek gerekirse, "A Şirketi" ile ilgili bilgiler kişisel veri değilken, "A Şirketi Satın Alma Departmanı Yöneticisi"ne ilişkin bilgiler kişisel veri olarak değerlendirilecektir.

3.1.3. –ye ilişkin

Bir bilginin kişisel veri olarak kabul edilmesi için bir gerçek kişiye ilişkin olması gerekmektedir. Kaba tabirle buradaki "-ye ilişkin" unsuru, bir gerçek kişiyle ilgili olması olarak ifade edilebilir. Madde 29 Çalışma Grubu (2007), bir bilginin gerçek kişiye ilişkin olup olmadığının tespiti için; içerik (content), amaç (purpose) ve sonuç (result) unsurlarından en az birisinin mevcut olması gerektiğini belirtmektedir.[3] Özetle; içerik unsurunun varlığını kabul edebilmek için bilginin içeriğinin bir gerçek kişi hakkında olması gerekmektedir. Amaç unsuru incelenirken ise bilginin bir gerçek kişinin davranışlarını veya durumunu değerlendirmek, gerçek kişiyi etkilemek veya ona bir şekilde muamelede bulunmak amacıyla kullanılma durumu veya kullanılma ihtimalinin olup olmadığı değerlendirilir. Sonuç unsurunda ise, bilginin kullanımının bir gerçek kişinin hak ve menfaatlerine etkisi olup olmadığı incelenir.[4] Tüm bu incelemeler sonucunda bir bilginin bir gerçek kişiye ilişkin olup olmadığına dolayısıyla kişisel veri olarak kabul edilip edilmeyeceğine karar verilebilecektir.

3.1.4. Her türlü bilgi

Kişisel veri tanımının son unsuru ise her türlü bilginin bu tanım kapsamına girebilecek olmasıdır. Ne KVKK'de ne de GVKT'de kişisel veri tanımına giren bilgiye ilişkin bir sınırlandırma yapılmıştır. Bu sebeple buradaki "her türlü bilgi" de tabiatıyla geniş yorumlanmalıdır. Madde 29 Çalışma Grubu (2007), buradaki her türlü bilgi ifadesini yine farklı unsurlar altında incelemiştir.[5] Buna göre, öncelikle, tabiatı açısından değerlendirildiğinde hem nesnel hem de öznel bilgilerin kişisel veri sınıflandırmasına tabi olacağı sonucuna varılmaktadır. Ayrıca, bir bilginin kişisel veri olarak kabul edilmesi için doğru olması gerekmemekte, pekâlâ yanlış bilgiler de kişisel veri olarak kabul edilebilmektedir. Bilgi, içeriği bakımından değerlendirildiğinde ise; hassas veya

[3] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data,* 10.
[4] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data,* 11.
[5] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data,* 6.

herkesçe bilinen bir içeriğe sahip olması fark etmeksizin kişisel veri olarak değerlendirilmektedir. Son olarak bilginin kişisel veri olarak kabul edilmesi değerlendirmesinde bilginin türünün bir önemi bulunmamaktadır. Yani bilginin türünün -bir ses kaydı, görüntü veya yazı olmasının-, verinin kişisel veri olup olmadığı değerlendirmesine bir etkisi bulunmamaktadır. Diğer unsurların karşılanması durumunda bilgi, kişisel veri olarak kabul edilecektir.[6]

3.2.Kişisel Verilerin Korunması ile İlgili Temel Kavramlar

3.2.1. Özel nitelikli kişisel veri

KVKK'nin 6'ncı maddesinin birinci fıkrasına göre; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir (special categories of personal data). Özel nitelikli kişisel verilerin işlenmesi; ilgili kişilerin ayrımcılığa uğrama risklerinin daha fazla olması, şeref ve onurlarının zedelenebilecek olması ve mağdur olmalarına sebep olabileceğinden daha sıkı işleme şartlarına ve tedbirlerine tabiidirler.

3.2.2. Kişisel verilerin işlenmesi

Kişisel verilerin işlenmesi KVKK'nin 3'üncü maddesinin birinci fıkrasının (e) bendinde; *"...Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,"* (data processing) olarak tanımlanmıştır. Tanımdan da anlaşılacağı üzere kişisel verilerin işlenmesi kavramı oldukça geniş ifade edilmiştir. Kişisel veriler üzerinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesi olarak kabul edileceğinden, bu işlemlerin her biri için KVKK ve ilgili mevzuat hükümleri geçerli olacaktır.

3.2.3. İlgili kişi

[6] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 7.

İlgili kişi (data subject), KVKK'nin 3'üncü maddesinin birinci fıkrasının (ç) bendinde, kişisel verisi işlenen gerçek kişi olarak tanımlanmaktadır. İlgili kişi kavramı halk arasında veri sahibi olarak da ifade edilebilmektedir.

3.2.4. Veri sorumlusu

Veri sorumlusu (data controller), KVKK'nin 3'üncü maddesinin birinci fıkrasının (ı) bendine göre; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi veri sorumlusu"* olarak tanımlanmıştır.

3.2.5. Veri işleyen

Veri işleyen (data processor), KVKK'nin 3'üncü maddesinin birinci fıkrasının (ğ) bendinde; *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi veri işleyen*" olarak tanımlanmıştır. Veri sorumlusu ile veri işleyen KVKK ve ilgili mevzuat gereğince çok farklı sorumluluklara tabi olduklarından bir gerçek veya tüzel kişinin hangi sıfat altında değerlendirileceğinin doğru bir şekilde tespit edilmesi oldukça önem arz etmektedir.

3.2.6. Otomatik yollarla veri işleme

Kişisel verilerin, bilgisayar ve telefon gibi işlemcisi olan cihazlar tarafından yazılım ve/veya donanım vasıtasıyla insan müdahalesi olmaksızın işlenmesi, kişisel verilerin otomatik yollarla işlenmesi olarak adlandırılır.

3.2.7. Kişisel verilerin anonimleştirilmesi

Anonimleştirme, kişisel verilerin başka bilgilerle birleştirilmesi veya çeşitli yöntemler ile analiz edilmesi sonucunda dahi hiçbir şekilde kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak tanımlanır.

3.2.8. Kişisel verilerin silinmesi

Kişisel verilerin silinmesi; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 8'inci maddesine göre, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Aynı Yönetmeliğin 4'üncü maddesinin ilk fıkrasının (b) bendinde ilgili kullanıcı; "*Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu*

içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler" olarak tanımlanmıştır. Dolayısıyla, kişisel verilerin silinmesi; verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişiler hariç olmak üzere diğer kişilerce hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir.

3.2.9. Kişisel verilerin yok edilmesi

Kişisel verilerin yok edilmesi; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 9'uncu maddesinin birinci fıkrasında, "*Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir."* şeklinde tanımlanmıştır. Silinme işleminden farklı olarak; yok edilme işleminde veriler, verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişiler de dahil olmak üzere hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilir.

3.3.Telekomünikasyon Verisi

Telekomünikasyon kelimesi, Eski Yunanca dilinde "uzak" manasında olan "tele" ile Latince dilinde "iletişim" anlamında gelen "komünikasyon" kelimelerinin birleşimiyle oluşur.[7] Buna göre telekomünikasyon kelimesinin uzaktan gerçekleştirilen iletişim anlamına geldiği söylenebilir. Türk Dil Kurumu internet sayfasında yer alan Güncel Türkçe Sözlük'e göre ise telekomünikasyon; *"Haber, yazı, resim, sembol veya her çeşit bilginin tel, radyo, optik vb. elektromanyetik sistemlerle iletilmesi, bunların yayımı veya alınması; uz iletişim"* olarak tanımlanmaktadır.[8] 05 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'nun 3'üncü maddesinin birinci fıkrasının (h) bendine göre; elektronik haberleşme, *"...Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması"* şeklinde tanımlanmıştır. İki tanım

[7] Bülent Kent, "Telekomünikasyon Sektöründe Evrensel Hizmet Kavramı" *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 16, sy.2 (2012): 170.
[8] Türk Dil Kurumu, "Telekomünikasyon" *Güncel Türkçe Sözlük*, https://sozluk.gov.tr, (03.09.2024).

incelendiğinde, “telekomünikasyon” ile “elektronik haberleşme” kavramlarının büyük benzerlik gösterdiği ve birbirlerinin yerine kullanılabileceği görülebilecektir.

Yukarıda da bahsedildiği gibi; özel hayatın gizliliği ile kişi temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esaslar Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik ile düzenlenmektedir. Bu Yönetmeliğin 2’nci maddesinde yer alan *“Bu Yönetmelik, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kişi abonelikleri dâhil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esasları kapsar.”* hükmüne göre Yönetmelik, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kişi abonelikleri dahil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esasları kapsamaktadır. Yönetmeliğin 4’üncü maddesinin birinci fıkrasının (ç) bendine göre işlem kaydı; “*Kişisel verilere ve ilişkili diğer sistemlere erişen kişiler tarafından yapılan işlemin, işlemin gerçekleştiği tarihten sonra tanımlanabilmesini teminen tutulan ve asgari olarak işlem, işlemin detayı, işlemi yapan kişi, işlemin yapıldığı tarih ve zaman ile işlemi yapan kişinin bağlandığı nokta bilgilerini içeren elektronik kayıtlar”* olarak tanımlanmıştır. Aynı fıkranın (h) bendine göre konum verisi, “*Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veri”* olarak tanımlanmıştır. Son olarak aynı fıkranın (k) bendine göre ise; bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen her türlü veriye trafik verisi denir. Yukarıdaki bilgiler ışığında telekomünikasyon verisi; işlem kaydı, trafik verisi ve konum verisi de dahil olmak üzere elektronik haberleşme çerçevesinde işlenen her türlü veri olarak tanımlanabilir. Bu tanımın Avrupa Birliği mevzuatı ile de uyumlu olduğu söylenebilir. Şöyle ki; her ne kadar yürürlükten kaldırılmış olsa da, Kamuya Açık Elektronik İletişim Hizmetlerinin veya Kamuya Açık İletişim Ağlarının Sağlanmasıyla Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Avrupa Parlamentosu ve Konseyi’nin 15 Mart 2006 tarihli ve 2006/24/EC sayılı Direktifi’nin (Data Retention

Directive) 2'nci maddesinin (a) bendiyle Direktif kapsamında veri ifadesinin trafik, konum ve kullanıcının belirlenmesi için gerekli ilgili veriler anlamına geleceği düzenlenmiştir.

Bu noktada kişisel veri ile telekomünikasyon verisi arasındaki ilişkinin netleştirilmesi gerekmektedir. Kişisel veri, "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmaktadır. Bir bilginin kişisel veri olarak tanımlanması için, kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilebilmesi gerekmektedir. Telekomünikasyon verisi ise gerçek kişiyle ilişkilendirilebilme niteliğinden bağımsız olarak elektronik haberleşme çerçevesinde işlenen verilerdir. Bu çerçevede her telekomünikasyon verisinin kişisel veri olmadığı söylenebilecektir. Örneğin, gerçek bir kişiyle ilişkilendirilebilir her türlü bilgiden arınmış, başka bir deyişle anonimleştirilmiş bir trafik verisi, artık kişisel veri tanımına girmese de hala telekomünikasyon verisi olmaya devam edecektir. Buradaki ayrım ilgili veri grubunun işlenmesinde geçerli olacak mevzuat açısından önem arz etmektedir. Örneğin kişisel veri olmayıp yalnızca telekomünikasyon verisi olarak sınıflandırılan veriler için kişisel veri koruma mevzuatı geçerli olmayacak, bu verilerin işlenmesinde yalnızca telekomünikasyon verilerine ilişkin düzenlemeler uygulanacaktır. Ancak günümüzde neredeyse her türlü verinin gerçek kişilerle ilişkilendirilebileceği gerçeği düşünüldüğünde neredeyse her telekomünikasyon verisinin kişisel veri olarak da sınıflandırılabileceği düşünülebilir.

4. KİŞİSEL VERİLERİN VE TELEKOMÜNİKASYON VERİLERİNİN İŞLENMESİ

4.1.Kişisel Veri İşleme İlkeleri

KVKK'nin 4'üncü maddesiyle kişisel verilerin işlenmesi sırasında uyulması zorunlu olan ilkeler düzenlenmektedir.

4.1.1. Hukuka ve dürüstlük kurallarına uygun olma

Kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak işlenmelidir. Kişisel verilerin hukuka uygun olarak işlenmesi, işleme faaliyeti sırasında kanunlar ve diğer hukuki düzenlemelere tam uyumun sağlanması olarak anlamlandırılır. Buradaki hukuka uygunluk ifadesi, evrensel hukuk ilkelerini ve genel mevzuata uygunluğu kapsar, dolayısıyla oldukça geniş yorumlanır.[1]

22 Kasım 2001 tarihli ve 4721 sayılı Türk Medeni Kanunu'nun 2'nci maddesinde "Dürüst davranma" kavramı, "*Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz.*" şeklinde açıklanmıştır. Dolayısıyla kişisel veriler işlenirken hakkın kötüye kullanılması yasağına uygun hareket edilmesi gerekir. Bu da veri işleme faaliyetine esas olan amaçlara ulaşmaya çalışırken ilgili kişilerin çıkarlarının ve makul beklentilerinin dikkate alınmasıyla gerçekleştirilir.[2] Bu ilke KVKK ve ilgili diğer mevzuat ile düzenlenen diğer yükümlülükleri de kapsar. Örneğin, kişisel verilerin mümkün olduğunca sınırlı miktarda işlenmesi kuralına aykırı hareket edilmesi veya aydınlatma yükümlülüğünün yerine getirilmemesi hem hukuka uygunluk hem de dürüstlük kuralına aykırı hareket edilmesine sebep olacaktır.[3] Bir şirket bünyesinde işlenen kişisel veri setine erişebilen çalışanların yetkilerinin sınırlandırılmaması da dürüstlük kuralına aykırı kişisel veri işlemeye başka bir örnek olarak gösterilebilir.

---

[1] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 2. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, (20.10.2024).

[2] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 4.

[3] Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-" *Kişisel Verileri Koruma Dergisi* 1, sy. 2 (Aralık 2019): 44.

4.1.2. Doğru ve gerektiğinde güncel olma

Yukarıda da sıkça bahsedildiği gibi, kişisel verilerin kullanılmasıyla bireyler hakkında önemli sonuçlar oluşturabilecek kararlar alınması mümkündür. Tabiatıyla alınan bu kararlar bireyleri hukuken veya maddi ve manevi etkileyebilmektedir. Örneğin, birtakım verilerin kombinasyonu ve analiziyle ortaya çıkan kredi risk skoruna göre insanların bankadan belirli bir miktar krediyi çekip çekemeyeceği belirlenmektedir. Bu gibi durumlarda kullanılan verilerin doğru ve güncel olmaması ilgili kişiler aleyhine beklenmedik sonuçlar oluşmasına neden olabilecektir. Tüm bu açıklamalarla uyumlu olarak, eğer kişisel verilerin işlenmesi sonucunda ilgili kişi hakkında bir sonuca varılıyorsa veri sorumlusunun bu verilerin doğru ve güncel olması hususunda aktif özen yükümlülüğü ve olası bir mağduriyetin önüne geçilmesini teminen verilerin doğru ve güncel tutulmasına ilişkin olarak ilgili kanalları her daim açık, bilinir ve güncel tutma yükümlülüğü bulunmaktadır.[4] Bir telefon numarasının ilgili kişiye gerçekten ait olup olmadığının belirlenmesi adına doğrulama kodu gönderilmesi ve bu yöntemle numaranın teyit edilmesi, kişisel verinin doğru olup olmadığının kontrolüne örnek olarak gösterilebilir.

4.1.3. Belirli, açık ve meşru amaçlar için işlenme

Kişisel veriler bir amaç doğrultusunda işlenmelidir. KVKK ve benzer şekilde GVKT'ye göre bu amaç belirli, açık ve meşru olmalıdır. Yani; kişisel veri işleme faaliyeti ilgili kişilerce açık bir şekilde anlaşılabilir olmalı, hangi hukuki sebebe dayanılarak işlendiği kolaylıkla anlaşılabilmeli ve kişisel veri işleme faaliyeti ve bu faaliyet ile ulaşılmak istenilen amaç belirliliği sağlanacak detayda ortaya konulmalıdır.[5] Ayrıca belirtmek gerekir ki, kişisel veri işleme faaliyeti yapılan iş veya sunulan hizmetle bağlantılı ve bunlar için gerekli olmalıdır.[6] Aksi halde kişisel veri işleme faaliyeti hukuka aykırı olacaktır. Örneğin, fatura hazırlamak için ilgili kişiden anne kızlık soyadı bilgisinin istenmesi bu ilkeye aykırılık teşkil edecektir.

4.1.4. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

---

[4] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 6.
[5] Daiman Clifford ve Jef Ausloos, "Data Protection and the Role of Fairness" *Yearbook of European Law*, 37 (2018): 142.
[6] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 8.

Kişisel verilerin belirli, açık ve meşru bir amaç için işlenmesi; bu kişisel veri işleme faaliyetinin hukuka uygun olması için tek başına yeterli değildir. Ayrıca, kişisel verilerin bu amaç ile bağlantılı, sınırlı ve ölçülü olarak işlenmesi gerekmektedir. Gerçekleştirilen kişisel veri işleme faaliyeti yalnızca belirlenen amacı sağlayacak şekilde tasarlanmalı ve bu doğrultuda yürütülmelidir. Amacın gerçekleştirilmesine hizmet etmeyen kişisel veriler işlenmemelidir. İşlenen her kişisel verinin ise amaç ile bir bağlantısı olmalıdır. İleride gerçekleşmesi muhtemel amaçlar için fazladan kişisel veri işlenmesi de yine hukuka aykırı olarak kabul edilecektir.[7]

4.1.5. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

KVKK'nin 4'üncü maddesinde belirtilen son ilke kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme zorunluluğudur. Bu ilkeye göre; öncelikle ilgili kişisel verilerin muhafazası için mevzuatta öngörülen bir süre bulunup bulunmadığı kontrol edilmelidir.[8] Mevzuatta bir süre öngörülmüş ise buna uyulması, öngörülmemişse işleme amacının gerektirdiği süre kadar muhafaza edilmesi gerekmektedir. Bir kişisel verinin belirtilen süreden daha fazla muhafaza edilmesi için geçerli bir nedenin olmaması halinde o kişisel verinin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekir.[9]

4.2. Kişisel Verilerin İşlenmesinin Hukuki Sebepleri

KVKK'nin 5'inci maddesiyle kişisel verilerin işleme şartları belirtilmiştir. Kişisel verilerin işlenmesi için bu maddede tanımlanan şartlardan en az birinin sağlanması gerekmektedir. Buradaki hukuki sebeplerden birine dayanılmaksızın gerçekleştirilen kişisel veri işleme faaliyetleri hukuka aykırı olarak nitelendirilecektir.

4.2.1. İlgili kişinin açık rızasının bulunması

KVKK'nin 3'üncü maddesiyle açık rıza*, "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlanmaktadır. Bu tanıma göre açık rızanın üç unsuru bulunmaktadır. Öncelikle açık rızanın geçerli olması için belirli bir konuyla sınırlandırılmış olması gerekmektedir. Yani açık rıza talep edilirken, tüm

[7] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 10.
[8] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 11.
[9] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, 11.

işleme faaliyetlerini kapsayan, geniş kapsamlı (blanket consent) bir rıza talep edilmemelidir.[10] Bir diğer şart ise açık rızanın bilgilendirmeye dayanmasıdır. Bilgilendirme mutlaka veri işleme faaliyetine başlanmadan önce, açık ve anlaşılır bir dille yapılmalıdır.[11] Son olarak açık rıza özgür iradeyle açıklanmış olmalıdır. Açık rıza alınırken kişinin iradesini sakatlayacak herhangi bir eylem gerçekleştirilmemeli, kişi rızasını tamamen kendi tercihi doğrultusunda vermelidir.[12] Örneğin, rızanın internet ortamında bir kutucuk aracılığıyla alınması durumunda, kutucuğun önceden işaretlenmiş olması ve rıza vermemiş sayılmak için kişinin kutucuktaki işareti kaldırmasının gerekmesi açık rızanın özgür iradeyle verilmiş olması ilkesine aykırılık teşkil edecektir.[13]

4.2.2. Kanunlarda açıkça öngörülmesi

Kanunlarda açıkça öngörülme şartına dayanılarak kişisel veri işlenebilmesi için işleme faaliyetinin doğrudan bir kanun tarafından açıkça öngörülmesi veya yine bir kanunun açıkça işaret ettiği bir ikincil mevzuat tarafından açıkça öngörülmesi gerekmektedir.[14] Herhangi bir kanun hükmü olmaması durumunda bu işleme şartına dayanılarak kişisel veri işlenmesi, hukuka aykırı olarak kabul edilecektir.

4.2.3. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması

Hastalık gibi durumlar sebebiyle rızasını o anda açıklamayacak durumda bulunan veya rızasının hukuki geçerliliği bulunmayan kişilerin kendisi ya da bir başkasının hayatının veya beden bütünlüğünün korunması için zorunlu olması durumlarında kişisel veri işleme faaliyeti bu işleme şartına dayanılarak gerçekleştirilebilir. Bu duruma örnek

---

[10] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679,* 10 Nisan 2008, 16. https://ec.europa.eu/newsroom/article29/items/623051/en, (10.09.2024).

[11] Kişisel Verileri Koruma Kurumu, *Açık Rıza*, 5. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, (20.10.2024).

[12] Kişisel Verileri Koruma Kurumu, *Açık Rıza*, 2.

[13] Avrupa Birliği Adalet Divanı Kararı, 1 Ekim 2019 günlü, C-673/17 sayılı karar.

[14] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, 74. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF, (21.10.2024).

olarak iş kazası geçiren bir işçinin yakınlarına durumun derhal haber verilmesi gibi nedenlerle telefonunun işçinin rızası olmadan ele geçirilmesi ve ilgili bilgilere işçinin telefonu üzerinden ulaşılması örnek olarak gösterilebilir.[15]

4.2.4. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması

Kişisel veri işleme faaliyetinin bir sözleşmenin kurulmasıyla veya bir sözleşmenin ifasıyla doğrudan doğruya ilgili olması şartıyla, bu sözleşmenin taraflarına ait kişisel veri işlemenin gerekli olması durumunda bu işleme şartına dayanılarak kişisel veri işlenebilir. Bu duruma örnek olarak, bir satıcının müşterisine sattığı bir malı teslim etmek amacıyla müşterisinin adresini taşıma şirketine vermesi gösterilebilir.

4.2.5. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

Kişisel veri işleme faaliyetinin veri sorumlusunun bir hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması durumunda bu işleme şartına dayanılabilir. Bir şirketin çalışanına maaş ödeyebilmesi için çalışanın evli olup olmadığı bilgisini işlemesi bu şarta dayanılarak kişisel veri işlenmesine örnek teşkil etmektedir.[16]

4.2.6. İlgili kişinin kendisi tarafından alenileştirilmiş olması

Alenileştirme kavramı, Kişisel Verileri Koruma Kurumu'nun 16 Aralık 2020 tarihinde yayımlanan "Alenileştirme Hakkında Kamuoyu Duyurusu" ile ilgili kişinin kişisel verilerinin, kendisi tarafından kamuoyuna açıklanması olarak tanımlanmıştır.[17] Başka bir deyişle; alenileştirme, kişisel verilerin ilgili kişi tarafından bilerek ve isteyerek herhangi bir şekilde açıklanmasıdır. Buna göre; ilgili kişinin kişisel verilerini kendisinin alenileştirdiği durumlarda, bu alenileştirme iradesi ve amacına uygun olarak kişisel verileri bu işleme şartına dayanılarak işlenebilir. Burada önemli olan,

---

[15] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, 75.

[16] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, 77.

[17] Kişisel Verileri Koruma Kurumu, *"Alenileştirme" Hakkında Kamuoyu Duyurusu*, 16.12.2020, https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU, (22.10.2024).

ilgili kişinin alenileştirme iradesi ve amacının dışına çıkılmamasıdır.[18] Örneğin, bir internet sitesinde aracını satmak için telefon numarasını paylaşmış kişinin su arıtma cihazı satmak maksadıyla aranması bu hukuki sebebe uygun bir işleme olarak kabul edilmeyecektir. Nitekim, Kişisel Verileri Koruma Kurulunun 07 Kasım 2019 tarihli ve 2019/331 sayılı kararında da ilgili kişi tarafından alenileştirilen cep telefonu numarasının bir şirket tarafından başka bir amaçla işlenmesinin hukuka aykırı olduğu belirtilmiştir.

4.2.7. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

Kişisel veriler; bir hakkın tesisi, kullanılması veya korunması için zorunlu olması durumunda bu işleme şartı çerçevesinde işlenebilmektedir. Bir şirketin, çalışanının ileride fazla mesaiye ilişkin açabileceği davada ispat için çalışana ait giriş-çıkış saatlerini dava zamanaşımı süresi boyunca muhafaza etmesi bu işleme şartına örnek olarak gösterilebilir.[19]

4.2.8. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olduğu durumlarda ilgili kişinin temel hak ve özgürlüklerine zarar vermemek şartıyla bu işleme şartına dayanılarak kişisel veriler işlenebilir. Bu işleme şartına dayanabilmek için öncelikle veri sorumlusunun menfaatinin gerçekten meşru olup olmadığı değerlendirilmelidir. Bu çerçevede menfaat, ilgili kişinin temel hak ve özgürlükleri ile yarışabilecek düzeyde ve halihazırda mevcut olmalıdır.[20] Bu değerlendirmenin olumlu sonuçlanması sonrasında ilgili kişilerin etkilenebilecek hak ve özgürlüklerinin tespiti gerekir. Tespit sonrasında ise veri sorumlusunun menfaati ile ilgili kişinin hak ve özgürlükleri

---

[18] Faruk Bilir, "Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır" *TRT Akademi* 6, sy.11 (Ocak 2021): 179.

[19] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, 4. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf, (19.10.2024).

[20] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, 7.

arasında bir denge testi gerçekleştirilmelidir.[21] Çalışan bağlılığını artırmak amacıyla ödül ve prim uygulanması için veri işlenmesi bu işleme şartına örnek olarak verilebilir.

4.3. Özel Nitelikli Kişisel Verilerin İşlenmesinin Hukuki Sebepleri

Yukarıda da belirtildiği gibi, özel nitelikli kişisel verilerin işlenmesi ilgili kişilerin mağdur olabilmesi ve şeref ile onurlarına zarar gelebilecek olması gibi sebeplerden dolayı daha sıkı işleme şartlarına tabiidir. Özel nitelikli kişisel verilerin işlenmesi bu sebeple diğer kişisel verilerin işlenme şartlarından ayrı olarak düzenlenmiştir. 12 Mart 2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 33, 34, 35 ve 36'ncı maddeleri ile KVKK'nin 6'ncı, 9'uncu, 18'inci ve Geçici 3'üncü maddelerinde değişiklik yapılmıştır. 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 33'üncü maddesiyle özel nitelikli kişisel verilerin işlenme şartlarını düzenleyen KVKK'nin 6'ncı maddesi güncellenmiştir. Söz konusu değişiklik 1 Haziran 2024 itibariyle yürürlüğe girmiştir. Bu maddeye göre, özel nitelikli kişisel verilerin işlenmesi belirtilen şartlardan birisinin olmaması halinde yasaklanmıştır.

4.3.1. İlgili kişinin açık rızasının bulunması

Bu işleme şartı yukarıda açıklandığından, bu bölümde ilave açıklamaya yer verilmemiştir.

4.3.2. Kanunlarda açıkça öngörülmesi

Bu işleme şartı yukarıda açıklandığından, bu bölümde ilave açıklamaya yer verilmemiştir.

4.3.3. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması

Bu işleme şartı yukarıda açıklandığından, bu bölümde ilave açıklamaya yer verilmemiştir.

---

[21] Ayşe Nida Günal ve Yasin Üstün, "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak "Meşru Menfaat"" *Kişisel Verileri Koruma Dergisi* 4, sy.2 (Aralık 2022): 12.

4.3.4. İlgili kişinin alenileştirdiği kişisel verilere ilişkin ve alenileştirme iradesine uygun olması

Bu işleme şartı yukarıda açıklandığından, bu bölümde ilave açıklamaya yer verilmemiştir.

4.3.5. Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması

Bu işleme şartı yukarıda açıklandığından, bu bölümde ilave açıklamaya yer verilmemiştir.

4.3.6. Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması

Özel nitelikli kişisel veri olarak düzenlenen sağlık verileri; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla gerekli olması şartıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca bu hukuki sebebe dayanılarak işlenebilecektir. Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumu'nun söz konusu maddede belirtilen amaçlarla işledikleri veriler ve kayıtlar bu kapsamda değerlendirilecektir.[22]

4.3.7. İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması

İstihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması

---

[22] Türkiye Büyük Millet Meclisi, *Karabük Milletvekili Cem Şahin ve İstanbul Milletvekili Şengül Karslı ile 124 Milletvekilinin Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi (2/2023) ve Adalet Komisyonu Raporu*, 21.02.2024, 26. https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y2/T2/DosyaKomisyonRaporunuVerdi/cfb35b8a-65cc-44e7-b1bc-4764e98175b9.pdf?TSPD_101_R0=08ffcef486ab2000ff6d9063f76177c27189b7e025b25454c512ff820de1d50765a39b27bcd1a034086738216614300c16a8f07b0ec74cc344efc58244c86db1757365a8b4157994ed518a02274a9b0deaa58622e1d44fd9b2073d0532fa767, (22.10.2024).

durumunda özel nitelikli kişisel veriler bu amaçlarla sınırlı olarak işlenebilecektir. 4857 sayılı İş Kanunu ile işverenlere yönelik olarak düzenlenen engelli veya hükümlü çalıştırma yükümlülüğünün yerine getirilmesi amacıyla çalışanların sağlık veya ceza mahkumiyetine ilişkin verilerinin işlenmesi bu hukuki sebep kapsamında değerlendirilecektir.[23]

4.3.8. Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumların, tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilere yönelik olması

Tâbi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak şartlarıyla siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek ve diğer kâr amacı gütmeyen kuruluş ya da oluşumlar; mevcut veya eski üyelerine ve mensuplarına veyahut bu kuruluş ve oluşumlarla düzenli olarak temasta olan kişilerin sendika üyeliği bilgisi gibi özel nitelikli kişisel verilerini bu hukuki sebebe dayanarak işleyebilecektir. Bir derneğin bağış yapmak suretiyle kendisiyle etkileşim halinde olan üyesinin kişisel verilerini işlemesi bu kapsamda değerlendirilecektir.[24]

4.4. Kişisel Verilerin Aktarımı

Yukarıda da açıklandığı gibi; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesi olarak adlandırılır. Bu doğrultuda kişisel verilerin aktarılması da ayrı bir kişisel veri işleme faaliyetidir. Bu

[23] Türkiye Büyük Millet Meclisi, *Karabük Milletvekili Cem Şahin* …, 26.
[24] Türkiye Büyük Millet Meclisi, *Karabük Milletvekili Cem Şahin* …, 27.

sebeple KVKK ve ilgili mevzuat ile düzenlenen tüm şartların aktarım için de ayrıca başlı başına geçerli olduğu söylenebilecektir.

Kişisel verilerin aktarılması, KVKK'nin 8'inci maddesiyle düzenlenmektedir. Söz konusu maddede, *"(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) a)Kişisel veriler; 5'inci maddenin ikinci fıkrasında, b) yeterli önlemler alınmak kaydıyla 6'ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması halinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir."* hükümlerine yer verilmiştir. Dolayısıyla, kişisel verilerin aktarılması için kişisel verileri işleme şartlarından en az birinin bulunması gerekmektedir.

Kişisel verilerin yurt dışına aktarılması konusuna, aşağıda detaylıca inceleneceğinden burada yer verilmemiştir.

4.5.Telekomünikasyon Verilerinin Önemi ve İşlenmesi

4.5.1. Kritik altyapı olarak telekomünikasyon

Telekomünikasyon verileri, ülkemizin iletişim altyapısının güvenliği ve sürdürülebilirliği açısından kritik önemi haiz olduğundan kişisel veri olup olmadığına bakılmaksızın ayrı şartlara tabi tutulmuştur. Bu duruma ilişkin gelişmeler özellikle 2012 yılında başlamış, bu tarihte ülkemizde siber güvenlik alanında çalışmalar hızlanmıştır. Bunun en temel göstergesinin, *Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemek amacıyla* 20 Ekim 2012 tarihli ve 28447 sayılı Resmî Gazete'de yayımlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı olduğu söylenebilir. Bakanlar Kurulu Kararı'nın 4'üncü maddesiyle siber güvenlikle ilgili olarak alınacak önemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla belirli kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur. Ayrıca aynı Bakanlar Kurulu Kararı'nın 5'inci maddesinin birinci fıkrasının (ç) bendiyle

Ulaştırma, Denizcilik ve Haberleşme Bakanlığına, ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapma görevi verilmiştir.

Bakanlar Kurulu Kararı ile kurulan Siber Güvenlik Kurulu, ilk toplantısını 21 Aralık 2012 tarihinde; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığında yapmıştır.[25] Bu toplantı sonucunda Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı kabul edilmiştir.[26] Ulusal Siber Güvenlik Stratejisi kapsamında kritik altyapılar*; işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar* olarak tanımlanmıştır. Bununla beraber Eylem Planı ile kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin sağlanması amaçlanmıştır. Bu çerçevede kritik altyapıların güvenliğinin sağlanması için özel sektörle karar mekanizmalarına katılımı da içeren tam iş birliğinin yapılması temel ilkelerden birisi olarak kabul edilmiştir. Yine; hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri de Eylem Planı çerçevesinde temel esas olarak kabul edilmiştir.[27]

Eylem Planının en önemli etkilerinden birisinin siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi ve yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması amaçlarıyla ulusal düzeyde etkin bir şekilde çalışacak Ulusal Siber Olaylara Müdahale Merkezinin (USOM) ve USOM'un koordinasyonunda çalışacak sektörel Siber Olaylara Müdahale Ekiplerinin (SOME) kurulmasının planlanmasıdır. Bu doğrultuda öncelikli olarak,

---

[25] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014*, 1. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf, (04.10.2024).

[26] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014*, 1.

[27] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014*, 7.

kritik altyapılara ait bilişim sistemleri, kritiklik seviyeleri, birbirleriyle ilişkileri ve sorumlularının belirlenmesi; kritik altyapı sektörlerine özel sektörel SOME'lerin kurulması ve sektörel SOME'lerin doğrudan USOM'un koordinasyonunda faaliyet yürütmesi tasarlanmıştır.[28]

Sürecin devamında SOME'lerin kuruluş, görev ve çalışmalarına dair usul ve esasları belirleyerek hizmetlerin etkin ve verimli bir şekilde yürütülmesini sağlamayı amaçlayan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ 11 Kasım 2023 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Tebliğ'in 3'üncü maddesinin birinci fıkrasının (ç) bendiyle *kritik altyapıları bünyesinde barındıran sektörler* kritik sektörler olarak adlandırılmıştır. Aynı Tebliğ'in 6'ncı maddesinin üçüncü fıkrasıyla kritik sektörlerde, sektörel SOME kurulması zorunlu tutulmuş ve kritik sektörlerin listesinin Siber Güvenlik Kurulu tarafından belirlenerek duyurulacağı belirtilmiştir. 2014'ün Kasım ayında yayımlanan Sektörel SOME Kurulum ve Yönetim Rehberi ile ülkemizin kritik altyapı sektörleri "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" olarak belirlenmiştir.[29] Bu çerçevede elektronik haberleşme (başka bir deyişle, telekomünikasyon) sektöründe sektörel SOME'nin, Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmasına karar verilmiştir.

Kritik altyapılarda karşılaşılan herhangi bir güvenlik riski, kamu hizmetinin sağlanmasını engelleyebilmekte, kamu düzenini bozabilmekte ve milli güvenliği tehdit edebilmektedir. Bu sebeple oluşabilecek güvenlik risklerinin azaltılması ve etkisiz kılınmasının sağlanması amacıyla alınması gerekli tedbirleri düzenlemek amacıyla 06 Temmuz 2019 tarihli ve 30823 sayılı Resmî Gazete'de yayımlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yürürlüğe girmiştir. Bu Genelgeye aşağıda yer verileceğinden, bu kısımda incelenmeyecektir.

---

[28] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014,* 10.

[29] Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, *Sektörel SOME Kurulum ve Yönetim Rehberi,* 7.

Özetle; telekomünikasyon verilerinin gizlilik, erişilebilirlik ve bütünlüğünün bozulmasının kamu düzeninin bozulmasından milli güvenliğe karşı tehdit oluşturmasına kadar birçok önemli güvenlik riskine sebep olabileceği söylenebilir. Ayrıca olası bir bilgi güvenliği ihlali; bir kamu hizmeti olan haberleşmenin sağlanamaması veya bireyler arasındaki iletişimin ifşa olması gibi sonuçlara yol açabileceğinden vatandaşların özel ve aile hayatına saygı hakkı, kişisel verilerin korunmasını isteme hakkı ve ifade özgürlüğü gibi temel hak ve hürriyetlerine de müdahaleyi beraberinde getirecektir. Bu sebeple telekomünikasyon verilerinin güvenliğinin sağlanmasının büyük bir önem arz ettiği kolaylıkla söylenebilecektir.

4.5.2. Telekomünikasyon verilerinin işlenmesi

Yukarıda da açıklandığı üzere, telekomünikasyon verisi olarak tanımlanan verilerin neredeyse tümünün kişisel veri tanımına da girdiğini söylemek yanlış olmayacaktır. Kişisel veri niteliğindeki telekomünikasyon verilerinin işlenmesi konusunda genel kurallar KVKK ile düzenlenmektedir. Telekomünikasyon verilerinin işlenmesi özelinde ise; EHK, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik ve ilgili diğer mevzuat incelenmelidir. Hatırlatmak gerekir ki; telekomünikasyon verilerinin işlenmesine ilişkin kurallar, söz konusu veriler kişisel veri olmasa dahi uygulama alanı bulacaktır. Dolayısıyla bir veri, herhangi bir gerçek kişiyle ilişkilendirilebilme yeteneğinden yoksun olsa dahi telekomünikasyon verisi olması dahilinde bu şartlara tabi olacaktır.

EHK'nin "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51'inci maddesi ile telekomünikasyon verilerinin işlenmesine ilişkin ana kurallar belirlenmiştir.

4.5.2.1. Telekomünikasyon Verilerinin İşlenmesinin Hukuki Sebepleri

Yukarıda kişisel verilerin işlenmesi için kanunda tanımlanmış hukuki sebeplerden en az birinin mevcudiyetinin gerekliliğine ve bu hukuki sebeplerden birine dayanılmaksızın gerçekleştirilen kişisel veri işleme faaliyetlerinin hukuka aykırı olarak nitelendirileceğine değinilmişti. EHK'nin 51'inci maddesi uyarınca telekomünikasyon verisine özel olarak işleme şartları getirilmiştir. Maddenin 2'nci fıkrasıyla; elektronik haberleşmenin ve ilgili trafik verisinin gizliliğinin esas olduğuna, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye

taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesinin yasak olduğuna hükmedilmiştir. Haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi gibi faaliyetler; KVKK uyarınca kişisel veri işleme faaliyetidir. Ancak telekomünikasyon verilerinin işlenmesi açısından özel düzenleme EHK iken, KVKK ise genel düzenleme olarak kabul edilmelidir. Her ne kadar bu faaliyetler kişisel veri işleme faaliyeti olsa da, EHK ile telekomünikasyon verilerinin işlenmesiyle ilgili özel bir düzenleme getirildiği için; bu işleme faaliyeti öncelikli olarak EHK'ye tabii olacaktır. Dolayısıyla bu veriler işlenirken yalnızca EHK'de belirtilen hukuki sebeplere dayanılabilecek, EHK'de belirtilmeyip KVKK'de belirtilen diğer hukuki sebeplere dayanılamayacaktır. Çünkü, EHK ile bu kişisel veri işleme faaliyetlerine özel bir işleme şartı getirilmiş ve ilgili verilerin yalnızca haberleşmeye taraf olanların tamamının rızası ile işlenebileceği düzenlenmiştir. Ancak, yine söz konusu maddede ilgili mevzuatın ve yargı kararlarının öngördüğü durumların hariç bırakıldığı görülmektedir. Burada kastedilenin 5271 sayılı Ceza Muhakemesi Kanunu'nun 135'inci maddesiyle düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması hükümleri olduğu söylenebilecektir. Bu madde ile; "*Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir*." hükmü düzenlenmiştir. Son olarak, bu faaliyetin gerçekleştirilmesinde genel düzenleme kabul edilecek KVKK'de yer verilen hukuki sebeplere de dayanılabileceği düşünülebilir. Örneğin KVKK'nin 5'inci maddesinin ikinci fıkrasının (f) bendiyle düzenlenen meşru menfaat hukuki sebebine dayanılarak haberleşmenin kaydedilmesi gündeme gelebilecektir. Ancak, bu durumun EHK ile tesis edilmek istenen haberleşmenin gizliliğine aykırılık teşkil edeceği ve özel kanun istisnasının yalnızca 5271 sayılı Ceza Muhakemesi Kanunu ve yargı kararları ile sınırlı tutulması gerektiği değerlendirilmektedir.

EHK'nin 51'inci maddesinde ise, "*Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.*" hükmü yer almaktadır. Burada da yukarıdaki hüküm ile aynı doğrultuda olacak şekilde; cep telefonu gibi terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak için kullanıcıların açık rızasının alınması gerektiği düzenlenmektedir.

Aynı maddenin beşinci fıkrasında, "*Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir*." hükmü bulunmaktadır. EHK'nin 49'uncu maddesiyle işletmecilere son kullanıcı ve tüketicilerin hizmet seçenekleri, hizmet kalitesi, tarifeler ile tarife paketlerinin yayımlanmasına ve benzeri hususlarda abonelerin bilgilendirilmesine yönelik yükümlülükler getirilebileceği düzenlenmektedir. Maddenin devamında ise işletmecilerin, özellikle hizmetler arasında seçim yapılırken ve abonelik sözleşmesi kurulurken tüketicilerin karar vermelerinde etkili olabilecek hususlar ile dürüstlük kuralı gereğince bilgilendirilmelerinin gerekli olduğu her durumda talep olmaksızın tüketicileri bilgilendirmesi gerektiğine hükmedilmektedir. Dolayısıyla 49'uncu madde ile işletmecilere yönelik olarak tüketicileri bilgilendirme yükümlülüğü getirildiği görülmektedir. Bu hususta işletmeciler, bilgilendirme faaliyetini yerine getirirken KVKK'nin 5'inci maddesinin ikinci fıkrasının (a) bendiyle düzenlenen *"Kanunlarda açıkça öngörülmesi"* hukuki sebebine dayanarak kişisel veri işleyebilecektir. Ayrıca işletmeciler, bu yükümlülüğü yerine getirdiklerini göstermek adına gerçekleştirdikleri kişisel veri işleme faaliyetlerinde de KVKK'nin 5'inci maddesinin ikinci fıkrasının (ç) bendiyle düzenlenen *"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* hukuki sebebine dayanabileceklerdir. Yine, EHK'nin 51'inci maddesinin beşinci fıkrası uyarınca işletmeciler, Kurum tarafından kendilerine getirilen yükümlülüklerin yerine getirilmesi için *"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* hukuki sebebine dayanarak kişisel veri işleyebileceklerdir.

EHK'nin 51'inci maddesinin yedinci fıkrasındaki; "*Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır."* hükmü ile trafik verilerinin hangi amaçlarla işlenebileceği ifade edilmiştir. Bu durumda trafik verilerinin aynı zamanda kişisel veri olması ve belirtilen amaçlarla işlenmesi durumunda KVKK'nin 5'inci maddesinin ikinci fıkrasının (a) bendiyle düzenlenen "Kanunlarda açıkça öngörülmesi" hukuki sebebine dayanılabilecektir. Maddenin devamında ise "*Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.*" ifadelerine yer verilmiştir. Buna göre konum verilerinin ve trafik verilerinin, katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla işlenebilmesi için ya kullanıcı/abonelerin açık rızalarının alınması ya da bu verilerin anonim hale getirilmesi gerekmektedir.

Kanun koyucu, konum verilerinin işlenebilmesini de şarta bağlamıştır. EHK'nin 8'inci maddesinde, "*İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir."* hükmü düzenlenmiştir. Bu madde ile abonelerin/kullanıcıların konum verilerinin esas olarak açık rızaları alınarak işlenebileceğine hükmedilmektedir. Ancak afet ve acil durum hallerinde abonelerin/kullanıcıların konum verileri ve ilgili kişilerin kimlik bilgilerinin açık rıza aranmaksızın işlenebileceği düzenlenmektedir. Bu işleme faaliyetinde de

KVKK'nin 5'inci maddesinin ikinci fıkrasının (a) bendiyle düzenlenen "Kanunlarda açıkça öngörülmesi" hukuki sebebine dayanılabilecekt.

EHK'nin 51'inci maddesinin dokuzuncu fıkrası ile, abone/kullanıcı şikayetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel verilerin belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebileceği düzenlenmektedir. Bu durumda veri sorumluları, kişisel veri işlerken KVKK'nin 5'inci maddesinin ikinci fıkrasının (a) bendiyle düzenlenen "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebebine dayanabileceklerdir.

Son olarak, EHK'nin aynı maddesinin on birinci fıkrasındaki; *"Tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir."* hükmü ile abonelere ilişkin birtakım bilgilerin işletmeciler ve BTK'nin merkezî mobil cihaz kimlik tanımı veri tabanı sistemi arasında paylaşılabileceği veya işlenebileceği öngörülmüştür.

5. KİŞİSEL VERİLERİ VE TELEKOMÜNİKASYON VERİLERİNİ KORUMA MEKANİZMALARI

5.1. Kişisel Verileri Koruma Mekanizmaları

Veri koruma mevzuatında düzenlenen kişisel verileri koruma mekanizmaları, elbette ki yalnızca veri işlemenin birtakım ilkelere ve şartlara bağlanması ve bu şartlar dışında veri işlemenin yasaklanması ile sınırlı değildir. Bunun yanında mevzuatta ilgili kişilerin mahremiyetinin korunması adına kişisel veri işleme faaliyetinin hukuka uygun olmasını sağlayacak başka koruma mekanizmaları da düzenlenmiştir. Bu başlık altında öncelikle kişisel verilerin korunmasına yönelik genel düzenlemelerden, sonrasında ise telekomünikasyon verilerine özel olarak öngörülmüş ek yükümlülüklerden bahsedilecektir.

5.1.1. Kişisel verilerin korunmasına yönelik genel düzenlemeler

5.1.1.1. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esaslar Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile düzenlenir. Kişisel veriler, yukarıda da bahsedildiği gibi, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Bu sürelerin sonunda kişisel verinin işlenmesi için başka bir hukuki sebebin bulunmaması durumunda işleme faaliyetine devam edilmesi hukuka aykırılık ile sonuçlanacaktır. KVKK'nin 7'nci maddesinin birinci fıkrasında; "*Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir."* hükmü yer almaktadır.

5.1.1.2. Veri sorumlusunun aydınlatma yükümlülüğü

Veri sorumlularının aydınlatma yükümlülüğünün düzenlendiği KVKK'nin 10'uncu maddesinde; *"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları,

konusunda bilgi vermekle yükümlüdür." hükmü yer almaktadır.

Aydınlatma yükümlülüğüne ilişkin detaylı kurallar ise Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ ile düzenlenmiştir.

5.1.1.3. İlgili kişinin hakları

Kişisel verilerin korunmasına ilişkin düzenlenen mekanizmanın en önemlilerinden birisinin ilgili kişinin hakları olduğu rahatlıkla söylenebilir. İlgili kişiler, kişisel verilerinin işlenmesiyle ilgili olarak veri sorumlularına kanunda tanımlanan haklarını kullanmak amacıyla başvurabilir. İlgili kişilerin hakları ise KVKK'nin 11'inci maddesiyle düzenlenmiştir. Buna göre ilgili kişiler;

"…a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme"

haklarına sahiptir.

İlgili kişilerin haklarını kullanırken veri sorumlusuna yapacakları başvuruya ilişkin kurallar ise Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ile düzenlenmiştir.

5.1.1.4. Veri güvenliğine ilişkin yükümlülükler

Kişisel verilerin başkaları tarafından öğrenilmesi, ilgili kişilerin mağduriyetine veya ayrımcılığa uğramalarına sebep olabileceğinden ve her halükârda mahremiyetlerinin ihlali anlamına geleceğinden veri sorumlularının işledikleri kişisel verilerin güvenliğini sağlama yükümlülüğü bulunmaktadır. Bu yükümlülük temel olarak KVKK'nin 12'nci maddesiyle düzenlense de yükümlülüğün neleri kapsadığı günbegün Kişisel Verileri Koruma Kurulu kararları ile detaylandırılmaktadır. KVKK'nin 12'nci maddesinin birinci fıkrasına göre veri sorumlusu; kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Aynı maddenin 3'üncü fıkrası ile veri sorumlularına veri güvenliğinin sağlanması adına denetim yapma veya yaptırma zorunluluğu da getirilmektedir.

5.1.1.5. Kişisel Verileri Koruma Kuruluna şikâyet

Yukarıda da bahsedildiği gibi, KVKK ile ilgili kişilerin hakları düzenlenmiştir ve ilgili kişiler bu haklarını veri sorumlularına başvurmak suretiyle kullanabilmektedir. KVKK'nin 14'üncü maddesine göre; veri sorumlusuna yapılan bu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir. Kanun koyucu, Kurul'a şikâyet için veri sorumlusuna başvuruyu ön koşul olarak düzenlemiştir. Başka bir deyişle, veri sorumlusuna başvuru yapılmaksızın doğrudan Kurul'a yapılan başvuru, incelenmeksizin reddedilecektir. Şikâyet üzerine yapılan incelemenin usul ve esasları ise KVKK'nin 15'inci

maddesiyle düzenlenmiştir. Kurulun bir inceleme başlatması için bir şikâyetin varlığına gerek olmadığı, Kurulun re'sen de inceleme başlatabileceği yine aynı maddeyle belirtilmiştir.

5.1.1.6. Veri Sorumluları Sicili

KVKK'nin 16'ncı maddesi ile Kişisel Verileri Koruma Kurulu gözetiminde kamuya açık olarak Veri Sorumluları Sicili tutulacağı düzenlenmiştir. Aynı maddenin ikinci fıkrasıyla kişisel verileri işleyen gerçek ve tüzel kişilere, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolma zorunluluğu getirilmiştir. Fıkranın devamında ise Kurul tarafından bu zorunluluğa istisna getirilebileceği belirtilmektedir. Veri Sorumluları Sicili, ilgili kişilerin veri sorumlularını kamuya açık bir sicil üzerinden aratarak işlenen kişisel verilerini öğrenebilmeleri açısından büyük önem arz etmektedir. Sicilin oluşturulması, idaresi ile sicile yapılması öngörülen kayıtlara ilişkin usul ve esaslar ise Veri Sorumluları Sicili Hakkında Yönetmelik ile düzenlenmiştir.

5.1.2. Telekomünikasyon verilerinin korunmasına yönelik düzenlemeler

Yukarıda da bahsedildiği gibi; bazı kişisel veriler, başkaları tarafından öğrenildiği takdirde ilgili kişilerin daha çok mağdur olmalarına veya ayrımcılığa maruz kalmalarına sebep olabilir. Aynı şekilde bazı veri türleri de milli güvenlik, kamu düzeninin korunması veya kritik altyapıların güvenliğinin sağlanması gibi nedenlerle diğer verilere nazaran daha kapsamlı bir koruma gerektirir. Bu gibi sebeplerle özellikle kritik altyapılar bünyesinde işlenen verilere ilişkin ek koruma mekanizmaları geliştirilmektedir.

5.1.2.1. Bilgilendirme yükümlülüğü

EHK'nin 3'üncü maddesine göre; elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri kaydıyla kullanılabilir. Pratik hayatta pek mümkün gözükmese de buradaki verilerin kişisel veri olmaması durumunda dahi bu yükümlülüklerin geçerli olacağını belirtmekte fayda bulunmaktadır.

Burada KVKK'nin 10'uncu maddesiyle düzenlenen veri sorumlusunun aydınlatma yükümlülüğü doğrultusunda bir düzenleme getirilmektedir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 4'üncü maddesine göre aydınlatma yükümlülüğü kişisel verilerin elde edilmesi sırasında yerine getirilmelidir. Aynı Tebliğ'in 5'inci maddesine göre, kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemleri ayrı ayrı yerine getirilmelidir. Buradaki işleme faaliyetinin de açık rızaya dayanması zorunlu olduğundan, açık rıza alınması ve aydınlatmanın bir arada yapılmasının hukuka aykırılık oluşturacağını söylemek mümkündür. Yine aynı Tebliğ maddesine göre kullanıcı/abonelere yapılacak bilgilendirme anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmelidir.

5.1.2.2. Sunulan hizmetin güvenliğini sağlama yükümlülüğü

EHK'nin 51'inci maddesinin dördüncü fıkrası ile işletmecilere; şebekelerin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alma yükümlülüğü getirilmiştir. Bu yükümlülüğün de KVKK'nin 12'nci maddesiyle düzenlenen veri güvenliğine ilişkin yükümlülüklere benzer bir düzenleme olduğu görülmektedir. Buradaki teknik ve idari tedbirler, abone/kullanıcılara ait kişisel verilerin yanında ayrıca abone/kullanıcılara sunulan hizmetlerin güvenliğine yönelik olarak da alınmalıdır. Dolayısıyla, söz konusu hizmetlere ilişkin öngörülen güvenliğin sağlanması yükümlülüğü, kişisel verilerin korunmasının yanında kritik altyapı olarak görülen telekomünikasyon sektörüne ilişkin geniş bir düzenlemedir.

5.1.2.3. Erişim/yetki ve ölçü/süre sınırlandırması yükümlülüğü

EHK ile trafik verilerinin işlenmesine ilişkin kurallar da öngörülmüştür. Kanunun 51'inci maddesinin yedinci fıkrasında; *"...(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır..."* hükmü

yer almakta olup buna göre, trafik verileri yukarıda yer verilen amaçlarla ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı olarak işlenebilir. Kanun koyucu burada trafik verilerinin işleme amaçlarını daraltmakla kalmamış, veriyi işleyebilecek kişileri de sınırlamıştır. Ayrıca, uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar trafik verilerinin gizliliğinin ve bütünlüğünün sağlanmasına hükmedilmiştir. Aynı şekilde konum ve trafik verileri, katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amaçlarıyla yalnızca işletmeci tarafından yetkilendirilen kişilerle sınırlı olarak, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilecektir. Bu sınırlama EHK'nin 51'inci maddesinin sekizinci fıkrası ile afet ve acil durumlarda açık rıza alınmaksızın işlenebilecek konum verileri ve ilgili kişilerin kimlik bilgileri için de tanımlanmıştır.

EHK ile belirlenen kişisel veri işleme sınırlamaları elbette ki yalnızca erişim veya amaç kısıtlaması değildir. Aynı maddenin onuncu fıkrası ile kişisel verilere ilişkin temel saklama süresi belirlenmiştir. Buna göre;

"…(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince,

saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir." hükmü ile de kişisel verilere ilişkin temel saklama süresi belirlenmiştir.

Veri Sorumluları Sicili Hakkında Yönetmelik'in 9'uncu maddesinin dördüncü fıkrasına göre; kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza süresi belirlenirken; ilgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre, ilgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis

edilen hukuki ilişkinin devam edeceği süre ve veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre gibi hususlar dikkate alınır. Bu durumda EHK'nin yukarıda bahsedilen hükmü uyarınca belirtilen kategorideki veriler belirtilen süreler boyunca saklanmalı, bu sürenin sonunda Veri Sorumluları Sicili Hakkında Yönetmelik'in 9'uncu maddesinin dördüncü fıkrasındaki hususların değerlendirilmesiyle bu kişisel verilerin imha edilmesi gerekliliği değerlendirilmelidir. Son olarak, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim hale Getirilmesi Hakkında Yönetmeliğin 7'nci maddesinin üçüncü fıkrası uyarınca, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanmalıdır.

5.1.2.4. Kişisel verilerin gizliliği ve güvenliğini sağlama ve bildirim yükümlülüğü

İşletmeciler, EHK kapsamında işlenen kişisel verilerin gizliliği ve güvenliğinin sağlanması ile amacı doğrultusunda kullanılmasının temini için EHK'nin 51'inci maddesinin on ikinci fıkrası ile yükümlü kılınmıştır. EHK'nin 51'inci maddesinin yanında Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik ile de düzenleme getirilmiştir. Bu kapsamda Yönetmeliğin 6'ncı maddesinin ikinci fıkrası ile işletmeciler asgari olarak aşağıdaki tedbirleri almakla sorumlu tutulmuştur:

- Kişisel verilerin 3.1. numaralı başlık altında incelenen kişisel veri işleme ilkeleri çerçevesinde işlenmesine yönelik güvenlik politikaları belirlenmelidir.
- İstem dışı, yetki dışı ya da mevzuata aykırı olarak; kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesi gibi ihlallere karşı kişisel verilerin korunması sağlanmalıdır.
- Kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin saklandığı sistemler ile kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliği sağlanmalıdır.

Yönetmeliğin devamında, GVKT'deki hesap verebilirlik (accountability) ilkesiyle uyumlu olarak, işletmecilerin kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtlarını iki yıl saklamakla yükümlüğü olduğu düzenlenmiştir.

Yönetmelik ile ayrıca işletmecilere yönelik olarak şebekelerinin ve sundukları hizmetlerin güvenliğini tehdit eden bir riskin varlığı durumunda, KVKK'de ve kişisel verilerin korunması mevzuatında tanımlanan yükümlülüklerden çok daha ağır sorumluluklar düzenlenmiştir. KVKK'nin 12'nci maddesinin beşinci fıkrasıyla kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusunun bu durumu en kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurulu'na bildirmesi zorunluluğu düzenlenmiştir. Bu kapsamda Kişisel Verileri Koruma Kurulu, 24 Ocak 2019 tarihli ve 2019/10 sayılı kararıyla; veri sorumlularının, kişisel veri ihlalini öğrendikleri tarihten itibaren derhal ve en geç 72 saat içinde Kurul'a bildirimde bulunmak zorunda olduklarına hükmetmiştir.[1] Aynı karar ile veri ihlalinden etkilenen kişilerin tespit edildikten sonra, makul bir süre içinde bu kişilere de bildirim yapılması gerekliliği belirtilmiştir. Burada bu bildirim yükümlülüğünün, bir veri ihlalinin meydana gelmesiyle ortaya çıktığına dikkat çekmek gerekir. Elektronik haberleşme hizmeti çerçevesinde işlenen kişisel veriler konusunda ise Yönetmelik, işletmecilerin bildirim yükümlülüğünün doğması için veri ihlali yaşanmasından önce; şebekelerin ve sundukları hizmetlerin güvenliğini tehdit eden bir riskin olmasını yeterli görmüştür. Böyle bir risk çıktığında işletmeciler, Yönetmelik'in 7'nci maddesinin birinci fıkrası uyarınca; ilgili aboneleri/kullanıcıları bu risk hakkında ve bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması halinde, söz konusu riskin kapsamı ve giderilme yöntemleri hakkında en kısa sürede bilgilendirmelidir. Aynı maddenin ikinci fıkrasında ise kişisel veri ihlali olması durumunda BTK'ye, Kişisel Verileri Koruma Kuruluna ve ilgili abonelere/kullanıcılara en kısa sürede bildirimin yapılması gerektiği de düzenlenmiştir.

5.1.2.5. Açık rızanın şartlara uygun olarak alınması yükümlülüğü

[1] Kişisel Verileri Koruma Kurulu Kararı, 24 Ocak 2019 tarih ve 2019/10 sayılı karar.

Telekomünikasyon verilerine ilişkin olarak açık rıza alma şartları, kişisel verilerin korunması mevzuatına göre oldukça detaylı düzenlenmiştir. KVKK ile açık rızanın yalnızca tanımına yer verilmiş, ancak açık rızanın alınma yöntemleri ve kuralları ile ilgili herhangi bir düzenleme yapılmamıştır. Yine Kişisel Verileri Koruma Kurumu tarafından yayımlanan yönetmelik ve tebliğlerde de açık rızanın nasıl alınacağına ilişkin hükümlere yer verilmemiş, ancak bahsi geçen Kurumun yayımlamış olduğu "Açık Rıza" isimli rehber ve bazı duyurularda açık rıza koşullarından bahsedilmiştir.[2] Buna karşılık olarak Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in 8'inci maddesiyle elektronik haberleşme hizmetleri çerçevesinde işlenen verilere ilişkin alınması gereken açık rızanın şartları detaylıca düzenlenmiştir. Buna göre; açık rıza beyanı belirli bir konuya ilişkin olarak işlem öncesinde alınır. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki rızalar geçersiz kabul edilir.

Maddenin devamında ise açık rıza beyanının özgür iradeyle açıklanması gerektiği; abonelik tesis edilmesi ve temel elektronik haberleşme hizmetleri veya cihazların sunulmasının, abonenin/kullanıcının verilerinin işlenmesine yönelik açık rıza verme ön şartına bağlanamayacağı, ancak hediye dakika, SMS ve veri gibi ek fayda sağlanması karşılığında aboneden/kullanıcıdan açık rıza talep edilebileceği düzenlenmiştir. Bu hükmün açık rızayı düzenleyen maddeye eklenmesi büyük önem arz etmektedir. Zira, bir hizmetin sunulmasının açık rıza verme ön şartına bağlanması, açık rızanın özgürce verilmiş olması şartını zedeleyecektir.[3] Başka bir ifadeyle, kullanıcıya açık rızasını vermezse, temel bir hizmeti/cihazı kullanamayacağının belirtilmesi; kullanıcının açık rıza verme hususundaki iradesini sakatlayacak ve hizmeti kullanmanın yegâne şartı olarak gösterilen açık rızayı istemediği halde vermesine sebep olabilecektir. Açık rızaya ilişkin getirilen bu yasak KVKK ile düzenlenmezken, GVKT'nin 7'nci maddesinin dördüncü fıkrasıyla açık bir şekilde düzenlenmiştir. Açık rızanın hukukiliğinin sağlanması açısından önemi sebebiyle bu sınırlamanın bu Yönetmelik hükmünde yer bulmasının telekomünikasyon verilerinin işlenmesi açısından oldukça önemli bir gelişme olduğu söylenebilecektir. Maddenin

[2] Kişisel Verileri Koruma Kurumu, *Açık Rıza*, 3.
[3] Göksu Hazar Erdinç, "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi", *Kişisel Verileri koruma Dergisi* 2, sy.1, (Haziran 2020): 15.

devamında hizmetin sağlanmasının açık rıza verme ön şartına bağlanma yasağının da istisnası tanımlanmıştır. Buna göre hediye dakika, SMS ve veri gibi ek fayda sağlanması karşılığında aboneden/kullanıcıdan açık rıza talep edilebilecektir.

Yönetmelik'in 8'inci maddesinin birinci fıkrasının (c) bendinde kişisel veri, trafik verisi ve konum verisi işleme faaliyetlerine ilişkin işletmecilerin bilgilendirme yükümlülüğü düzenlenmiştir. Maddenin devamındaki (ç) bendiyle ise açık rıza beyanının bilgilendirme sonrasında abonenin/kullanıcının "evet/onay/kabul" şeklinde yazılı olarak veya elektronik ortamda alınması gerektiğine hükmedilmiş ve açık rızanın diğer onay beyanlarıyla birleştirilmesi yasaklanmıştır. Söz konusu fıkranın (d) bendinde ise, GVKT'deki hesap verebilirlik (accountability) ilkesiyle uyumlu olarak, abonelerin/kullanıcıların açık rızalarını gösteren kayıtların asgari olarak abonelik süresince saklanması yükümlülüğü düzenlenmiştir.

Açık rıza koşullarına ilişkin son düzenleme ise aynı Yönetmelik'in 13'üncü maddesiyle yapılmıştır. Bu maddenin birinci fıkrasında; abonelerin/kullanıcıların verdikleri açık rızayı kolayca geri alabilmelerinin sağlanması, geri alma imkanının açık rıza alınırken yapılan bilgilendirmede belirtilmesi, ikinci fıkrasında işletmeciler tarafından her yıl abonelere/kullanıcılara açık rızaları kapsamında verilerinin işlendiğinin hatırlatılması, hatırlatma yapılmaması durumunda veri işleme faaliyetinin durdurulma zorunluluğu, üçüncü fıkrasında engelli tarifelerinden yararlanan abonelere/kullanıcılara yapılacak bilgilendirmenin işitsel ve/veya görsel yöntemler kullanılarak yapılması, dördüncü fıkrasında aboneliğin sonlanması durumunda aksi talep olmaması halinde tüm açık rızaların geri alınmış sayılması, beşinci fıkrasında tüm bilgilendirmelerin ücretsiz yapılması ve yedinci fıkrasında açık rızanın geri alınması durumunda tüm veri işleme faaliyetlerinin derhal durdurulması zorunluluğu düzenlenmiştir. Bu madde ile, aslında veri sorumlusunun bir yükümlülüğü olan açık rızanın hukuka uygun olarak alınmasının yöntemleri açıklanmakta ve bu şekilde veri sorumlusu yöntem arama zahmetinden bir miktar da olsa kurtarılmaktadır. Ancak aynı maddenin altıncı fıkrasıyla açık rıza, abone/kullanıcı talebi ve onayına ilişkin ispat sorumluluğu, GVKT ve KVKK ile uyumlu olarak yine işletmeciyle verilmiştir. Tüm bu düzenlemeler elektronik haberleşme sektöründe kişisel verilerin korunması ve mahremiyetin sağlanması hususunda büyük bir önem arz etmektedir.

5.1.2.6. Aktarıma ilişkin yükümlülükler

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in 8'inci maddesinin birinci fıkrasının (e) bendinde trafik ve konum verilerinin aktarımına ilişkin işletmecilere yükümlülükler getirilmiştir. Buna göre söz konusu maddenin (e) bendi; "*Trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlar için; 1) Aktarılacak verinin kapsamı, 2) Aktarılacak tarafın adı ve açık adresi, 3) Aktarma amacı ve süresi, 4) Üçüncü tarafın yurt dışında olması halinde verinin aktarılacağı ülkenin adı, şeklindeki bilgiler verilerek ayrıca açık rıza alınır. Bu bilgilerde değişiklik olması halinde tekrar açık rıza alınır."* şeklinde olup bu hükümden hareketle, trafik ve konum verilerinin aktarımına yönelik ayrıca bir koruma sağlanmasının amaçlandığı söylenebilecektir. İşlenen trafik ve konum verilerinin aktarımı için ayrıca açık rıza alınması ve bahsedilen bilgilerde bir değişiklik olması durumunda tekrar açık rıza alınması şartı getirilerek abonelerin/kullanıcıların kritik veri olarak kabul edilen trafik ve konum verilerinin aktarımına ilişkin söz sahibi olması sağlanmaya çalışılmıştır. Bahsi geçen hüküm ile ayrıca verilerin yurt dışına aktarılacak olması halinde aktarım yapılacak ülkenin adının da aboneyle/kullanıcıyla paylaşılması gerekmektedir. Söz konusu Yönetmelik'in 8'inci maddesinin birinci fıkrasının son hükmü olan (f) bendi ile, işletmecilere trafik ve konum verilerinin aktarıldığı üçüncü kişilerin işleme faaliyetlerinin aktarım kapsamı içerisinde gerçekleştiğinin temin edilmesi yükümlülüğü tanımlanmıştır. Bu hüküm, işletmecilere verinin aktarımından sonra maruz kaldığı işleme faaliyetlerini denetleme yükümlülüğü de getirmektedir. Bu doğrultuda işletmeciler; verilerin aktarılması için gerekli olan açık rızanın ve de bu açık rızanın dayandığı bilgilendirmenin kapsamının doğru bir şekilde belirlendiğinden emin olmalı ve üçüncü kişilerin de bu kapsamın dışına çıkmadığından emin olmalıdır.

6. VERİ LOKALİZASYONU

6.1.Veri Lokalizasyonu Kavramı

Daha önce de detaylıca değinildiği gibi, bireylerin mahremiyeti ve kişisel verilerinin korunması temel bir insan hakkıdır. Mahremiyetin ve kişisel verilerin korunmasına yönelik olarak gerçekleşecek bir ihlal ise ilgili kişilerin ayrımcılığa maruz kalmaları gibi ciddi mağduriyetlere sebebiyet verebilmektedir. Bu sebeple hem ülkemizde hem de uluslararası hukukta mahremiyetin ve kişisel verilerin korunmasına ilişkin birçok düzenleme yapılmış ve koruma mekanizmaları geliştirilmiştir. Aşağıda da bahsedileceği gibi; devletler zamanla, ilerleyen teknoloji başta olmak üzere birtakım ekonomik, siyasi ve stratejik sebeplerle bu koruma mekanizmalarını yetersiz bulmuş ve yeni düzenlemeler getirmeye başlamıştır. Süreç içerisinde kişisel verilerin yurt içinde saklanmasının mahremiyet ve kişisel verilerin korunması açısından önemli ve gerekli bir yöntem olduğu düşüncesi gelişmiştir.

Verilerin yurt içinde tutulması, yalnızca kişisel verilerle sınırlı tutulmamıştır. Bu korumalar her ne kadar bireylerin menfaati gereği kişisel veriler ve mahremiyet üzerine geliştirilmiş olsa da devletlerin korumakla yükümlü olduğu başka menfaatler de bulunmaktadır. Örneğin devletler, AİHS'in 2'nci maddesiyle bireylerin yaşam hakkını ve 5'inci maddesiyle özgürlük ve güvenlik hakkını koruma altına almakla ve sağlamakla yükümlüdür. Yine kamu düzeninin sağlanması ve milli güvenliğin korunmasının da devletlerin temel yükümlülükleri arasında olduğu kolaylıkla söylenebilecektir. Bunlardan hareketle devletler; kamu hizmeti olarak görülen ve vatandaşların temel ihtiyaçlarını karşılayan sağlık, enerji ve iletişim gibi sektörleri düzenli olarak denetlemekte ve diğer sektörlere göre daha katı kurallarla düzenlemektedir. Ülkemizde de bu sektörler kritik altyapı olarak sınıflandırılmakta ve ilave kurallara tabi tutulmaktadır.[1] Bu kritik altyapıların kesintiye uğraması, vatandaşların temel haklarından mahrum kalmasına ve kamu düzeninin bozulmasına sebep olabilecektir. Bu sebeple devletler kritik altyapıların korunması hususunda katı düzenlemeler yapma yoluna gidebilmektedir. Kritik altyapıların korunmasının en önemli unsurlarından birisi de elbette ki kritik altyapılara ilişkin bilgilerin

[1] Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, *Sektörel SOME Kurulum ve Yönetim Rehberi,* 7.

korunmasıdır. Devletler bu korumayı sağlamak için kritik altyapılara ilişkin bilgi ve verilerin de yurt içinde saklanması yoluna başvurabilmektedir. Hem kişisel verilerin hem de kritik altyapılara ilişkin verilerin yurt içinde saklanmasına yönelik genel eğilim, veri lokalizasyonu kavramını gündeme getirmiştir.

Veri lokalizasyonu, verinin ulusal sınırlar dışına aktarımını engelleyen veya zorlaştıran kurallar olarak tanımlanabilir.[2] Daha detaylı bir tanıma göre ise veri lokalizasyonu, doğrudan veya dolaylı olarak verilerin belirli bir egemenlik alanı içerisinde münhasıran veya münhasır olmayan bir şekilde depolanmasını veya işlenmesini öngören zorunlu yasal veya idari gereksinimlerdir.[3] Tanımlardan da anlaşılacağı gibi, verilerin yurt içinde depolanmasını ve/veya işlenmesini zorunlu kılan, verilerin yurt dışına aktarımını engelleyen veya zorlaştıran kurallara veri lokalizasyonu denmektedir.

Veri lokalizasyonu tanımının yurt dışı aktarım kurallarını içerip içermediği hususunda literatürde netlik bulunmamaktadır. Başka bir deyişle, verilerin yurt dışına aktarımını birtakım şartlara bağlayan düzenlemelerin veri lokalizasyonu kabul edilip edilmeyeceği konusu tartışmalıdır. Bazı yazarlar yurt dışı aktarım şartlarını da veri lokalizasyonu tanımına dahil ederken[4], bazı yazarlar veri lokalizasyonu kurallarının sert bir veri egemenliği politikası olduğunu ve yurt dışı aktarım kurallarının veri lokalizasyonu olmadığını savunmaktadır.[5] Veri lokalizasyonu tanımları incelendiğinde, yurt dışına veri aktarımını zorlaştıran kuralların da veri lokalizasyonu olarak kabul edildiği görülecektir. Ayrıca, verilerin yurt dışı aktarımının birtakım şartlara bağlı olması, her ne kadar düzenlenen şartlar göreceli olarak kolaylıkla sağlanabiliyor olsa bile söz konusu verinin yurt içinde kalmasının esas olduğunun bir göstergesidir. Kanun koyucunun iradesinin de söz konusu şartların sağlanmaması

---

[2] Chander ve Lê, "Data Nationalism": 718.

[3] Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *Data localisation trends and challenges, Considerations for the review of privacy guidelines,* Aralık 2020, https://www.oecd.org/en/publications/data-localisation-trends-and-challenges_7fbaed62-en.html, (01.07.2024).

[4] Courtney M. Bowman, "A Primer on Russia's New Data Localization Law", *Proskauer*, 27 Ağustos 2015, https://privacylaw.proskauer.com/2015/08/articles/data-privacy-laws/a-primer-on-russias-new-data-localization-law/ (16.09.2024).

[5] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*

durumunda verilerin yurt içinde kalması yönünde olduğu söylenebilecektir. Son olarak, yurt dışı aktarım kuralları doğrudan bir veri lokalizasyonu kuralı olmasa dahi sektörde veri lokalizasyonu politikası ile aynı sonuçlara sebep olmaktadır.[6] Tüm bu nedenlerle, verilerin yurt dışı aktarımının belli şartlara bağlanması da bu tez kapsamında veri lokalizasyonu olarak değerlendirilecektir.

6.2.Veri Lokalizasyonu Türleri

Veri lokalizasyonu politikaları ülkeden ülkeye farklılık gösterebilmekte ve birçok türde uygulanabilmektedir. Her ülkenin ve sektörün kendi ihtiyacı doğrultusunda benzersiz olarak geliştirilebileceğinden doğru ve kesin bir sınıflandırmadan söz edilemeyecektir. Aşağıda uygulamadaki veri lokalizasyonu politikalarından ve mevcut sınıflandırmalardan yararlanmak suretiyle farklı türler incelenmiştir.

6.2.1. Uygulamaya göre veri lokalizasyonu türleri

Veri lokalizasyonu temel olarak katı, yumuşak, karma ve zorlaştırılmış veri aktarımı olmak üzere dört ana başlık altında incelenebilir[7]:

6.2.1.1. Katı veri lokalizasyonu

Katı veri lokalizasyonu politikaları, verilerin ancak bu kuralları düzenleyen ülkenin sınırları içerisinde işlenebileceğini ve depolanabileceğini öngören kurallardır.[8] Başka bir deyişle, katı veri lokalizasyonu kuralları; verilerin yalnızca o ülke sınırları içerisinde depolanmasını şart koşmakla kalmaz, aynı zamanda veri üzerinde gerçekleştirilecek herhangi bir işlem de o ülke içerisinde olmalıdır. Dolayısıyla, katı veri lokalizasyonu kurallarının uygulandığı bir ülkede verilere yurt dışından erişilmesi dahi mümkün değildir.

6.2.1.2. Yumuşak veri lokalizasyonu

Verilerin bir kopyasının ülke sınırları içerisinde tutulması şartıyla işleme veya depolama amacıyla yurt dışına aktarımına izin verilmesini öngören kurallar, yumuşak

---

[6] Chander ve Lê, "Data Nationalism": 715.
[7] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*
[8] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*

veri lokalizasyonu olarak adlandırılır.[9] Bu lokalizasyon türü, şartlı kopyalama (*conditional mirroring*) olarak da adlandırılmaktadır.[10] Yumuşak veri lokalizasyonu politikasının uygulandığı bir ülkede veriler, kopyasının o ülkede tutulması şartıyla yurt dışında işlenebilecek ve yurt dışına aktarılabilecektir.

6.2.1.3. Karma veri lokalizasyonu

Karma veri lokalizasyonu politikaları hem katı hem de yumuşak veri lokalizasyonu kurallarının özelliklerini barındırır. Bu politikayı benimseyen bir ülkede, veriler yurt içinde depolanması şartıyla yurt dışında da işlenebilir.[11] Örneğin, verilerin yurt içinde tutulması şartını koşan ancak yurt dışından söz konusu verilere erişilmesini yasaklamayan bir ülkede karma veri lokalizasyonundan söz edilecektir.

6.2.1.4. Zorlaştırılmış veri aktarımı

Verilerin doğrudan o ülke içerisinde işlenmesi veya depolanması şartının bulunmadığı, ancak verilerin yurt dışına aktarımı için belirli şartların düzenlendiği politikalar 'de facto veri lokalizasyonu' olarak adlandırılır.[12] Bu durumda katı veya yumuşak türde bir veri lokalizasyonu teoride bulunmamaktadır. Ancak, verilerin yurt dışına aktarımı belirli şartlara tabi tutulduğundan verilerin yurt dışında işlenebilmesi zorlaştırılmaktadır. Bu durum da sektörde veri lokalizasyonunun yukarıda açıklanan üç türünde gerçekleşen etkilerin aynısını oluşturduğundan, veri lokalizasyonu olarak kabul edilmektedir.[13] Bunun dışında yurt dışına veri aktarımı için vergi uygulaması da bir de facto veri lokalizasyonu olarak kabul edilebilir.[14] Bu politikaların tam manasıyla bir veri lokalizasyonu politikası olmaması, ancak benzer sonuçlara yol açabilmesi sebebiyle bu tez kapsamında de facto veri lokalizasyonu politikaları, zorlaştırılmış veri aktarımı olarak adlandırılacaktır.

---

[9] Daniel Castro ve Alan Mcquinn, "Cross-Border Data Flows Enable Growth in All Industries" *Information Technology & Innovation Foundation*, Şubat 2015.
[10] Anirudh Burman ve Upasana Sharma, "How Would Data Localization Benefit India?" *Carnegie Endowment for International Peace*, Nisan 2021, https://carnegie-production-assets.s3.amazonaws.com/static/files/202104-Burman_Sharma_DataLocalization_final.pdf, (20.09.2024).
[11] Burman ve Sharma, *How Would Data…* 16.
[12] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*
[13] Bowman, "A Primer on Russia's…"
[14] Chander ve Lê, "Data Nationalism": 719.

6.2.2. Diğer veri lokalizasyonu ayrımları

6.2.2.1. Sektöre göre veri lokalizasyonu ayrımı

Yukarıda da bahsedildiği gibi, devletler kamu düzeninin sağlanması ve vatandaşların temel ihtiyaçlarının kesintiye uğramaması adına bazı sektörleri kritik altyapıyı haiz olarak görmektedir. Bu beisle kritik altyapıya sahip sektörleri korumak adına bu altyapı çerçevesinde işlenen verilere ayrı bir önem verilmektedir. Çoğu ülkede genel bir veri lokalizasyonu politikasından ziyade sektör bazlı lokalizasyon kuralları uygulanmaktadır.[15]

6.2.2.2. Veri sorumlusuna göre veri lokalizasyonu ayrımı

Bazı ülkelerde sektör veya ilgili altyapının kritik olarak tanımlanmasından bağımsız olarak veri, türünden dolayı kritik olarak görülmektedir. Örneğin, 06 Temmuz 2019 tarihli ve 30823 sayılı Resmî Gazete'de yayımlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile kamu kurumları tarafından işlenen verilerin ülke sınırları içerisinde tutulması gerekliliği düzenlenmiştir.

6.3.Veri Lokalizasyonunun Gerekçeleri ve Gerekçelerin Değerlendirilmesi

Ülkeler birçok nedenle veri lokalizasyonu politikalarını benimseyebilmektedir. Bu başlık altında veri lokalizasyonu politikalarının en sık karşılaşılan gerekçeleri incelenecek ve devamında ise gerekçelerin değerlendirmesi yapılacaktır.

6.3.1. Mahremiyetin ve kişisel verilerin korunması

Mahremiyet ve kişisel verilerin korunmasını isteme hakkı, bireylerin temel hakları arasında yer almaktadır. Bu hakların ihlal edilmesi durumunda bireylerin ayrımcılığa maruz kalmaları gibi oldukça olumsuz durumlarla karşılaşma riskleri bulunmaktadır. Yukarıda da açıklandığı üzere, devletler vatandaşların mahremiyetinin ve kişisel verilerinin korunmasını sağlamakla yükümlüdür. Bu yükümlülüklerini ise bu alanda geliştirdikleri mevzuat ile düzenlen koruma mekanizmaları ile sağlamaktadır. Örneğin; KVKK gereği şirketler, vatandaşların kişisel verilerini istedikleri gibi kullanamamakta, birtakım kurallar çerçevesinde işleme faaliyetlerini

[15] Burcu Tuzcu Ersin vd., "Türk Veri Koruma Hukuku 2021 İlk 5 Yılda Uygulamadaki Gelişmeler" *Moroğlu Arseven*, (2021): 12.

gerçekleştirebilmektedir. Bu anlayış çerçevesinde kişisel verilerin yurt dışına aktarılması da birtakım kurallara tabi tutulmuştur. Nitekim, kişisel verilerin yurt dışına aktarılmasının bu kurallara bağlı olmaması durumunda veri sorumluları verileri kolaylıkla koruma düzeyi çok güçlü olmayan bir ülkeye aktarabilecek veya verileri yurt dışındaki şirketlere pazarlayabilecektir. Bu gibi durumların önüne geçilmesi için KVKK'nin 9'uncu maddesiyle kişisel verilerin yurt dışına aktarılması ayrıntılı olarak düzenlenmiştir.

Kişisel verilerin yurt dışına aktarımı konusunda genel yaklaşım yukarıda bahsedilen zorlaştırılmış veri aktarımı rejiminin benimsenmesi yönündedir. Hem KVKK hem de GVKT, kişisel verilerin yurt dışına aktarılabilmesi için öncelikli şart olarak verilerin aktarılacağı ülkenin kişisel veriler için en az kendisinin sunduğu korumayı sağlamasını belirlemiştir. Genel uygulama, bu korumayı sağladığı düşünülen ülkeler için bir yeterlilik kararı verilmesi ve bu ülkelere aktarımın yurt içi aktarım şartlarına tabi olarak daha kolay bir şekilde gerçekleştirilebilmesidir. Yeterlilik kararı bulunmayan ülkeler için ise aktarım yine yapılabilmekte, ancak bu aktarım belirli şartlara tabi tutulmaktadır.

Gerçekten de nasıl ki ülke içerisinde kişisel verilerin işlenmesi için belirli kurallara uyulması gerekiyorsa, aynı şekilde bu verilerin yurt dışına aktarılması için de kuralların tanımlanması gerekmektedir. Burada önemli olan, tanımlanan veri lokalizasyonu kurallarının sağlanmak istenen koruma veya menfaat ile orantılı olmasıdır. Buradaki dengenin sağlanmaması, gereğinden daha katı veri lokalizasyonu politikaları ortaya çıkarabilecek ve global açıdan birçok olumsuz etkinin doğmasına sebep olabilecektir. Örneğin; veri lokalizasyonu politikaları, bilginin ve verilerin ülke içerisinde depolanmasını zorunlu tuttuğundan bilgilerin sınırlar arası özgürce dolaşmasını engellemektedir.[16] Ayrıca veri lokalizasyonu politikaları, özellikle birden fazla ülkede faaliyet gösteren şirketler için regülasyona uyumluluk ve teknoloji maliyetleri getirebilmekte ve bazı şirketler bu maliyetlere katlanmaktansa katı mevzuatın uygulandığı ülkelerden çekilmeyi tercih edebilmektedir. Bu durum da o ülkedeki vatandaşların birtakım ürün ve hizmetler ile teknolojik yeniliklerden mahrum

[16] Chander ve Lê, "Data Nationalism": 718.

kalmasına sebep olabilecektir.[17] OECD, bunun gibi veri lokalizasyonunun global açıdan oluşturduğu olumsuz etkilerinin önüne geçmek amacıyla bireylerin hak ve özgürlüklerinin korunması ile veri lokalizasyonu ile ulaşılması istenen menfaat arasındaki dengenin sağlanması konusunda dikkate alınabilecek bazı kriterler yayımlamıştır.[18] Buna göre veri lokalizasyonu kurallarının sağlayacağı faydalar ile bu kuralların beraberinde getireceği risklerin orantılı olup olmadığının tespiti için;

- verilerin hassasiyeti;
- işlemenin amacı ve bağlamı;
- veri yerelleştirme tedbirinin getirildiği hedeflere etkili bir şekilde ulaştığının ne ölçüde kanıtlandığı;
- yürürlüğe konabilecek daha az kısıtlayıcı bir tedbir olup olmadığı;
- tedbirlerin doğrudan ve dolaylı, ulusal ve uluslararası etkileri;
- tespit edilmesinin mümkün olduğu durumlarda niyet kanıtı; ve
- diğer ülkelerin de aynı tedbiri benimsemesi halinde ortaya çıkabilecek sonuçların

beraberce değerlendirilmesi gerekmektedir.[19]

Bu noktada kişisel verilerin korunması amacıyla oluşturulmuş veri lokalizasyonu kurallarının bireylerin iradesinin önüne geçmemesi gerektiğini de belirtmek gerekmektedir. Bir vatandaşın verisinin başka bir ülkeye aktarılmasını kendisinin talep etmesi veya söz konusu aktarıma rıza göstermesi durumunda, ortada korunacak başkaca bir menfaatin bulunmayacağı açıktır. Ayrıca böylesi bir durumda dahi katı veri lokalizasyonu politikası uygulayarak kişisel verinin aktarımını engellemek, başkaca bir menfaatin olmaması halinde, yukarıda belirtilen faktörlerin ışığında orantılı kabul edilemeyecektir. Zira, aşağıda daha detaylıca açıklanacağı üzere, verilerin paylaşımı konusunda ekonomik ve teknolojik gelişmelere fayda sağlaması başta olmak üzere birçok menfaat bulunmaktadır.

[17] Burman ve Sharma, *How Would Data…* 14.
[18] Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *Data localisation trends and challenges…* , 25.
[19] Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *Data localisation trends and challenges…* , 30.

Bazı yazarlar, veri lokalizasyonu politikalarının mahremiyet ve kişisel verilere ilişkin bir koruma sağlamayacağını düşünmektedir. Chander ve Lê'ye göre, veri lokalizasyonu sonucunda veriler yalnızca yerel sunucularda depolanabilecektir ve bu sebeple veriler farklı konumlarda dağınık bir şekilde tutulamayacaktır.[20] Bu durum ise kötü niyetli kişilere karşı verilerin tek bir noktada toplanmasına ve dolayısıyla siber güvenlik zafiyetlerine sebep olabilecek, bu durumda insanların mahremiyeti ve kişisel verileri ifşa olabileceği için tehlikeli bir pozisyona düşülecektir. Yine aynı yazarlara göre, veri lokalizasyonu politikaları sunucuların tesisi ve korunmasına yönelik teknolojilerin global seçeneklerle sağlanmamasına ve yerel imkanlarla karşılanmasına sebep olacak, bu durum da siber güvenlik açıklarına neden olacaktır.[21] Öncelikle söylemek gerekir ki; bir ülkede uygulanan veri lokalizasyonu politikası, verilerin o ülke içerisindeki farklı sunucularda depolanmasını engellememektedir. Dolayısıyla verilerin kötü niyetli kişilere karşı tek bir noktada saklanması yerine farklı sunucularda depolanabilmesi mümkündür. Bunun yanında veri lokalizasyonu politikası ile sunucuların ülke sınırları içerisinde bulunması zorunluluğunun düzenlendiği, ancak, kanuni bir engel yoksa, donanım temini konusunda yurt dışındaki imkanlardan hala yararlanabileceği unutulmamalıdır. Son olarak Ünver ve Kim'in de belirttiği gibi, siber güvenliğin sağlanması konusunda önemli olan sunucunun veya verilerin konumu değil, alınan idari ve teknik tedbirlerdir.[22] Bu doğrultuda söz konusu verileri ve sunucuyu korumak adına gerekli tedbirlerin alınması halinde sunucunun fiziki olarak bulunduğu yer önem arz etmeyecektir.

Tüm bu sebepler doğrultusunda, mahremiyetin ve kişisel verilerin korunması adına "de facto veri lokalizasyonu politikası" olarak kabul edilen yurt dışı aktarım kurallarının benimsenmesinin temel insan haklarının tesisi ve korunması amacıyla zorunlu olduğu söylenebilecektir. Başka bir deyişle, temel hak ve hürriyetlerinin korunması açısından zorlaştırılmış veri aktarımı kurallarının uygulanması zaruridir. Öte yandan katı ve yumuşak veri lokalizasyonu kurallarının uygulanmasının da

[20] Chander ve Lê, "Data Nationalism": 719.
[21] Chander ve Lê, "Data Nationalism": 721.
[22] Akın Ünver ve Grace Kim, "Cross-Border Data Transfers and Data Localization" *EDAM Cyber Policy Paper Series 2016/3*. Haziran 2016. https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf. (09.10.2024).

korunmak istenen menfaat ile değerlendirildiğinde orantılı olmayacağı değerlendirilmektedir.

6.3.2. Kolluk ve istihbarat faaliyetleri

Bir devletin en temel görevlerinden birisinin kamu düzeninin sağlanması olduğunu söylemek yanlış olmayacaktır. Bu kapsamda devletler; suçların tespiti ve önlenmesi, terörizmin önüne geçilmesi ve milli güvenliğin sağlanması gibi amaçlar doğrultusunda faaliyetler yürütmektedir. Bu faaliyetler tabiatıyla büyük miktarda kişisel verinin işlenmesini gerektirebilmekte ve bu amaçlarla vatandaşların mahremiyet alanına müdahale edilebilmektedir. Teknolojinin getirdiği imkanlar da düşünülerek, günümüzde tartışılması gereken konu, devletlerin milli güvenlik ve suçların önlenmesi amaçlarıyla vatandaşların verilerini kontrol edip edememesi değil, ne kapsamda edebileceğinin belirlenmesidir.[23] Zira, örneğin, devletlerin suçların önlenmesi ve soruşturulması kapsamında vatandaşların verilerine erişebilmesi gerekmektedir. Ancak burada kamu menfaati karşısında mahremiyet ve kişisel verilerin korunması hakkının ölçülülük ve orantılılık kapsamında bir denge testine tabi tutulması ve devletin sınırlarının belirlenmesi gerekmektedir.

Tüm bu sebepler doğrultusunda devletler, kolluk ve istihbarat faaliyetleri amacıyla kişisel verilere erişmekte ve erişebileceği kişisel verilerin niceliği ile niteliğini artırmaya çalışmaktadır. Bu durum, kolluk ve istihbarat makamlarını verileri egemenliği altında tutma çabasına itmiş; bu da beraberinde devletlerin veri lokalizasyonu politikalarına başvurmaya başlamasına sebep olmuştur.[24] Her ne kadar devletlerin veriye erişim kabiliyetinin artmasının kolluk ve istihbarat faaliyetlerini güçlendireceği açık olsa da literatürde veri lokalizasyonu politikaları ile devletlerin amaçlarına ulaşamayacağını savunan görüşler mevcuttur. Yayboke'ye göre kolluk ve istihbarat faaliyetleri kapsamında devletlerin elinde halihazırda ulaşmak istedikleri amacı sağlayacak nitelik ve nicelikte araçlar mevcut olduğundan, ayrıca bir de veri lokalizasyonu politikası izlemek gerekli, ölçülü ve orantılı olmayacaktır.[25] Yerel firmalara ilişkin olarak devletlerin verilerin incelenmesine ilişkin yeterli kaynakları

[23] Atlı, "Kişisel Verilerin Önleyici…": 7.
[24] Singh, "A dissertation submitted…": 27.
[25] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*

olsa dahi yurt dışında bulunan verilerin incelenmesi hususunda uygulamada büyük problemlerle karşılaşılmaktadır. Bu noktada Brezilya'da 2006 yılında görülmüş bir davayı örnek göstermek yerinde olacaktır.[26] Davada federal mahkeme, Google'ın sahibi olduğu bir sosyal medya platformu olan Orkut'a çocuk pornografisinin yayılması ve uyuşturucu madde satılması suçlarından soruşturma yürütülen bir grup Brezilya vatandaşının verisini talep eden bir emir göndermiş, Orkut ise verilerin Brezilya'da değil yurt dışında tutulması sebebiyle paylaşım emrini reddetmiştir.[27] Her ne kadar sonrasında Google, Brezilya ile iş birliği yapmayı kabul etmiş olsa da ciddi nitelikteki soruşturmalarda bu şekilde verilen ret kararlarının veya süre kayıplarının ne kadar mühim olduğu düşünüldüğünde konunun önemi daha kolay anlaşılacaktır.

Chander ve Lê, verilerin yabancı bir ülkede olması halinde de devletlerin karşılıklı adli yardımlaşma (mutual assistance) yöntemini kullanabileceğini ve bu şekilde verilere erişebileceğini belirtmektedir.[28] Ancak yurt dışındaki verilere erişim talebi uzun bir bürokratik süreç içermekte, soruşturmaların aylar sürmesine ve dolayısıyla anlamını yitirmesine sebep olabilmektedir.[29] Özellikle kritik soruşturmalarda kolluk ve istihbarat kurumlarının verilere anlık ve kolay bir şekilde erişebilmesi gerekmekte ve literatürde iddia edilenin aksine veri lokalizasyonu bu durumu sağlamakta ve güçlendirmektedir.[30]

Diğer yandan, veri lokalizasyonu politikaları veriyi yalnızca bir bölgeye hapsederek demokrasiyi ve insan haklarını kısıtlayan bir dijital otoriterleşme aracı olarak kullanılabilir.[31] Ayrıca, veri lokalizasyonu politikalarının ülkeleri kara paranın aklanması gibi bazı suçlar için güvenli bölgeler halinde getirme riski bulunmaktadır.

---

[26] Ellen Nakashima, "Google to Give Data To Brazilian Court" *The Washington Post*, 2 Eylül 2006, https://www.washingtonpost.com/archive/business/2006/09/02/google-to-give-data-to-brazilian-court-span-classbankheadrequest-differs-from-uss-it-saysspan/f0b42222-f508-4185-a2b4-46d215decdf4/, (28.09.2024).
[27] Erika Morphy, "Google to Comply With Brazilian Court Order" *TechNewsWorld*, 5 Eylül 2006, https://www.technewsworld.com/story/google-to-comply-with-brazilian-court-order-52830.html, (28.09.2024).
[28] Chander ve Lê, "Data Nationalism": 724.
[29] Burman ve Sharma, *How Would Data…* 16.
[30] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, 2018, 85. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, (11.10.2024).
[31] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*

Şöyle ki; trafik verilerinin hiçbir koşulda yurt dışına çıkmayacağına ilişkin katı düzenlemeleri olan bir ülke, siber suçlar için bir cazibe merkezi haline gelebilir. Aynı zamanda genelleştirilerek uygulanan katı veri lokalizasyonu politikalarının, uygulayan ülkeyi dış dünyadan soyutlayacağını ve interneti çıkış mantığına aykırı bir hale getireceğini söylemek mümkündür.[32] Bu sebeplerle veri lokalizasyonu politikaları istenilen amacı sağlayacak ölçüde ve orantıda uygulanmalıdır. Veri lokalizasyonu politikaları tasarlanırken milli güvenliğe en çok zarar veren hususlar düşünülmeli ve lokalizasyon kuralları uygulanacak veriler için genetik, biyometrik, sağlık verileri ve kritik veriler gibi ayrımlara gidilmelidir.

6.3.3. Yabancı ülke istihbarat faaliyetlerinin engellenmesi

Ülkelerin veri lokalizasyon politikalarına yönelmelerinin en temel sebebinin yabancı ülke istihbarat faaliyetlerinin engellenmesi olduğu söylenebilir. Zira, dünya genelinde veri lokalizasyon politikalarının uygulanması Snowden'ın ifşaları sonrasında büyük bir artış göstermiştir. Amerikan Ulusal Güvenlik Kurumunda (*National Security Agency*) istihbarat görevlisi olarak çalışan Edward Snowden, 2013 yılında İngiliz The Guardian gazetesine sızdırmış olduğu belgelerle; Amerikan istihbaratının 35'ten fazla ülke liderini gözetlediğini ve Amerika Birleşik Devletleri içinde ve dışında sayısız kişinin kişisel verisini gizlice ele geçirdiğini ve incelediğini ortaya çıkarmıştır.[33] Bu olay, Birleşmiş Milletler de dahil olmak üzere uluslararası kuruluşlar ile devletleri harekete geçirmiş ve dünya genelinde kişisel verilerin korunmasına ve verilerin ülke içerisinde tutulmasına verilen önem artmaya başlamıştır.[34] Bunun sonucunda Avustralya, Fransa, Kanada, Malezya ve Brezilya başta olmak üzere birçok devlet veri lokalizasyonu politikası uygulamayı değerlendirmeye başlamıştır.[35]

---

[32] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair…* ,87.

[33] Gleen Greenwald vd., "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, 11 Haziran 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, (14.10.2024).

[34] Birleşmiş Milletler, *UN rights chief urges protection for individuals revealing human rights violations*, 12 Temmuz 2013. https://news.un.org/en/story/2013/07/444512, (21.10.2024).

[35] Jonah Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders" *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance* (2014): 3.

Literatürde veri lokalizasyonu politikalarının yabancı devletlerin istihbarat faaliyetlerini önleyip önleyemeyeceği sıklıkla tartışılan bir konudur. Bir görüşe göre istihbarat faaliyetleri yürüten ülkeler, bu faaliyetlerini zaten kendi ülkeleri dışında gerçekleştirdiğinden istihbarat faaliyetine konu olmamak için verilerin o ülke içerisinde transfer edilmesinden çekinmesine gerek yoktur.[36] Ancak, bir ülkedeki yabancı istihbarat faaliyetlerinin önlenmesi, o ülkenin kendi istihbaratının görevidir. Dolayısıyla önlenmesi gereken bir faaliyetin varlığını kabul ederek ona göre yasal düzenleme yapılması ise abesle iştigal olacaktır. Ayrıca, istihbarat faaliyeti yürüten ülkeler, kendi içerisindeki kaynaklara daha kolay nüfuz edebileceğinden; yukarıdaki görüş doğru olsa dahi verileri o ülkenin sınırları içerisine göndermek istihbarat faaliyetini kolaylaştıracaktır.

Bir diğer görüşe göre ise, verinin yerelleştirilmesi yabancı ülkelerin kötü amaçlı yazılımlar aracılığıyla istihbarat faaliyetlerini yürütmelerinden dolayı bu faaliyetleri önleyemeyecektir.[37] Ancak yukarıda da bahsedildiği gibi verilerin güvenliği verinin bulunduğu konumdan ziyade güvenliğin sağlanması için alınan önlemler ile sağlanmaktadır.[38] Verilerin güvenliğinin sağlanması için gerekli idari ve teknik tedbirlerin alınması durumunda, verinin bulunduğu konumun önemi olmayacaktır. Her ne kadar veri lokalizasyonu politikaları, yabancı ülkelerin politikanın düzenlendiği ülke içinde gerçekleştirdiği istihbarat faaliyetlerini önleyemese de; Snowden ifşalarındaki gibi olayların önüne geçilmesinde önemli bir araç olarak değerlendirilebilecektir.

6.3.4. Yerel ekonominin gelişmesi

Veri lokalizasyonu politikalarını savunan görüşlerin dayandığı temel noktalardan birisi de bu politikaların yerel ekonomiye katkıda bulunacağı tezidir. Veri lokalizasyonu politikaları, verilerin kuralların düzenlendiği ülke içerisinde tutulmasını ve depolanmasını öngöreceğinden; bu politikaların o ülke içerisinde yeni veri merkezlerinin kurulması, yeni iş pozisyonlarının oluşması, yerel endüstrinin gelişmesi, yerel işletmelerin rekabet imkanının artması ve ülkeye yeni yatırımların yapılması gibi

[36] Chander ve Lê, "Data Nationalism": 722.
[37] Ünver ve Kim, "Cross-Border Data Transfers…".
[38] Ünver ve Kim, "Cross-Border Data Transfers…".

birçok avantajı beraberinde getireceği iddia edilmektedir.[39] Bu çerçevede, veri lokalizasyonu düzenlemelerinin zorunlu kıldığı yükümlülüklerin özellikle modern, yüksek kapasiteli ve enerji verimliliği yüksek veri merkezlerinin kurulmasını hızlandırdığı; böylece hem bulut bilişim ekosisteminin hem de kritik dijital altyapı yatırımlarının ülke içinde yoğunlaşmasına katkı sunduğu ileri sürülmektedir.[40]

Yapılan bir araştırmaya göre verilerin uluslararası transferini zorlaştıran düzenlemeler ve genel olarak veri lokalizasyonu politikaları Amerika Birleşik Devletleri için gayrisafi yurt içi hasılada %0,1 ila 0,36 arası, diğer ülkeler için ise %0,7 ila 1,7 arası düşüşe sebep olmaktadır.[41] Özellikle yurt dışı merkezli şirketler için lokalizasyon politikası uygulanan ülkede veri merkezi kiralama veya kurma maliyetinin oldukça yüksek olması, personel istihdamının zor olması ve tecrübesiz personelin de eğitiminin uzun sürmesi, bu şirketleri yatırımdan uzaklaştırmaya sevk edebilecektir.[42] Bu sebeple yurt dışı merkezli şirketlerin o ülkeye yatırım yapmaktan kaçınması ise, vatandaşların teknolojiden ve diğer ülkelerde sağlanan birtakım imkanlardan mahrum kalmasına sebep olabilecektir.[43] Zira yabancı şirketler, söz konusu veri lokalizasyon kurallarına uyumun maliyeti ile gerçekleştirmeyi planladıkları yatırımın muhtemel gelirini karşılaştırarak yatırımdan vazgeçme yolunu tercih edebilmektedir.[44]

Bunlara karşılık olarak verinin yurt içinde depolanma şartının yerel işletmelere daha çok veriyi analiz edebilme, ekonomik büyüme ve büyük teknoloji firmalarıyla rekabet imkânı sağlayacağını ve özellikle küçük işletmeler için bilimsel inovasyonların daha kolay erişilebilir hale gelebileceğini öngören görüşler de mevcuttur.[45] Ancak, veri lokalizasyonu politikaları sonucunda oluşan faydaların sebep olunan ekonomik

---

[39] Martina F. Ferracane, "The Costs of Data Protectionism" *Big Data and Global Trade Law*, Mira Burri, (Londra: Cambridge University Press, 2021): 67.
[40] Shamel Azmeh ve Christopher Foster, "The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements" *Working Paper Series* 16, sy.175 (Ocak 2016): 28.
[41] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology & Innovation Foundation*, Mayıs 2017.
[42] Ünver ve Kim, "Cross-Border Data Transfers…".
[43] Chander ve Lê, "Data Nationalism": 727.
[44] Yatırım Ortamını İyileştirme Koordinasyon Kurulu, "Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi", Nisan 2022, https://www.akib.org.tr/files/downloads/2024/06/e53a2f00fc734de53a2f00fc734de53a2f00fc734de53a2f00.pdf, (17.05.2025).
[45] Burman ve Sharma, *How Would Data…* 17.

zararları karşılayamayacağını söylemek mümkündür.[46] Bu tartışmaya ülkemizden bir örnek olarak PayPal'ın Türkiye'den çekilmesi gösterilebilir. Bankacılık Düzenleme ve Denetleme Kurumu, 2016 yılında Paypal'ın lisans başvurusunu, ödeme kuruluşlarına ve elektronik para kuruluşlarının bilgi sistemlerine ilişkin mevzuatın öngördüğü kuruluşların sistemlerini Türkiye'de bulundurması zorunluluğuna uymadığı gerekçesiyle reddetmiştir.[47] Bunun üzerine PayPal, bu mevzuata uymaktansa Türkiye'deki faaliyetlerini durdurma kararı almış ve Türkiye'den çekilmiştir.

Tüm bunlar veri lokalizasyonu politikalarının uygulanmaması için bir sebep olarak görülmemeli, yalnızca bu politikaların kapsamının geniş tutulmaması konusunda gerekçe olarak düşünülmelidir. Zira, kamu düzeninin sağlanması için getirilen her kural, birtakım maliyetleri ve fırsat kayıplarını da beraberinde getirecektir.[48] Bu sebeple veri lokalizasyonu politikalarının ülkeyi ekonomik açıdan dezavantajlı bir duruma getiriyor olması, bu kuralların düzenlenmemesi gerektiği anlamına gelmemekte, sınırlarının belirlenmesine yardımcı olarak görülmesi gerektiği değerlendirilmektedir. Veri lokalizasyonunun ekonomik etkileri değerlendirilirken yalnızca maliyet unsurlarına odaklanmak yerine, bu politikaların uzun vadede ulusal veri merkezleri altyapısını güçlendirerek dijital egemenliği, veri güvenliğini ve teknolojik bağımsızlığı artırma potansiyelinin de dikkate alınması gerekmektedir.

6.4.Türkiye'de Veri Lokalizasyonu

6.4.1. Verilerin yurt dışına aktarılması

6.4.1.1. Kişisel verilerin yurt dışına aktarılması

Türkiye'de kişisel verilerin yurt dışına aktarılması hususu KVKK ve Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile düzenlenmektedir. 12 Mart 2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile KVKK'de kişisel verilerin yurt dışına aktarılması hususunda dönüm noktası olarak kabul edilebilecek değişiklikler gerçekleştirilmiştir. Bu konu ülkemizin

---

[46] Daniel Castro ve Alan Mcquinn, *Cross-Border Data Flows…*

[47] Sümeyye Dalkılınç, "'Kanuna uygun olmadığından PayPal'ın lisans başvurusu onaylanmadı'" *Anadolu Ajansı*, 2 Haziran 2016, https://www.aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825, (19.10.2024).

[48] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair…* ,88.

veri lokalizasyonu politikasının değerlendirilmesi açısından önem arz ettiğinden düzenleme değişiklik öncesi ve sonrası olmak üzere iki ayrı başlık altında incelenecektir.

6.4.1.1.1. Kişisel verilerin yurt dışına aktarılmasına yönelik eski düzenleme

Kişisel verilerin yurt dışına aktarılması, KVKK'nin 9'uncu maddesi ile düzenlenmektedir. Maddenin değişiklik öncesindeki hali;

"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 Türkiyedeki ve ilgili yabancı ülkedeki sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması,

kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir." şeklindeydi.

Söz konusu maddenin birinci fıkrasından da anlaşılacağı gibi değişiklik öncesinde kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılması yasaklanmıştı. Buna göre kural, kişisel verilerin yurt dışına aktarılamamasıyken, açık rıza ve kanunda tanımlanmış sınırlı şartlar bu kuralın istinası olarak belirlenmişti.

Bu düzenleme, her ne kadar kişisel verilerin yurt dışına aktarımı için farklı yöntemler öngörse de, uygulamada her kişisel veri aktarım faaliyeti için ilgili kişilerden açık rıza alınması yoluna başvurulması kişisel verilerin yurt dışına aktarımının de facto olarak yasaklandığı izlenimini oluşturuyor ve özellikle uluslararası şirketler için büyük problemler oluşturuyordu. GVKT'den oldukça farklılık arz eden bu düzenleme, ülkemizde neredeyse katı veri lokalizasyon uygulaması olarak yorumlanabilecek ağır bir veri yerelleştirme öngörüyordu. Maddenin ikinci fıkrasında düzenlenen yazılı taahhütname yönteminde ise; kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunmaması durumunda, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurulunun izninin bulunması şartıyla, kişisel verilerin açık rıza olmaksızın

yurt dışına aktarılmasına imkân tanınmaktaydı. Bu yöntem, teoride açık rıza alınmasına gerek kalmaksızın veri aktarımını mümkün kılsa da, Kurul nezdinde iznin alınması sürecinin uzun ve belirsiz olması sebebiyle uygulamada tercih edilmesi güçleşmekteydi. Nitekim, Kişisel Verileri Koruma Kurulunun 2023 yılına kadar yalnızca altı taahhütname başvurusunu onaylaması da yazılı taahhütname yolunu pratik hayatta işlevsiz duruma getiriyordu.[49] Veri sorumluları, yurt dışına veri aktarmak zorunda oldukları durumlarda dahi ilgili kişilerin açık rızalarının alınması yoluna başvuruyor ve bu durum da açık rızaların hukuka uygunluğunun sorgulanmasına sebep oluyordu.

Bu durum üzerine KVKK'nin 9'uncu maddesinde değişiklik yapılarak GVKT'deki yurt dışı aktarım düzenlemesine uyum sağlandı.

6.4.1.1.2. Kişisel verilerin yurt dışına aktarılmasına yönelik mevcut düzenleme

KVKK'nin mevcut 9'uncu maddesiyle, kişisel verilerin kural olarak yurt dışına aktarılmasının yasaklanmasından vazgeçilmiş, aktarım GVKT düzenlemesi ile uyumlu olarak birtakım şartlara bağlanmıştır. Buna göre kişisel veriler, aşağıdaki durum ve şartlar dahilinde yurt dışına aktarılabilmektedir.

6.4.1.1.2.1. Yeterlilik kararı

KVKK'nin 9'uncu maddesinin birinci fıkrasında; kişisel verilerin, 5'inci ve 6'ncı maddelerde belirtilen şartlardan birinin varlığı ve aktarımın yapılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar hakkında yeterlilik kararı bulunması halinde, veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabileceği hüküm altına alınmıştır.

Maddenin 2'nci ve 3'üncü fıkrasında ise yeterlilik kararı verilmesinin usul ve esasları düzenlenmiştir. Bu tezin yazıldığı tarih itibariyle henüz Kişisel Verileri Koruma Kurulu tarafından yeterlilik kararı verilen bir ülke bulunmamaktadır. Dolayısıyla mevcut koşullar altında bu fıkrada düzenlenen koşul ile yurt dışına kişisel veri aktarımı mümkün değildir.

---

[49] Elif Kösedağ, "KVKK Tarafından Yurt Dışına Kişisel Veri Aktarımları Onaylanan Şirketler", *KVKKHaber*, 28 Eylül 2023, https://www.kvkkhaber.net/onaylanan-yurt-disina-kisisel-veri-aktarimi-taahhutnameleri, (19.10.2024).

6.4.1.1.2.2. Uluslararası sözleşme niteliğinde olmayan anlaşma

KVKK'nin 9'uncu maddesinin dördüncü fıkrası; *"(4) Kişisel veriler, yeterlilik kararının bulunmaması durumunda, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, aşağıda belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir:*

a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi." hükmünü amirdir.

Bu yurt dışı aktarım şartı, yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan veri aktarımları için kullanılabilmektedir. Bu kurum ve kuruluşlar arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kişisel Verileri Koruma Kurulunun aktarıma izin vermesi halinde kişisel veriler aktarılabilmektedir.

6.4.1.1.2.3. Bağlayıcı şirket kuralları

KVKK'nin 9'uncu maddesinin dördüncü fıkrasının (b) bendine göre; *"...b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı"* halinde kişisel veriler yurt dışına aktarılabilmektedir. Bağlayıcı şirket kuralları aracılığıyla yurt dışı kişisel veri aktarımına izin verilmesi aslında kişisel veri koruma mevzuatında yeni bir yöntem değildir. Kişisel Verileri Koruma Kurumunun internet sitesinde 10 Nisan 2024 tarihinde yapılan duyuru ile, çok uluslu şirket toplulukları arasında yapılacak veri aktarımlarında bağlayıcı şirket kurallarının kullanılabileceği belirtilmiştir. Yine aynı duyuru ile bağlayıcı şirket kuralları, yeterli korumanın bulunmadığı ülkelerde faaliyet gösteren çok uluslu grup şirketleri için kişisel verilerin yurt dışına aktarımında kullanılan ve yeterli bir korumanın yazılı olarak taahhüt edilmesini sağlayan veri

koruma kuralları olarak tanımlanmıştır. KVKK'de yapılan son değişiklik ile bağlayıcı şirket kuralları kanunda da yurt dışı aktarım şartlarından birisi olarak yer bulmuştur.

6.4.1.1.2.4. Standart sözleşme

GVKT'de yer almasına rağmen hukukumuza KVKK'de yapılan son değişiklik ile yeni dahil edilen standart sözleşme yöntemi, KVKK'nin 9'uncu maddesinin dördüncü fıkrasının (c) bendinde, *"Kişisel veriler, yeterlilik kararının bulunmaması durumunda, 5 inci ve 6 ncı maddelerde belirtilen şartlardan birinin varlığı, ilgili kişinin aktarımın yapılacağı ülkede de haklarını kullanma ve etkili kanun yollarına başvurma imkânının bulunması kaydıyla, aşağıda belirtilen uygun güvencelerden birinin taraflarca sağlanması halinde veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilir:*

...

c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı.

..." düzenlemesi yer almaktadır. Buna göre, Kişisel Verileri Koruma Kurulu tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı halinde yurt dışına kişisel veri aktarımı yapılabilecektir. Kişisel Verileri Koruma Kurulu; veri sorumlusundan veri sorumlusuna, veri sorumlusundan veri işleyene, veri işleyenden veri işleyene ve veri işleyenden veri sorumlusuna aktarımlarda kullanılmak üzere dört farklı standart sözleşme yayınlamıştır.[50] Burada önemli olan husus, standart sözleşme yöntemi tercih edilerek kişisel verilerin yurt dışına aktarılmasında Kişisel Verileri Koruma Kurulunun ayrıca onay veya iznine ihtiyaç bulunmamasıdır. Aynı maddenin beşinci fıkrasındaki *"...(5) Standart sözleşme, imzalanmasından itibaren beş iş günü içinde veri sorumlusu veya veri işleyen tarafından Kuruma bildirilir."*

[50] Kişisel Verileri Koruma Kurulu tarafından yayınlanan standart sözleşmeler için bakınız: https://kvkk.gov.tr/Icerik/7929/Standart-Sozlesmeler.

şeklindeki hüküm ile standart sözleşmelerin imzalanmasından itibaren beş iş günü içerisinde veri sorumlusu veya veri işleyen tarafından Kişisel Verileri Koruma Kurumuna bildirilmesi zorunluluğu düzenlenmektedir. KVKK'nin 18'inci maddesinin birinci fıkrasına eklenen (d) bendi ile bu bildirim yükümlülüğünü yerine getirmeyenler hakkında 50.000 Türk Lirasından 1.000.000 Türk Lirasına kadar idari para cezası verileceğine hükmedilmiştir.

6.4.1.1.2.5. Yazılı taahhütname

Yazılı taahhütname yöntemi, bağlayıcı şirket kuralları gibi değişiklik öncesi KVKK'de halihazırda bulunan bir aktarım yöntemidir. KVKK'nin 9'uncu maddesinin dördüncü fıkrasının (ç) bendinde yer alan *"...ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi"* hükmüne göre yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kişisel Verileri Koruma Kurulu tarafından aktarıma izin verilmesi halinde yurt dışına kişisel veri aktarımı yapılabilecektir.

6.4.1.1.2.6. Arızi aktarım halleri

GVKT'de bulunup KVKK'de yapılan değişikliğe kadar hukukumuzda bulunmayan kişisel verilerin yurt dışına aktarılmasının şartlarından en önemlilerinden birisinin arızi aktarım halleri olduğu söylenebilir. KVKK'nin 9'uncu maddesinin altıncı fıkrası; *"...(6)Veri sorumluları ve veri işleyenler, yeterlilik kararının bulunmaması ve dördüncü fıkrada öngörülen uygun güvencelerden herhangi birinin sağlanamaması durumunda, arızi olmak kaydıyla sadece aşağıdaki hallerden birinin varlığı halinde yurt dışına kişisel veri aktarabilir:*

a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.

b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.

c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.

ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması…"

şeklindedir.

Son olarak, KVKK'nin 9'uncu maddesinin *"…(9)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. "* şeklindeki dokuzuncu fıkrası ile, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşünün alınması ve Kişisel Verileri Koruma Kurulunun izin vermesiyle kişisel verilerin yurt dışına aktarılabileceği düzenlenmiştir.

KVKK'de yapılan değişiklik ile, neredeyse katı veri lokalizasyonu politikası olarak değerlendirilebilecek kurallarda devrim niteliğinde güncellemeler yapılmış ve zorlaştırılmış veri aktarımı politikası benimsenmiştir. Kişisel verilerin kanundaki koşulların sağlanması şartıyla yurt dışına aktarılmasında bir engel kalmadığı, bu koşulların ise hayatın olağan akışına göre zorluk oluşturmayan, gerekli, ölçülü ve orantılı oldukları değerlendirilmektedir.

6.4.1.2. Telekomünikasyon Verilerinin Yurt Dışına Aktarılması

EHK'nin 51'inci maddesinin, *"…(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."* şeklindeki altıncı fıkrasına göre trafik ve konum verileri için ilgili kişilerin açık rızalarının alınması şartı

öngörülmüş ve diğer yurt dışı aktarım koşullarına başvurulamayacağı belirtilmiştir. Bu düzenleme ile, trafik ve konum verilerinin yurt dışı aktarımının diğer kişisel verilere göre zorlaştırılmasının amaçlandığı rahatlıkla söylenebilecektir. Ancak EHK'de ilgili kişilerin açık rızalarının alınması durumunda verilerin aktarılmasını kısıtlayan başkaca bir kural bulunmamaktadır.

Trafik ve konum verilerine ilişkin tek düzenleme elbette ki yalnızca EHK değildir. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in 5'inci maddesi ile kişisel verilerin işlenmesinde uyulması zorunlu olan ilkeler düzenlenmektedir. Söz konusu maddenin birinci fıkrasında KVKK'de de yer alan ilkeler tekrar edilirken, ikinci fıkrasındaki *"...(2) Milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmaması esastır."* şeklindeki hüküm ile milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmamasının esas olduğuna hükmedilmektedir. Söz konusu hüküm ile EHK'ye uygun olarak trafik ve konum verilerinin kural olarak yurt içinde kalması gerektiği belirtilmektedir. Yönetmelikte EHK'den farklı olarak burada korunan menfaatin mahremiyet yerine milli güvenlik olması ise dikkat çekicidir. Yönetmelik'in 8'inci maddesinin birinci fıkrasının (e) bendinde yer alan *"...e) Trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlar için;*

...

4) Üçüncü tarafın yurt dışında olması halinde verinin aktarılacağı ülkenin adı,

şeklindeki bilgiler verilerek ayrıca açık rıza alınır. Bu bilgilerde değişiklik olması halinde tekrar açık rıza alınır." şeklindeki hüküm ile; trafik ve konum verilerinin üçüncü taraflara aktarımında, üçüncü tarafın yurt dışına olması halinde aktarılacak ülkenin adının da ilgili kişiye yapılan bilgilendirme içerisinde yer alması gerekliliği düzenlenmektedir.

6.4.2. Genel aktarım kuralları dışındaki veri lokalizasyonu düzenlemeleri ve değerlendirilmesi

6.4.2.1. Cumhurbaşkanlığı mevzuatı

6.4.2.1.1. 2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi

Kritik altyapılarda gerçekleşen güvenlik riskleri; kamu hizmetinin aksaması, kamu düzeninin bozulması ve milli güvenliğin sağlanmasında tehdit oluşturması gibi olumsuz etkilere sebep olabileceğinden bu riskleri azaltacak veya ortadan kaldıracak tedbirlerin uygulanması büyük bir önem arz etmektedir. Bu beisle, dijital ortamda karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla alınan tedbirleri açıklamak üzere 06 Temmuz 2019 tarihli ve 30823 sayılı Resmî Gazete'de yayımlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi uygulamaya konulmuştur. Genelgenin 1'inci maddesinde yer alan, "*Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır."* şeklindeki hüküm ile belirli türden verilerin yurt içinde saklanması, 3'üncü maddesinde yer alan, "*Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır."* şeklindeki hüküm ile verilerin yerli hizmet sağlayıcılar dışındaki bulut depolama hizmetlerinde saklanamayacağı, 20'nci maddesindeki, "*Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmecilerin Türkiye'de internet değişim noktası kurmakla yükümlü olduğu, yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır."* hükmü ile de işletmecilerin Türkiye'de internet değişim noktası kurmakla yükümlü olduğu, yurt içinde değiştirilmesi gereken yurt içi iletişim trafiğinin yurt dışına çıkarılmaması hususları düzenlenmiştir.

Genelgenin 1'inci maddesiyle düzenlenen nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve kritik türdeki verilerin Türkiye'de depolanmasına ilişkin düzenleme; bir aktarım yasağından çok, bilgilerin ve verilerin ya da yedeklerinin Türkiye'de de depolanması yükümlülüğü olarak yorumlanmaktadır.[51] Dolayısıyla bu düzenlemenin bir yumuşak veri lokalizasyonu olduğunu söylemek mümkündür. Aynı şekilde kamu

[51] Begüm Yavuzdoğan Okumuş ve Yalçın Umut Talay, "Verilerin Türkiye'de Depolanması Yönünde Gelişmeler", *Gün+ Partners Avukatlık Bürosu*, Mayıs 2021.

kurum ve kuruluşlarına ait verilerin kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmamasına ilişkin yükümlülük de bu kapsamda değerlendirilebilir. Nitekim söz konusu düzenleme ile bu verilerin aktarımına ilişkin bir hüküm öngörülmemekte, verilerin yalnızca depolanması kapsam içine alınmaktadır. Ancak her ne kadar bu yükümlülük kamu kurum ve kuruluşları ile sınırlı tutulsa da, kamu kurum ve kuruluşlarına ürün ve hizmet sunan özel hukuk kişilerini de kapsayacağı unutulmamalıdır.[52]

Ayrıca Genelgenin 4'üncü maddesindeki "*Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır."* hükmü, 6'ncı maddesindeki "*Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir."* hükmü ve 11'inci maddesindeki "*Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır."* hükmü ile özellikle kamu kurum ve kuruluşlarında yerli ve milli uygulama ile sistemlerin teşvik edilmesi ve hatta kullanılma zorunluluğu getirilmektedir. Yabancı uygulama ve sistemlerin kullanımı sonucunda bu uygulama ve sistemlerin sunucularının yurt dışında olması gibi sebeplerle verilerin yurt dışına aktarılması ve yurt dışı aktörlerince hukuka aykırı şekilde erişilmesi riskleri meydana geldiğinden, bu düzenlemelerin de bu risklerin önüne verilerin Türkiye'de kalmasını amaçlayarak geçmeye çalıştığı söylenebilecektir. Dolayısıyla bu uygulamalar da bir veri lokalizasyonu politikası olarak değerlendirilebilir.

6.4.2.1.2. Bilgi ve İletişim Güvenliği Rehberi

Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi kapsamında kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken Bilgi ve İletişim Güvenliği Rehberinin hazırlık çalışmaları, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda tamamlanmış

[52] Okumuş ve Talay, "Verilerin Türkiye'de Depolanması…"

ve rehber 24 Temmuz 2020 tarihinde onaylanmıştır.[53] Rehber, bilgi sistemlerinde gerçekleşebilecek güvenlik risklerinin azaltılması ve etkisiz kılınması ile milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik altyapı verilerinin güvenliğinin sağlanması amacıyla, tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde bulunan bilgi sistemlerinde uyulması zorunlu olan tedbirleri düzenlemektedir.[54] Bu noktada belirtmek gerekir ki; 19 Mart 2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ile birlikte, Dijital Dönüşüm Ofisinin bu alana ilişkin görev ve yetkileri Siber Güvenlik Başkanlığı tarafından yürütülmek üzere yeniden düzenlenmiş ve ülkemizin siber uzaydaki milli gücünü oluşturan tüm unsurlara yönelik tehditlerin tespit edilmesi ve önlenmesi amacıyla stratejik siber güvenlik politikalarının oluşturulması ve kritik altyapıların korunmasına yönelik koordinasyonun sağlanması gibi görevler de Başkanlığın sorumluluk alanına alınmıştır.

"*E-Posta Eklerinin Kum Havuzlarında Çalıştırılması*" adlı 3.1.4.19 numaralı tedbir ile; *Kuruma dışarıdan gelen e-posta eklerinin çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmesi, bu aşamadan sonra hala kategorilendirilmemiş e-posta eklerinin kum havuzunda çalıştırılması ve kum havuzu çözümlerinde dosyaların yurt içinde yerleşik olan sunucularda taranması* gerektiği düzenlenmektedir.

"*Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması*" adlı 3.2.7.2 numaralı tedbir ile; Kurumların kendi özel sistemleri veya yurt içinde yerleşik kurum kontrolündeki hizmet sağlayıcılar hariç olmak üzere kurumsal kritik verilerin saklanması/depolanması amacıyla bulut depolama hizmetleri kullanılmaması gerektiğine hükmedilmektedir. "*Bulut Hizmeti Kullanımı*" adlı 4.3.1.1 numaralı tedbirde ise kritik verilerin yurt içinde depolandığının ve yurt dışında barındırılmayacağının garanti altına alınması gerektiği, Kurumlara ait özel bulut

[53] Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, *Bilgi ve İletişim Güvenliği Rehberi*, 2020. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, (03.10.2024).
[54] Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, *Bilgi ve İletişim Güvenliği Rehberi*.

sistemleri haricinde, bulut servis sağlayıcılardan yer, sunucu veya servis tabanlı bulut hizmeti kullanılacaksa,

- Erişen personel, yetki ve yetkinlik düzeylerinin,
- Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesinin,
- Güncelleme durum alarmlarının,
- Siber olay alarmlarının,
- Performans ve kapasite göstergelerinin kurum tarafından kontrol edilmesi gerektiği düzenlenmiştir.

Bu hükümden kritik verilerin yurt dışına barındırılmaması gerektiği açıkça anlaşılmaktadır. Düzenlemenin bu haliyle bir veri lokalizasyonu kuralı olduğu belli olsa da hangi veri lokalizasyonu türünün benimsendiği ilgili mevzuatın incelenmesiyle anlaşılabilecektir.

Benzer şekilde "*Bulut Ortamı Güvenliği*" adlı 4.3.1.7 numaralı tedbirle operatörler tarafından sunuculara erişimde trafiğin yurt içinde kalmasına yönelik tedbirlerin uygulanması gerektiği belirtilmektedir. Ayrıca, "*İnternet Değişim Noktası*" başlıklı ve 4.5.3.13 numaralı tedbire göre yurt içi iletişim trafiğinin ülke sınırları içerisinde kalması sağlanmalı, bu trafiğin ve abone kayıtlarının yurt dışına çıkarılarak tekrar yurt içine yönlendirilmesi engellenmelidir. 4.3.1.1 numaralı tedbirden farklı olarak 4.5.3.13 numaralı tedbirde, iletişim trafiği ve abone kayıtlarının yurt dışına çıkarılarak tekrar yurt içine yönlendirilmesinin engellenmesi gerektiği belirtilmektedir. Tedbirlerin lafzından bu verilerin hiçbir koşulda yurt dışına çıkarılamamasının düzenlendiği açıktır. Ancak bu düzenlemede benimsenen veri lokalizasyonu türünün tespiti için yurt dışından erişim olanağı olup olmadığı veya vatandaşların açık rızası ile verilerin aktarılıp aktarılamadığı incelenmeli, dolayısıyla ilgili mevzuat araştırılmalıdır. Mevzuat araştırmasına aşağıda yer verildiğinden, bu kısımda detaylı inceleme yapılmayacaktır.

Rehberin "Açık Rıza Yönetimi" başlıklı bölümünde kişisel verilerin işlenmesi amacıyla açık rıza alınması gerekli durumlara ilişkin de ayrıca tedbirler düzenlenmiştir. "*Açık Rıza Unsurlarının Belirlenmesi*" başlıklı 4.1.7.1 numaralı tedbire göre, kişisel verilerin yurt içi veya yurt dışı aktarımı söz konusu ise bu husus

açık rıza metninde ifade edilerek ayrı bir bölüm halinde düzenlenmeli ve ilgili kişilerden ayrı bir açık rıza alınmalıdır. Son olarak Rehberde, ihtiyaç duyulan güvenlik gereksinimlerinin ve iletişim ihtiyacının karşılanması için yerli ve milli ürünlerin tercih edilmesi gerektiği belirtilmektedir. Örneğin, "*Mesajlaşma Uygulaması Seçimi*" başlıklı 4.2.1.1 numaralı tedbire göre, kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan mesajlaşma uygulamaları kullanılmalıdır. Kurumun kendine ait bir haberleşme uygulaması yoksa mesajlaşma amacıyla sunucuları yurt içinde bulunan yerli ve milli uygulamalar tercih edilmelidir.

6.4.2.2. Sağlık sektörü düzenlemeleri

Sağlık Bilgi Sistemleri Uygulamaları Hakkında 2015/17 sayılı Genelge ile sağlık bilişimi alanında faaliyet gösteren tedarikçiler ile tüm kamu ve özel sağlık kurum ve kuruluşlarının uyması gereken kurallar ile sağlık bilişimi konusunda izlenmesi gereken yol haritasının açıklanması amaçlanmaktadır. Genelge'nin 2.7. maddesinde *"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."* düzenlemesi yer almaktadır. Ayrıca Genelgenin 5.1.10. maddesiyle sağlık bilişimi uygulama yazılımlarının süreç, fonksiyon, güvenlik, ara yüz standartlarının ülkemiz şartları ve uluslararası standartlar çerçevesinde geliştirilmesi ve bu standartlara uygunluk denetim ve sertifikasyon çalışmalarının yapılması adına birtakım standart ve kurallar belirlenmiştir.

6.4.2.3. Sermaye piyasası düzenlemeleri

Sermaye piyasasının güvenilir, şeffaf, etkin, istikrarlı, adil ve rekabetçi bir ortamda işleyişinin ve gelişmesinin sağlanması, yatırımcıların hak ve menfaatlerinin korunması için sermaye piyasasının düzenlenmesi ve denetlenmesi amacıyla 6362 sayılı Sermaye Piyasası Kanunu (SPK) düzenlenmiştir. Kanunun 35'inci maddesi ile faaliyette bulunabilecek sermaye piyasası kurumları belirtilmiştir ve (h) bendiyle veri depolama kuruluşları bu kurumlar arasında gösterilmiştir.

SPK'nin 87'nci maddesinin birinci fıkrası, *"...1) Sistemik riskin gözetimi ve finansal istikrarın korunması amacıyla, Kurul, sermaye piyasasında gerçekleştirilen işlemlere ilişkin olarak, bu işlemleri gerçekleştirenlerden, bu işlemlere ilişkin bilgilerin,*

belirleyeceği şekil ve içerikte, doğrudan kendisine veya yetkilendireceği bir veri depolama kuruluşuna bildirmesini isteyebilir. Bu madde kapsamında, bildirim yapmakla yükümlü olanlar, özel mevzuatındaki gizlilik ve sır saklama yükümlülüklerini ileri sürerek talep edilen bilgileri vermekten imtina edemez." hükmünü amirdir. Aynı maddenin üçüncü fıkrasında *"...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."* hükmüne yer verilmiştir. Burada, veri depolama kuruluşlarına ilişkin bilgilerin aktarımına ayrıca bir de Sermaye Piyasası Kurulunun onayı şartı getirilmiştir. Başka bir deyişle ilgili verilerin saklanmasına veya erişimine ilişkin bir düzenleme getirilmemekte, yalnızca Kurul onayı şartı eklenerek aktarım zorlaştırılmaktadır. Dolayısıyla bu düzenlemenin zorlaştırılmış veri aktarımı olduğunu söylemek mümkündür.

Ayrıca bazı kurum, kuruluş ve ortaklıkların bilgi sistemlerinin yönetimine ilişkin usul ve esasları belirlemek için Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) hazırlanmış ve Tebliğ, 05 Ocak 2018 tarihli ve 30292 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Tebliğ'in 4'üncü maddesinin birinci fıkrasının (a) bendiyle birincil sistemler, "…*a) Kurum, kuruluş ve ortaklıkların SPK'dan ve SPK'ya ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmeleri için gerekli bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkan sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı…"* olarak, (g) bendiyle de ikincil sistemler, *"...g) birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve SPK'da ve SPK'ya ilişkin alt düzenlemelerde kurum, Kuruluş ve Ortaklıklar için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistem yedekleri…"* olarak tanımlanmıştır. Tebliğ'in *"Bilgi sistemleri sürekliliği"* başlıklı 26'ncı maddesinin birinci fıkrasında *"...(1) Kurum, kuruluş ve ortaklıkların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur."* hükmü yer almıştır. Bu hüküm ile hedeflenen amacın, Tebliğin 4'üncü maddesinde yer verilen birincil ve

ikincil sistemlerin tanımlarıyla birlikte değerlendirildiğinde; bu sistemlerde yer alan bilgilere kesintisiz ve istenildiği an ulaşılabilmesi olduğu görülmektedir. Ayrıca sistemlerin yurt içinde bulundurulması zorunlu tutulurken, yurt dışı aktarımına ilişkin ayrıca bir husus düzenlenmemiştir. Dolayısıyla buradaki kuralın da bir yumuşak veri lokalizasyonu düzenlemesi olduğu değerlendirilmektedir.

6.4.2.4. Bankacılık ve finans sektörü düzenlemeleri

6.4.2.4.1. 5411 sayılı Bankacılık Kanunu

01 Kasım 2005 tarihli ve 25983 mükerrer sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 5411 sayılı Bankacılık Kanunu; finansal piyasalarda güven ve istikrarın sağlanmasına, kredi sisteminin etkin bir şekilde çalışmasına, tasarruf sahiplerinin hak ve menfaatlerinin korunmasına ilişkin usul ve esasları düzenlemektedir. Kanunun "*Sırların saklanması*" başlıklı 73'üncü maddesinin üçüncü fıkrasındaki; "…*Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. 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."* hükmü ile bu Kanun, Bankacılık Düzenleme ve Denetleme Kuruluna, ekonomik güvenliğe ilişkin yapacağı değerlendirmeler sonucunda müşteri sırrı ya da banka sırrı niteliğinde olan her türlü veri için veri lokalizasyonu kurallarını uygulayabilme yetkisini vermiştir.

Buna ek olarak; 15 Mart 2020 tarihli ve 31069 sayılı Resmî Gazete'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik; bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin

yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerini düzenlemektedir. Yönetmelik'in 10'uncu maddesinin birinci fıkrası, *"...(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 yurtiçindeki ve yurtdışındaki üçüncü kişilerle paylaşamaz ve bunlara aktaramaz.*" hükmünü içermektedir. Bu düzenleme ile, veri aktarımının yapılabilmesi için ayrıca bir şart daha tanımlanarak zorlaştırılmış veri aktarımı politikası benimsenmiştir.

Yönetmeliğin "*Birincil ve ikincil sistemler*" başlıklı 25'inci maddesi;

"(1) Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Birincil sistemlerin kaçıncı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve birinci fıkra hükmüne tabidir.

...

(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." hükmünü haizdir.

Bu madde uyarınca birincil, ikincil sistemler ve bu sistemler ile sürdürülen hizmetin yürütülmesinde kullanılan bilgi sistemleri ve bunların yedekleri yurt içinde bulundurulmalıdır. Sermaye piyasası mevzuatıyla benzer olarak burada hedeflenen amacın bu sistemlerde yer alan bilgilere kesintisiz ve istenildiği an ulaşılabilmesi olduğu açıktır. Ayrıca sistemlerin yurt içinde bulundurulması zorunlu tutulurken, yurt dışı aktarımına ilişkin bir husus düzenlenmemiştir. Dolayısıyla buradaki kuralın da bir yumuşak veri lokalizasyonu düzenlemesi olduğu değerlendirilmektedir.

6.4.2.4.2. 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun

27 Haziran 2013 tarihli ve 28690 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun; ödeme ve menkul kıymet mutabakat sistemlerine, ödeme hizmetlerine, ödeme kuruluşlarına ve elektronik para kuruluşlarına ilişkin usul ve esasları düzenlemektedir. Bu Kanun'un 3'üncü maddesinin birinci fıkrasının (z) bendiyle sistem, ödeme sistemi ve menkul kıymet mutabakat sistemi; (aa) bendiyle sistem işleticisi, sistemin günlük işleyişinden sorumlu olan ve sistem işletimi için gerekli olan faaliyet iznine sahip tüzel kişi olarak tanımlanmıştır. Kanun'un "*Belge ve kayıtların saklanması ile kişisel bilgilerin korunması, değişikliklerin bildirilmesi*" başlıklı 23'üncü maddesinin birinci fıkrası, "*...(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. Ödeme kuruluşu ve elektronik para kuruluşunun faaliyetlerini yürütmede kullandıkları bilgi sistemlerine ilişkin usul ve esaslar Bankaca belirlenir."* hükmünü içermektedir. Bu düzenleme ile sistem işleticilerine faaliyetlerini yürütürken kullandığı bilgi sistemleri ve bunların yedeklerinin yurt içinde tutulması zorunluluğu getirilmiş, verilerin aktarımına ilişkin bir hükme yer verilmemiştir. Ancak kanun koyucu verilerin yedekleriyle birlikte Türkiye'de tutulma zorunluluğu ile, yumuşak veri lokalizasyonuna göre daha ağır bir politika benimsemiştir. Bu doğrultuda buradaki düzenlemenin bir karma veri lokalizasyonu olduğu değerlendirilmektedir.

6.4.2.5. Hazine ve Maliye Bakanlığı

6.4.2.5.1. Vergi Usul Kanunu Genel Tebliği (Sıra No: 509)

19 Ekim 2019 tarihli ve 30923 sayılı Resmî Gazete'de yayımlanan Vergi Usul Kanunu Genel Tebliği (Sıra No: 509); Vergi Usul Kanunu uyarınca düzenlenmesi zorunlu olan belgelerin elektronik ortamda düzenlenmesine yönelik usul ve esasları belirlemektedir. Tebliğin V.1.2 maddesinin yedinci fıkrasındaki; *"...(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."* hükmü ile aynı Tebliğin VI. maddesinin dördüncü fıkrasındaki *"...(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.*" hükümlerine bakıldığında yumuşak veri lokalizasyonu politikasının benimsendiğini söylemek mümkündür. Burada son hükümde, e-Belgelerin muhafazasının ülkemiz sınırları içerisinde yapılmasının zorunlu olduğu, ancak bu zorunluluğun yurt dışında ikincil bir arşivleme yapılmasına engel teşkil etmeyeceğinin düzenlenmesi; yumuşak veri lokalizasyonu politikasının benimsendiğinin vurgulanması açısından ayrıca önem arz etmektedir.

6.4.3. BTK Mevzuatı

6.4.3.1. 5809 sayılı Elektronik Haberleşme Kanunu

EHK'nin *"Kişisel verilerin işlenmesi ve gizliliğin korunması"* başlıklı 51'inci maddesinin altıncı fıkrasında veri yerelleştirme konusunda düzenleme yapılmış olup kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümlerinin saklı kalması kaydıyla, trafik ve konum verilerinin ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabileceği hüküm altına alınmıştır. Hükümden de anlaşılacağı gibi; EHK ile verilerin saklanması ve işlenmesi veya verilere erişilmesi

konusunda gerçek anlamda bir lokalizasyon kuralı belirlenmemiş, yalnızca yurt dışı aktarımına yönelik ilgili kişilerin açık rızalarının alınması şartı düzenlenmiştir. Bu doğrultuda, söz konusu düzenlemede zorlaştırılmış veri aktarımı politikasının benimsendiği değerlendirilmektedir.

6.4.3.2. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

23 Mayıs 2007 tarihli ve 26530 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 sayılı Kanun); içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektedir. Kanunun 2'nci maddesinin birinci fıkrasının (s) bendiyle sosyal ağ sağlayıcısı, sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır. Aynı Kanunun ek madde 4'ün altıncı fıkrasındaki *"...(6) 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."* hükmü ile telekomünikasyon verileri ve haberleşme alanında işlenen kişisel veriler kapsamında veri yerelleştirme konusunda düzenleme yapılmıştır.

6.4.3.3. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik

4 Aralık 2020 tarihli ve 31324 sayılı Resmî Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik, Bilgi Teknolojileri ve İletişim Kurumu tarafından özel hayatın gizliliği ile kişi temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve

esasları belirlemek amacıyla hazırlanmıştır. Yönetmelik'in *"İlkeler"* başlıklı 5 inci maddesinin ikinci fıkrasında *"...(2)Milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmaması esastır."* hükmü, *"Açık rıza alma şartları"* başlıklı 8 inci maddesinin birinci fıkrasının (e) *bendinde "...4) Üçüncü tarafın yurt dışında olması halinde verinin aktarılacağı ülkenin adı, şeklindeki bilgiler verilerek ayrıca açık rıza alınır.*" hükmü yer almıştır. EHK ile uyumlu olarak, bu Yönetmelikte de zorlaştırılmış veri aktarımı politikasının benimsendiği söylenebilecektir.

6.4.3.4. Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik

23 Ocak 2004 tarihli ve 25355 sayılı Resmî Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın hukuki ve teknik yönleri ile kullanımına ilişkin esaslar düzenlenmektedir.

Elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenlemek için ise BTK tarafından hazırlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik 15 Ekim 2021 tarihli ve 31629 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmelik'in *"İmza oluşturma ve doğrulama verileri"* başlıklı 18'inci maddesinin birinci fıkrasında *"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."* hükmü yer almıştır. Buna göre Elektronik Sertifika Hizmet Sağlayıcıları; imza oluşturma verisi, imza doğrulama verisi ve elektronik sertifika verilerini Türkiye'de oluşturmak; imza oluşturma verisini de hiçbir şekilde Türkiye dışına çıkarmamak zorundadır. İmza doğrulama verisi ve elektronik sertifikanın yalnızca ülkemiz içerisinde üretilebileceği, ancak Türkiye dışına çıkarılabileceği söylenebilecektir. Bu doğrultuda imza doğrulama verisi ile elektronik sertifika bakımından yumuşak veri lokalizasyonu kuralının benimsendiği söylenebilir. Ancak; imza oluşturma verisinin hem Türkiye'de oluşturulması hem de hiçbir koşulda Türkiye dışına çıkarılmaması gerekmektedir. Bu beisle imza oluşturma verisinin Türkiye dışına çıkarılmadan yurt dışında işlenmesi

hala imkân dahilinde olduğundan, bu kuralın karma veri lokalizasyonu olduğunu söylemek mümkündür.

6.4.3.5. Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik

25 Ağustos 2011 tarihli ve 28036 sayılı Resmî Gazete'de yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, kayıtlı elektronik posta sisteminin hukukî ve teknik yönleri ile işleyişine ilişkin usul ve esasları düzenlemektedir. Yönetmeliğin 4'üncü maddesinin birinci fıkrasının;

(i) bendiyle kayıtlı elektronik posta (KEP*), "...elektronik iletilerin, gönderimi ve teslimatı da dahil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şekli,"*

(j) bendiyle kayıtlı elektronik posta hizmet sağlayıcısı (KEPHS*), "...13/1/2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu kapsamındaki yetkilendirme çerçevesinde KEP sistemi kurmak ve işletmek için kurulan anonim şirket ile başvuru yapması ve gerekli koşulları sağlaması hâlinde 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanununun hükümlerine göre elektronik ortamda tebligat yapmaya yetkili kılınmış idare,"*

(k) bendiyle KEP delili, *"...belirli bir işlemin belirli bir zamanda meydana geldiğini gösteren, KEP sisteminde üretilen ve KEPHS'nin işlem sertifikası ile imzalanmış veri,"*

(l) bendiyle KEP hesabı, *"...Orijinal ileti gönderme ve alma ile KEP iletisi alma yeteneğine sahip KEP sisteminde oluşturulan elektronik posta hesabı,"*

(m) bendiyle KEP iletisi, *"...KEP sistemi içerisinde KEPHS tarafından üretilen KEP delilini içeren ve KEPHS'nin işlem sertifikası ile imzalanmış ileti,"*

(n) bendiyle KEP rehberi, *"...KEP hesabı bilgilerinin doğruluğunun ve güncelliğinin sorgulanabilmesi amacıyla işletilen bilgi ve sorgu sistemi,"*

(o) bendiyle KEP sistemi, *"...elektronik iletişim platformları aracılığıyla gerçekleşen, gönderildi ve alındı onayları da dâhil olmak üzere KEP iletilerinin tüm süreçlerine ilişkin olarak KEP delili oluşturulması, güvenli bir şekilde kimlik tespiti yapılması,*

KEP hesabı, KEP rehberi ve arşiv hizmetleri verilmesi gibi işlevlere sahip sistem," olarak tanımlanmıştır.

Yönetmeliğin "*KEPHS'nin yükümlülükleri*" başlıklı 16'ncı maddesi ile kayıtlı elektronik posta hizmet sağlayıcısının yükümlülükleri sayılmış olup maddenin (l) bendindeki "*KEP sistemine ilişkin ana ve yedek sistemlerini Türkiye Cumhuriyeti sınırları içerisinde bulundurmak*" hükmü ile KEP sistemine ilişkin sistemler hakkında yumuşak veri lokalizasyonu politikasının benimsendiği değerlendirilmektedir. Bu veri lokalizasyonu kuralına yukarıda tanımlarına yer verilen KEP delili, KEP hesabı, KEP iletisi ve KEP rehberi KEP sisteminde yer alan tüm işlev ve veriler dahil olacaktır.

6.4.3.6. 112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call) Konulu Kurul Kararı (2018/DK-YED/27)

Bilgi teknolojileri ve iletişim sektöründe yaşanan gelişmelerin kişisel güvenlik, siber güvenlik ve milli güvenlik risklerini de beraberinde getirmesi, ayrıca Acil Çağrı Merkezinden e-Call çağrısı başlatan numaranın geri aranması ihtiyacı halinde yabancı operatörler üzerinden yapılacak bağlantı sürecinde aksaklıkların yaşanabilmesi hususlarındaki risklerin bertaraf edilmesi amacıyla Bilgi Teknolojileri ve İletişim Kurulu tarafından 22 Ocak2018 tarihli, 2018/DK-YED/27 sayılı ve "112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call)" konulu karar alınmıştır. Kararın 2'nci maddesiyle*; "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 eCall ile birlikte katma değerli hizmet sunumuna imkan sağlayan haberleşme sistemlerinde; SIM kart, eSIM kart veya SIM kart özelliğini taşıyan bir modül vb. kullanılması halinde, söz konusu SIM kartların, eSIM kartların veya SIM kart özelliğini taşıyan modül vb.nin ülkemizde mobil elektronik haberleşme hizmeti sunmak üzere yetkilendirilmiş işletmecilerden temin edilmesi veya söz konusu işletmeciler tarafından kontrol edilebilecek şekilde programlanabilir olması…"* zorunlu tutulmuştur. Başka bir deyişle, ülkemizde kullanılacak araçlardaki eCall ve diğer katma değerli hizmetlerin sunumuna imkân sağlayan haberleşme sistemlerinde SIM kart vb. modüllerin yerli işletmecilerden temin edilmesi gerekmektedir. Kararın bu maddesi ile, ülkemizde kullanılacak araçların üreticisi firmanın merkezi nerede olursa olsun haberleşme hizmetini Türkiye'de yerleşik bir

işletmeciden sağlaması gerekliliği düzenlenmiştir. Böylece, hem kritik altyapı olarak kabul edilen haberleşme/iletişim sektörüne ilişkin verilerin Türkiye'de kalması hem de kritik altyapıda faaliyet gösterecek işletmecilerin yalnızca BTK tarafından yetkilendirilmiş hizmet sağlayıcılardan birisi olmasının sağlanması amaçlanmıştır.

Kurul Kararı'nın 3'üncü maddesi ise, "*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…"* hükmünü içermektedir. Açıklamak gerekirse bu madde doğrultusunda, bağlantılı araçlardaki e-Call ve katma değerli hizmetlerin sunumuna imkân sağlayan haberleşme sistemlerinde hizmet verecek sunucular Türkiye'de bulunmalı ve bu sistemdeki kişisel veriler ilgili kişilerin açık rızası olmaksızın yurt dışına çıkartılmamalıdır.

Her iki madde de incelendiğinde; verilerin Türkiye'de depolanmasının ve yerli işletmecilerden hizmet alınmasının şart koşulduğu ve ilgili kişinin açık rızası olmaksızın kişisel verilerinin yurt dışına çıkarılmaması gerektiği görülmektedir. Bu sebeple bu düzenlemelerin karma veri lokalizasyonu politikası benimsenerek oluşturulduğu söylenebilir. Ancak; bağlantılı araçlardaki haberleşme hizmeti kapsamında işlenen kişisel verilerin yalnızca ilgili kişilerin açık rızası ile yurt dışına aktarılabilmesinin zorlaştırılmış veri aktarımı kuralı olduğu değerlendirilmektedir.

6.4.3.7. Uzaktan Programlanabilir SIM Teknolojileri (eSIM) Konulu Kurul Kararı (2019/DK-TED/053)

eSIM teknolojilerine yönelik olarak; yenilikçi teknolojilerin ülkemize kazandırılması, bilgi ve haberleşme teknolojilerinde etkin rekabetin sağlanması, abone değişimi sürecinde yaşanabilecek olası sorunların en aza indirilebilmesi, tüketici haklarının ve kişisel verilerin korunması, siber güvenliğin azami seviyede sağlanması, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla

mevzuatın öngördüğü tedbirlerin alınması, işletmecilerin elektronik haberleşme sistemleri üzerinden ilgili kanunlarda getirilen düzenlemelere yönelik elektronik haberleşme sistemlerinin kurulması amaçlarıyla Bilgi Teknolojileri ve İletişim Kurulu tarafından 12 Şubat 2019 tarihli, 2019/DK-TED/053 sayılı ve "Uzaktan Programlanabilir SIM Teknolojileri (eSIM)" konulu Kurul Kararı alınmıştır. Kurul Kararı'nın 1'inci maddesiyle*; "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 sağlanmasına…"* karar verilmiştir. Bu madde ile, 2018/DK-YED/27 sayılı Kurul Kararı ile uyumlu olarak; hem kritik altyapı olarak kabul edilen haberleşme/iletişim sektörüne ilişkin verilerin Türkiye'de kalması hem de kritik altyapıda faaliyet gösterecek işletmecilerin yalnızca BTK tarafından yetkilendirilmiş hizmet sağlayıcılardan birisi olmasının sağlanması amaçlanmıştır.

Kurul Kararı'nın 2'nci maddesiyle, *"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 işletmeci tarafından veya tüm sorumluluk işletmeciye ait olmak üzere işletmecilerin 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 kurulmasına…" karar verilmiştir. Bu karar ile, eSIM süreçlerine yönelik olarak kullanılan sunucular, veri merkezleri, yazılımlar ve ekipmanlar da dahil tüm yapı, sistem ve depolama birimlerinin ülkemiz sınırları içinde tesis edilmesi ve tüm verinin ülkemiz sınırları içerisinde tutulmasına hükmedilmiştir.

Kurul Kararı'ndaki maddeler çerçevesinde; eSIM teknolojisine ilişkin verilerin yurt dışında işlenmesi veya yurt dışına aktarılması ile ilgili yasaklayıcı bir düzenleme bulunmadığı, ancak verilerin Türkiye'de depolanması ve eSIM süreçlerinde yerel işletmecilerden hizmet alınması gerektiği değerlendirilmektedir. Tüm bunlar birlikte değerlendirildiğinde bu Kurul Kararının eSIM süreçlerine ve bu süreçlerde işlenen verilere ilişkin karma veri lokalizasyonu politikası izlediği söylenebilir.

6.4.3.8. Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar

5651 sayılı Kanun'un ek 4'üncü maddesine dayanılarak sosyal ağ sağlayıcının yükümlülükleri ile bu yükümlülüklerin uygulanmasına ilişkin usul ve esasları belirleyen Bilgi Teknolojileri ve İletişim Kurulu'nun 29 Eylül 2020 tarihli ve 2020/DK-İD/274 sayılı Kararı, 02 Ekim 2020 tarihli ve 31262 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Usul ve Esasların 4'üncü maddesinin birinci fıkrasının (h) bendiyle veri, *"...Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"*olarak tanımlanmıştır. Usul ve Esaslar'ın *"Verilerin Türkiye'de barındırılması"* başlıklı 12'nci maddesi *"...(1) Yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alır. (2) Bu maddenin uygulanmasında temel kullanıcı bilgileri ile Kurum tarafından bildirilebilecek hususlara ilişkin verilerin Türkiye'de barındırılması yönünde gerekli tedbirlerin alınmasına öncelik verilir. (3) Bu madde kapsamında alınan tedbirlere ilişkin olarak her raporlama döneminde Kurum tarafından bildirilen hususları da kapsayacak şekilde Kuruma bilgi verilir."* hükümlerini amirdir. Söz konusu hüküm ile sosyal ağ sağlayıcılara kullanıcıların yalnızca kişisel verilerini değil tüm verilerini Türkiye'de barındırma yönünde gerekli

tedbirleri alma yükümlülüğü getirmiştir. Bu düzenlemenin karma veri lokalizasyonu politikası çerçevesinde değerlendirilmesi mümkündür.

6.5. Veri Lokalizasyonu Politikalarının Avantajları ve Dezavantajları

Aşağıda detaylıca inceleneceği gibi; son yıllarda birçok ülke, özellikle veri güvenliği, mahremiyet ve milli egemenlik konularında artan endişeler nedeniyle dijital verilerin sınırlar içinde kalmasını zorunlu kılan yasal düzenlemelere yönelmiştir. Bu düzenlemelerin temelinde, kritik ve hassas verilerin yabancı ülkelerin yargı yetkisine tabi olmadan korunması ve yönetilmesi hedefi yatmaktadır.[55] Özellikle büyük teknoloji şirketlerinin verileri çoğunlukla küresel sunucularda depolaması, devletlerin veri üzerinde denetim kurma isteğini daha da güçlendirmiştir.[56] Ancak veri lokalizasyonu politikaları yalnızca güvenlik ve denetim avantajları sağlamakla kalmamakta; aynı zamanda çeşitli ekonomik, teknolojik ve hukuki maliyetleri de beraberinde getirmektedir.[57] Bu politikalar, yerli veri altyapısının gelişimini teşvik edebilirken; küresel rekabet, yatırım çekiciliği, inovasyon kapasitesi ve ifade özgürlüğü gibi alanlarda ciddi soru işaretleri doğurabilmektedir. Dolayısıyla veri lokalizasyonunun, tek boyutlu bir uygulama değil, çok katmanlı sonuçları olan ve stratejik bir tercih olduğu değerlendirilmektedir.

6.5.1. Veri Lokalizasyonu politikalarının avantajları

Veri lokalizasyonu politikalarının en önemli avantajlarından biri, kişisel verilerin ve mahremiyetin korunmasına sağladığı katkıdır. Verilerin ülke sınırları içinde depolanması ve işlenmesi, bu verilerin yerel veri koruma düzenlemelerine tabi olmasını sağlamaktadır.[58] Böylece bireylerin sağlık, finans, iletişim ve konum gibi hassas bilgilerinin işlenmesi ve paylaşılması, ulusal mevzuat kapsamında daha sıkı denetime tabi tutulmaktadır. Özellikle gelişmekte olan ülkelerde, veri lokalizasyonu uygulamaları, güçlü bir veri koruma çerçevesi oluşturma sürecine ivme kazandırabilmektedir.[59] Ayrıca bu tür politikalar, bireylerin kişisel verileri üzerindeki kontrolünü artırarak, rızaya dayalı veri kullanımını teşvik etmekte ve şeffaflık ilkesini

[55] Burman ve Sharma, *How Would Data…* 30.
[56] Singh, "A dissertation submitted…": 27.
[57] Chander ve Lê, "Data Nationalism": 718.
[58] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*
[59] Burman ve Sharma, *How Would Data…* 17.

güçlendirmektedir.[60] Yabancı ülkelerdeki farklı gizlilik standartlarına bağlı kalmak yerine, verilerin yerel düzenlemelere uygun şekilde korunması, veri ihlallerinin önlenmesi ve hukuki uyuşmazlıklarda daha etkili müdahale imkânı sunabilmektedir.[61] Başka bir deyişle; verilerin yabancı ülkelerdeki gözetim rejimlerine, belirsiz hukuki süreçlere veya düşük koruma standartlarına maruz kalma riskinin azaltılması, bireysel mahremiyetin korunmasına doğrudan katkı sağlamaktadır. Verilerin sınır dışına çıkarılmaması, özellikle kişisel verilerin yabancı istihbarat servisleri tarafından erişilme riskini düşürmekte ve böylece bireylerin mahremiyetinin uluslararası müdahalelere karşı daha sıkı şekilde güvence altına alınmasını sağlamaktadır.[62] Ayrıca verilerin ülke içerisinde tutulması, veri sorumluları ve işleyenler üzerinde daha etkin denetim yapılmasına, yerel otoritenin teknik incelemeleri hızlı biçimde yürütebilmesine ve ihlallerin tespiti ile müdahalesinin gecikmeksizin gerçekleştirilebilmesine imkân vermektedir.[63] Bu durumun, yaptırımların caydırıcılığını artırdığı, veri güvenliği süreçlerinin aksamadan işlemesini sağlayarak bireylerin kişisel verilerinin ulusal hukuk düzeni içinde daha yüksek bir koruma standardına kavuşmasına katkı sunduğu değerlendirilmektedir. Bu bağlamda veri lokalizasyonunun, bireysel mahremiyetin korunmasında önemli bir araç olduğu söylenebilecektir.

Veri lokalizasyonu politikalarının en güçlü avantajlarından bir diğeri ise ulusal güvenliğin dijital düzlemde korunmasıdır. Devletler, kritik öneme sahip verilerin – özellikle kamu kurumlarına, savunma sanayiine ve iletişim sistemlerine ait bilgilerin – yabancı ülkelerdeki sunucularda depolanmasını güvenlik riski olarak görmektedir.[64] Bu tür verilerin başka ülkelerin yargı yetkisine veya istihbarat servislerine açık olması, siber casusluk ve dış müdahale risklerini artırmaktadır.[65] Özellikle kriz, savaş ya da diplomatik gerilim dönemlerinde, verinin, ürediği ülkenin kontrolünde olması, bilgi güvenliğini sağlanması açısından kritik öneme sahiptir. Ayrıca, yabancı teknoloji

[60] Cory, "Cross-Border Data…", 4.
[61] Bowman, "A Primer on Russia's…"
[62] Erica Fraser, "Data Localisation and The Balkanisation of The Internet" *SCRIPTed* 13, sy.3 (Aralık 2016): 3.
[63] Singh, "A dissertation submitted…": 27.
[64] Bowman, "A Primer on Russia's…"
[65] Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *Data localisation trends and challenges…* , 6.

şirketlerinin yerel güvenlik standartlarına tam olarak uymaması durumunda, veri lokalizasyonu ulusal düzeyde bir güvenlik filtresi görevi görebilecektir.[66] Bu çerçevede, kritik verilerin ülke içinde tutulması, ilgili kurumlarının bu verilere daha hızlı ve kesintisiz erişebilmesini, olay müdahale süreçlerini daha etkin biçimde yönetebilmesini ve olası tehditleri yerinde tespit ederek bertaraf etmesini mümkün kılacaktır. Verilerin yabancı ülkelerde çeşitlilik gösteren güvenlik protokollerine, zayıf altyapılara veya farklı istihbarat faaliyetlerine maruz kalma ihtimalinin azaltılması ise, milli stratejik çıkarların korunmasında önemli bir avantaj sağlayacaktır.[67] Ayrıca, veri lokalizasyonunun, kritik altyapılar üzerinde yabancı şirketlere veya devletlere aşırı bağımlılığın azaltılmasına, böylece dijital egemenliğin güçlendirilmesine katkıda bulunduğu söylenebilecektir.[68] Bu yönüyle bakıldığında, veri lokalizasyonu, yalnızca teknik bir düzenleme değil, aynı zamanda bir milli güvenlik stratejisi olarak görülebilmektedir.

Veri lokalizasyonu politikaları, güvenlik ve mahremiyet odaklı yaklaşımın beraberinde, yerel ekonomik kalkınmayı teşvik eden stratejik bir araç olarak da işlev görebilir. Verilerin ülke içinde depolanması zorunluluğu, yerli veri merkezlerinin kurulmasını, bilgi teknolojileri altyapısının geliştirilmesini ve nitelikli iş gücüne olan ihtiyacın artmasını beraberinde getirebilmektedir.[69] Bu sayede veri lokalizasyonu düzenlemeleri, veri barındırma kapasitesinin ülke içinde yoğunlaşmasına yol açarak veri merkezi pazarının ölçek kazanmasına sebep olabilecektir. Özellikle büyük ölçekli bulut sağlayıcılarının ülke içinde operasyon kurmak zorunda kalması, veri merkezi sektöründe hem altyapı yatırımlarını hem de rekabeti artıran bir etki doğurabilecek; bu da uzun vadede daha sağlam, kesintiye dayanıklı ve güvenli dijital altyapıların oluşmasına katkı sağlayabilecektir.[70] Ayrıca bu durum, bulut bilişim hizmetleri, siber güvenlik, yazılım geliştirme ve veri yönetimi gibi alanlarda yeni iş olanakları da yaratabilecektir. Aynı zamanda, yerli firmaların küresel teknoloji devleriyle rekabet

[66] Erika Morphy, "Google to Comply…"
[67] Fraser: 3.
[68] Samuele Fratini, "Data localization as contested and narrated security in the age of digital sovereignty: the case of Switzerland" *Information, Communication & Society* 28, sy.8 (Haziran 2024): 1368.
[69] Ferracane, "The Costs of Data Protectionism", 67.
[70] Azmeh ve Foster: 28.

edebilmesi için devlet destekli projelerin ve inovasyon yatırımlarının önü veri lokalizasyonu politikalarıyla açılabilecektir.[71]

Öğretide ise; veri merkezi kiralama veya kurma maliyetlerinin yüksek olması, personel istihdamının zor olması ve tecrübesiz personelin de eğitiminin uzun sürmesi gibi sebeplerle, veri lokalizasyonu politikalarının şirketleri yatırımdan uzaklaştırmaya sevk edebileceği ve uzun vadede yerel ekonomiye zarar vereceği görüşü baskındır.[72] Buna rağmen bazı yazarlar, yerel veri merkezi kapasitesindeki artışın zaman içerisinde ölçek ekonomileri yaratarak maliyetleri düşürebileceğini, böylece başlangıçta yüksek görülen ekonomik yükün uzun vadede stratejik bir altyapı yatırımı niteliğine dönüşebileceğini savunmaktadır.[73]

6.5.2. Veri Lokalizasyonu politikalarının dezavantajları

Veri lokalizasyonu politikalarının en belirgin olumsuz etkilerinden biri, yüksek altyapı ve işletme maliyetleridir. Verilerin yerel sunucularda saklanmasını zorunlu kılan bu politikalar, kamu kurumları ve özel sektör aktörlerinin kendi veri merkezlerini kurmalarını veya mevcut altyapılarını ciddi şekilde geliştirmelerini gerektirir. Bu süreç; fiziksel tesislerin inşası, enerji tüketimi, soğutma sistemleri, ağ altyapısı, siber güvenlik önlemleri ve sürekli teknik destek gibi çok sayıda kalemde önemli harcamaları beraberinde getirir.[74] Özellikle gelişmekte olan ülkelerde, bu yatırımları karşılayabilecek yerel kaynakların sınırlı olması ciddi bir engel teşkil edebilecektir. Küçük ve orta ölçekli işletmeler için bu tür maliyetler, operasyonel verimliliği düşürecek düzeyde olabilecek ve rekabet avantajlarını zayıflatabilecektir.[75] Bu çerçevede, veri lokalizasyonu uygulamaları, maliyet etkinliği açısından önemli bir yük oluşturabilmekte ve dijital dönüşüm süreçlerini yavaşlatabilmektedir.

Veri lokalizasyonu politikaları, ülkelerin dijital egemenliğini artırma amacı taşısa da, bu politikaların katı bir şekilde uygulanması çoğu zaman küresel teknolojiye erişimi sınırlayan bir etki yaratmaktadır.[76] Günümüzde birçok yenilikçi dijital hizmet –

[71] Burman ve Sharma, *How Would Data…* 17.
[72] Ünver ve Kim, "Cross-Border Data Transfers…".
[73] Azmeh ve Foster: 27.
[74] Cory, "Cross-Border Data…", 14.
[75] Ünver ve Kim, "Cross-Border Data Transfers…".
[76] Bowman, "A Primer on Russia's…"

özellikle yapay zekâ, büyük veri analitiği, makine öğrenimi, nesnelerin interneti (IoT) ve küresel bulut platformları – uluslararası ölçekte çalışan sistemlere ve çok uluslu teknoloji şirketlerinin altyapılarına dayanmaktadır. Veri lokalizasyonu zorunluluğu, bu hizmetlerin doğrudan veya tam kapasiteyle kullanılmasını engelleyebilmektedir.[77] Örneğin, verilerin ülke dışındaki sunuculara aktarılamaması durumunda, bazı yazılım ve servislerin çalışması teknik olarak mümkün olmayabilecek ya da sınırlı bir sürümle kullanılmak zorunda kalınabilecektir. Bu da özellikle teknolojiye dayalı sektörlerde faaliyet gösteren şirketlerin küresel pazarlarda rekabet etme kapasitesini zayıflatabilecektir.[78] Ayrıca veri lokalizasyonu politikalarının ağır bir şekilde uygulanması, teknolojik izolasyonun giderek arttığı bir ortamda, ülkelerin ekonomik ve bilimsel anlamda dışa kapalı hale gelmesi riskini de beraberinde getirmektedir. Bu nedenle veri lokalizasyonu, teknolojiye erişim açısından hem kısa vadeli verimlilik kaybı hem de uzun vadeli gelişme engeli anlamına gelebilecektir.

Son olarak veri lokalizasyonu politikaları; teknik ve ekonomik etkilerinin ötesinde, bireysel hak ve özgürlükler açısından da kaygı verici sonuçlar doğurabilmektedir. Verilerin yerel sunucularda tutulması, otoriter eğilimlere sahip yönetimlerde devletin dijital alan üzerindeki denetimini artırarak ifade özgürlüğünü kısıtlama aracı haline gelebilir.[79] Bu durum, demokratik toplumların temelini oluşturan hakların – özellikle bilgiye erişim, ifade özgürlüğü ve iletişim özgürlüğü – zedelenmesine yol açabilecektir.

Görülebileceği üzere veri lokalizasyonu politikaları birçok fayda sağlamanın yanında birtakım dezavantajları da beraberinde getirmektedir. Veri lokalizasyonunun sağladığı avantajları en üst düzeyde kullanabilmek ve olası olumsuz etkilerini dengeleyebilmek için, risk odaklı, şeffaf, esnek ve insan haklarını temel alan bir düzenleme tasarlanmalıdır. Bir veri lokalizasyonu politikasının hayata geçirilmesinden önce, ilgili sektörün düzenleyici kurumunun – örneğin telekomünikasyon verileri bağlamında BTK'nin – Cumhurbaşkanlığı koordinasyonunda ve uzman kurumların

[77] Chander ve Lê, "Data Nationalism": 738.
[78] Yatırım Ortamını İyileştirme Koordinasyon Kurulu, "Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi".
[79] Yayboke vd. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies.*

temsilcilerinden oluşacak bir kurul ya da komisyonun onayını almasının zorunlu hale getirilmesi, avantaj ve dezavantajların dengelenmesi açısından önemli bir araç olarak önerilebilir.[80]

6.6.Veri Lokalizasyonunun Uluslararası Örnekleri

6.6.1. Almanya

Katma Değer Vergisi Kanunu'nun (*Umsatzsteuergesetz*) 14b maddesinin ikinci fıkrası ile faturalara ilişkin detaylı bir lokalizasyon kuralı düzenlenmiştir. Buna göre Almanya'da yerleşik tüccarlar, tüm faturaları elektronik ortamlar da dahil olmak üzere Almanya'da saklamak zorundadır. İlgili veriler bulut sistemleri gibi uzaktan erişilebilen ortamlarda tutulmaları durumunda, tam çevrim içi erişim ve indirmenin garanti altına alınması şartıyla Avrupa Birliği içerisinde de saklanabilir. Ancak bu durumda, tacirin yetkili vergi dairesine söz konusu verilerin yerini bildirme yükümlülüğü bulunmaktadır.

Vergi Kanunu (*Abgabenordnung*) bölüm 146(2)'de ise uluslararası şirketler için istisnalar tanımlanmış olmakla birlikte, vergi ödemekle yükümlü tüm kişilerin defter ve kayıtlarını Almanya içerisinde tutma zorunluluğu düzenlenmektedir.

Telekomünikasyon Kanunu'nun (*Telekommunikationsgesetz*) 176 ile 180. bölümlerinde yer alan hükümler ile, Almanya'daki telekomünikasyon hizmeti sağlayıcılarının konum verilerini dört, trafik verilerini ise on hafta boyunca saklaması ve talep üzerine bu verileri kolluk kuvvetleriyle paylaşması yükümlülüğünü düzenlemektedir. Bunun yanında düzenleme; arayan ve aranan telefon numaraları, arama zamanı, arama konumu, IP adresleri, internet kullanım süresi, veri miktarı ve fatura miktarı gibi kılavuz verilerini (metadata*)* de içermektedir. Kanun tüm bu verilerin ise Almanya sınırları içerisindeki sunucularda tutulmasını emretmektedir. Ancak devam eden yasal süreçler nedeniyle Federal Ağ Ajansı (*Bundesnetzagentur*) 2017 yılında bu kanun ile öngörülen verilerin saklanmasının hukuka aykırı olacağı gerekçesiyle bu hükümlerin uygulanmasını askıya aldığını açıklamıştır.[81] Avrupa

[80] Yatırım Ortamını İyileştirme Koordinasyon Kurulu, "Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi".

[81] Federal Commissioner for Data Protection and Freedom of Information (BfDI), *Data Retention*, https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Telefon-Internet/Positionen/Vorratsdatenspeicherung.html, (20.10.2024).

Birliği Adalet Divanı'nın 20.09.2022 tarihli kararıyla ise trafik ve konum verilerinin saklanmasını düzenleyen bu hükümlerin genel ve geniş kapsamlı bir veri depolamasını öngörmesi sebebiyle hukuka aykırı olduğuna hükmedilmiştir.[82]

Kişisel verilerin yurt dışı transferine ilişkin hükümler aşağıda "Avrupa Birliği" başlığı altında incelenecektir.

6.6.2. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri (ABD), oluşturduğu olumsuz ekonomik etkileri sebebiyle veri lokalizasyonu karşıtı politika izleyen ülkelerin başında gelmektedir.[83] Bu politikaya örnek olarak; ABD, Kanada ve Meksika arasında imzalanan Amerika Birleşik Devletleri-Meksika-Kanada Anlaşması (*The United States-Mexico-Canada Agreement, USMCA*) gösterilebilir. 1 Temmuz 2020 tarihinde yürürlüğe giren anlaşma, Kuzey Amerika Serbest Ticaret Anlaşması'nın (*North America Free Trade Agreement, NAFTA*) yerini almıştır. Anlaşmanın "Finansal Hizmetler (*Financial Services*)" başlıklı bölümünün 17.18 numaralı maddesinin ikinci fıkrasında; *"...bir tarafın mali düzenleyici makamları, düzenleme ve denetleme amaçları doğrultusunda, kapsam dahilindeki kişilerin o tarafın toprakları dışında kullandığı veya konumlandırdığı bilgi işlem tesislerinde işlenen veya depolanan bilgilere anında, doğrudan, eksiksiz ve sürekli erişime sahip olduğu sürece, hiçbir taraf, kapsam dahilindeki bir kişinin tarafın topraklarında iş yapmasının bir koşulu olarak tarafın topraklarındaki bilgi işlem tesislerini kullanmasını veya konumlandırmasını zorunlu kılmayacaktır*." hükmü yer almaktadır. Bu maddeden hareketle, taraf devletlerin anında, doğrudan, eksiksiz ve sürekli erişime sahip olmasının sağlanması şartıyla, tarafların kendi yetki alanlarında veri lokalizasyonu politikası uygulamasının yasaklandığı söylenebilecektir. Ayrıca, anlaşmanın "Dijital Ticaret (*Digital Trade*)" başlığı altındaki 19.11 numaralı maddesiyle; hiçbir tarafın işinin/işletmesinin yürütülmesi için gerekli olan kişisel bilgiler de dahil olmak üzere bilgilerin elektronik

---

[82] Avrupa Birliği Adalet Divanı Kararı, 20 Eylül 2020 günlü, C-793/10 ve C-794/19 sayılı karar.

[83] Frontier Economics, *The Extent and Impact of Data Localisation*, 1 Haziran 2022, https://assets.publishing.service.gov.uk/media/63a1a2e88fa8f539198d9bb5/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf, (09.10.2024).

yollarla sınır ötesi transferini engellemeyeceği veya sınırlayamayacağı düzenlenmektedir.

ABD'nin veri lokalizasyonu politikalarına verilebilecek bir başka örnek de 2018'in Eylül ayında imzalanmış olan ABD-Kore Ticaret Anlaşmasıdır (*The US-Korea Trade Agreement*). Anlaşmanın 15.8 numaralı maddesiyle, tarafların sınır ötesi elektronik bilgi akışına gereksiz engeller koymaktan veya bu engelleri sürdürmekten kaçınmaya gayret edecekleri düzenlenmektedir. Her ne kadar bu maddedeki ifadeler bağlayıcı olmasa da ve hangi engellerin "gereksiz" olduğuna ilişkin açık bir tanımlama bulunmasa da, ABD'nin veri lokalizasyonu ile ilgili tutumunu yansıtması sebebiyle önemli bir anlaşmadır.[84]

Bu aşamada değinilmesi gereken bir diğer düzenleme ise, 23 Mart 2018 tarihinde yürürlüğe giren Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Kanunu'dur (*The Clarifying Lawful Overseas Use of Data Act, the CLOUD Act*). Bu düzenleme ile ABD'nin kolluk kuvvetlerine, ülke dışında olsa bile ABD'de yerleşik işletmeler tarafından depolanan iletişim verilerini talep etme yetkisi verilmektedir. Dolayısıyla bu kanun ile; nerede depolandığına bakılmaksızın ABD'li hizmet sağlayıcılarının işledikleri verilere ilişkin ABD mahkeme kararları ve emirleri ülke dışında da etkili olacaktır.[85] Elbette ki ABD mahkemelerinin emriyle ABD dışındaki verilerin talep edilebilmesi, diğer ülkelerin mevzuatlarıyla çelişebileceğinden tartışmalı bir husus olarak dünya gündeminde yer almaktadır. Bu sebeple düzenleme, veri talebini içeren mahkeme emrine ilgili kişinin ABD'de ikamet etmemesi veya verinin bulunduğu ülke hukukuna aykırılık teşkil etmesi gibi sebeplerle şirketlere itiraz hakkı tanımaktadır. Bu kanun uyarınca verilen bir mahkeme emrinin KVKK'de düzenlenen şartlar sağlanmaksızın uygulanmasının, Türk hukuku bakımından hukuka aykırılık teşkil edeceği söylenebilecektir. Ancak, itiraz yetkisinin ABD'de faaliyet gösteren şirketlere tanınmış olması, hukukumuz için tehlike oluşturan bir soru işareti olarak yer almaktadır. Bu Kanun ile getirilen ikinci önemli düzenleme ise; Kanunun 104(j) maddesi ile ABD'ye yabancı ülkelerle karşılıklı olarak, taraf ülkede bulunan

[84] Yik-Chan Chin ve Jingwu Zhao, "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits" *Laws* 11, sy. 4. (2022): 71.
[85] European Union Agency for Criminal Justice Cooperation, *The CLOUD Act*, 22 Aralık 2022, 4. https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf.

hizmet sağlayıcıların verilerini diğer taraf ülke tarafından verilen doğrudan emirlerle talep edilebilmesine yönelik anlaşma yapma yetkisi vermesidir. ABD bu doğrultuda Birleşik Krallık ve Avusturalya ile anlaşma yapmıştır.[86] Bu anlaşmanın karşılıklı adli yardımlaşma (mutual assistance) çerçevesinde değerlendirilebileceği söylenebilir. Tüm bunların yanında ABD'de de vergi ve milli güvenlik konularında veri lokalizasyonu politikalarının uygulandığı görülebilmektedir.[87]

6.6.3. Avrupa Birliği

Avrupa Birliği ülkeleri içerisinde veri lokalizasyonu politikalarının benimsenmesi hususunda bir birliğin sağlanmamış olduğu söylenebilir. Zira Fransa ve Almanya gibi ülkeler veri lokalizasyonu politikalarına ağırlık vermekteyken, İsveç gibi ülkeler verilerin sınırlar arası özgürce dolaşımını destek veren politikaları desteklemektedir.[88]

Avrupa Birliği mevzuatında kişisel verilerin işlenmesiyle ilgili olarak korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kurallar Genel Veri Koruma Tüzüğü (*General Data Protection Regulation*) ile belirlenir. GVKT'nin "Üçüncü ülkeler veya uluslararası kuruluşlara kişisel veri aktarımı (*Transfers of personal data to third countries or international organisatons*)" başlıklı beşinci bölümüyle kişisel verilerin Avrupa Birliği dışına aktarımı düzenlenmektedir. KVKK yapılan son değişiklikler ile yurt dışına veri aktarım rejimi açısından büyük oranda GVKT ile uyumlu hale gelmiştir.

Avrupa Birliği dışına kişisel verilerin aktarımına imkân sağlayan ilk koşul GVKT'nin 45'inci maddesiyle düzenlenmiştir. Buna göre; Avrupa Komisyonunun bir üçüncü ülke veya söz konusu üçüncü ülke dâhilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun yeterli düzeyde bir koruma sağladığına karar verdiği hâllerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir. Bu düzenleme, KVKK'nin 9'uncu maddesinin birinci fıkrasıyla uyumludur. Bu tezin yazıldığı tarih itibariyle Avrupa Komisyonu; Andorra, Arjantin, Kanada, Faroe adaları, Guernsey, İsrail, Man adası, Japonya,

[86] European Union Agency for Criminal Justice Cooperation, *The CLOUD Act*, 7.
[87] Cory, "Cross-Border Data…", 6.
[88] Cory, "Cross-Border Data…", 11.

Jersey, Yeni Zelanda, Güney Kore, İsviçre, Birleşik Krallık, Amerika Birleşik Devletleri ve Uruguay'ın yeterli koruma sağladığını kabul etmiştir.[89]

GVKT'ye göre yeterlilik kararı bulunmaması halinde, kişisel verilerin Avrupa Birliği dışına aktarımı ancak 46'ncı madde çerçevesinde düzenlenen uygun güvencelere tabi olarak gerçekleştirilebilir. GVKT'nin 46'ncı maddesinin ikinci fıkrasının (a) bendiyle, hukukumuzda KVKK'nin 9'uncu maddesinin dördüncü fıkrasının (a) bendi ile düzenlenen kamu makamları veya organları arasında hukuki bağlayıcılığı bulunan ve uygulanabilir bir belgeye dayanılarak gerçekleştirilebilecek kişisel veri aktarımları düzenlenmiştir. GVKT'nin 46'ncı maddesinin ikinci fıkrasının (b) bendi ve 47'nci maddesiyle bağlayıcı şirket kuralları yolu da bir kişisel veri aktarımı yöntemi olarak gösterilmiştir. GVKT'nin 46'ncı maddesinin ikinci fıkrasının (c) bendiyle Avrupa Komisyonu tarafından kabul edilen standart veri koruma hükümleriyle, (d) bendiyle bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümleriyle, (e) bendiyle onaylı davranış kuralları ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleriyle ve (f) bendiyle de 42'nci madde uyarınca onaylı bir belgelendirme mekanizması ile birlikte üçüncü ülkedeki veri sorumlusu veya veri işleyenin uygun güvenceler uygulamaya ilişkin bağlayıcı ve uygulanabilir taahhütleriyle kişisel verilerin Avrupa Birliği dışına aktarılabileceği öngörülmüştür. Yine KVKK'nin 9'uncu maddesinin altıncı fıkrasıyla uyumlu olarak GVKT'nin 49'uncu maddesine göre, yukarıda düzenlenmiş koşulların sağlanmaması halinde ancak aktarımın yinelemeli olmaması, yalnızca sınırlı sayıda ilgili kişiyi ilgilendirmesi, veri sorumlusu tarafından gözetilen ve karşısında ilgili kişinin menfaatleri veya hakları ile özgürlüklerinin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda gerekli olması ve veri sorumlusunun veri aktarımı ile ilgili tüm koşulları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olması durumunda, kişisel veriler bu maddede düzenlenen birtakım koşulların sağlanmasıyla Avrupa Birliği dışına aktarılabilecektir.

[89] European Commission, *Adequacy Decisions,* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, (20.10.2024).

GVKT ile getirilen yurt dışı aktarım düzenlemesinin de KVKK ile uyumlu olarak bir zorlaştırılmış veri aktarımı politikası olduğu söylenebilecektir.

6.6.4. Avusturalya

63 sayılı ve 2012 tarihli Bireysel Kontrollü Elektronik Sağlık Kaydı Kanunu'nun (*Personally Controlled Electronic Health Record Act*) 5'inci bölümü altında düzenlenen 77'nci maddesi, vatandaşların sağlık verilerinin Avusturalya içinde tutulmasını ve işlenmesini zorunlu tutmaktadır. Aynı maddenin devamında; bu verilerin bir gerçek kişi ya da kuruluşu tanımlayıcı bir bilgi içermemesi durumlarında verilerin, Avusturalya dışında tutulabileceği ve işlenebileceği düzenlenmiştir.

1988 tarihli Avusturalya Federal Gizlilik Kanunu'na göre ise; kişisel verilerin yurt dışına aktarılmadan önce, aktaran, alıcının Avusturalya gizlilik ilkelerini ihlal etmeyeceğinden emin olmak adına gerekli idari ve teknik tedbirleri almalıdır. Ülkemizde olduğu gibi bu kuralın da ilgili kişinin rızasının alınması, verilerin aktarılacağı ülkede Avusturalya'daki korumaya benzer bir korumanın sağlanıyor olması gibi istisnaları mevcuttur.

6.6.5. Belçika

Belçika'da Sosyal Güvenlik Kurumu bildirimleri gibi iş ve istihdam ilişkisi ile ilgili bilgi ve belgeler, Sosyal Belgelerin Saklanmasına ilişkin 08 Ağustos 1980 tarihli Kraliyet Kararnamesi'nin 22'nci maddesi uyarınca (*Koninklijk besluit van 8 augustus 1980 betreffende het bijhouden van sociale documenten*) ülke içinde saklanmalıdır. Ayrıca, Belçika Gelir Vergisi Kanunun (*Wetboek van de Inkomstenbelastingen*) 315'inci maddesine göre gelir vergisinin tespitine ilişkin bilgi ve belgeler; vergi mükellefinin ofisinde, şubesinde, acentesinde veya vergi dairesi bünyesinde tutulmalıdır. Son olarak, Belçika Şirketler Kanunu'na göre (*het Wetboek van Vennootschappen en Verenigingen*) şirketlerin hissedar ve tahvil kayıtları şirketlerin kayıtlı ofislerinde depolanmalıdır.

6.6.6. Çin Halk Cumhuriyeti

Çin Halk Cumhuriyeti'nin, veri lokalizasyonu politikalarının en katı şekilde uygulandığı ülkelerden biri olduğunu söylemek yanlış olmayacaktır. Çin Merkez Bankası'nın (*People's Bank of China*) 17 numaralı ve 21 Ocak 2011 tarihli

"Bankacılık Finans Kuruluşlarını Kişisel Finansal Bilgileri Korumaya Çağıran Bildiri (*Notice to Urge Banking Financial Institutions to Protect Personal Financial Information*)" bildirisi ile, bankalar tarafından toplanan kişisel verilerin yalnızca Çin sınırları içerisinde işlenmesi, depolanması ve analiz edilmesi ve bu kişisel verilerin Çin dışına transfer edilmemesi düzenlenmiştir. Bunun yanında Çin Ulusal Sağlık ve Aile Planlaması Komisyonu tarafından 13 Mayıs 2014 tarihinde yayınlanan Nüfus Sağlığı Bilgilerinin Yönetimine İlişkin Tedbirlere (*Administrative Measures for Population Health Information*) göre, sağlık bilgileri Çin sınırları içerisinde işlenmeli ve muhafaza edilmelidir.[90] Bir başka örnek ise 664 numaralı ve 26 Kasım 2015 tarihli Harita Yönetimi Tüzüğü'dür (*The Regulation on Map Management*). Bu düzenlemeye göre; çevrim içi harita hizmeti sunan gerçek ve tüzel kişilerin, bu hizmete ilişkin sunucuları Çin sınırları içinde kurmaları ve bu hizmeti sunabilmeleri için resmi bir sertifika almaları gerekmektedir. Yine, Çin Devlet Basın, Yayın, Radyo, Film ve Televizyon İdaresi ile Sanayi ve Bilgi Teknolojileri Bakanlığının 4 Şubat 2016 tarihli Çevrim içi Yayıncılık Hizmetlerinin İdaresine İlişkin Düzenlemesiyle (*Provisions on the Administration of Online Publishing Services*); metinler, resimler, haritalar, oyunlar, animasyonlar, sesler ve videolar da dahil olmak üzere herhangi bir çevrim içi içerik yayıncısının gerekli teknik ekipmanlarını, sunucularını ve depolama cihazlarını Çin'de bulundurması gerekliliği düzenlenmiştir.

Çin Halk Cumhuriyeti Devlet Sırlarının Korunması Hakkında Kanun'un (*Law of the People's Republic of China on Guarding State Secrets)* 26'ncı maddesiyle yetkili birimlerin onayı olmaksızın devlet sırrı olarak sınıflandırılan belge, materyal veya nesnelerin ülke toprakları dışına taşınması, iletilmesi, postalanması veya nakledilmesi yasaklanmıştır. Bu çerçevede devlet sırrı olarak nitelendirilen herhangi bir veri grubunun da yurt dışına aktarımının yasak olduğu söylenebilecektir.

Ulaştırma Bakanlığı, Sanayi ve Bilgi Teknolojileri Bakanlığı, Kamu Güvenliği Bakanlığı, Ticaret Bakanlığı, Devlet Sanayi ve Ticaret İdaresi, Kalite Denetimi, Teftiş ve Karantina Genel İdaresi ve Çin Siber Uzay İdaresi'nin 2016 tarihli, 60 sayılı ve

[90] National Health Commission of the People's Republic of China, *Interpretation on Population Health Information Management Measures (Trial Implementation),* 15.06.2014, http://en.nhc.gov.cn/2014-06/15/c_46801.htm, (21.10.2024).

"Çevrim içi Taksi Rezervasyonu İşletme Faaliyetleri ve Hizmetlerinin İdaresine İlişkin Geçici Tedbirler (*Interim Measures for the Administration of Online Taxi Booking Business Operations and Services*)" başlıklı emri uyarınca, çevrim içi taksi şirketleri kullanıcı verilerini Çin sınırları içerisindeki sunucularda barındırmalıdır.

1 Haziran 2017 tarihinde yürürlüğe giren Çin Siber Güvenlik Kanunu (*Cybersecurity Law of the People's Republic of China*) da veri lokalizasyonu açısından önem arz etmektedir. Kanun, "Kritik Bilgi Altyapısı için Operasyon Güvenliği (*Operations Security for Critical Information Infrastructure*)" başlıklı bölümü altında yer alan 31'inci maddesiyle; tahrip olması, işlevini yitirmesi veya veri sızıntısı yaşanması halinde ulusal güvenliği, ulusal refahı, halkın geçimini veya kamu yararını ciddi şekilde tehlikeye atabilecek altyapılar, kritik bilgi altyapısı olarak tanımlamıştır. Aynı madde ile kamu iletişim ve bilgi hizmetleri, elektrik, trafik, su kaynakları, finans, kamu hizmeti ve e-devlet birer kritik bilgi altyapısı olarak sayılmış, ancak tanım bu altyapılarla sınırlı tutulmamıştır. Devamında ise, kritik bilgi altyapı operatörleri tarafından toplanan bu kritik bilgilerin Çin sınırları içerisinde tutulması ve Çin dışına aktarılması için iş/işletme gereksinimi bulunması durumunda güvenlik değerlendirmelerinin yapılması gerekliliği düzenlenmiştir.

Tüm bu anlatılanların dışında Çin Halk Cumhuriyeti, kişisel finans bilgileri, e-bankacılık bilgileri, kredi kartı bilgileri, sigorta endüstrisine ilişkin bilgiler gibi birçok veri grubuna ilişkin katı veri lokalizasyonu politikaları izlemekte ve bulut hizmetleri gibi hizmetleri sunan firmalara da yurt içinde sunucu kurma gibi külfetler yüklemektedir.[91] Bu çerçevede Çin'in dünyadaki en katı veri lokalizasyonu politikalarını izleyen ülkelerden birisi olduğunu söylemek yanlış olmayacaktır. Bu durum, Çin'in global internetin dışında kalmasına ve vatandaşlarının diğer ülke vatandaşlarının yararlandığı imkanlardan mahrum kalmasına neden olmuştur.[92]

6.6.7. Finlandiya

[91] Cory, "Cross-Border Data…", 9.
[92] Chander ve Lê, "Data Nationalism": 721.

Finlandiya, veri lokalizasyonu politikalarının oldukça hafif bir şekilde uygulandığı ülkelerden birisidir. 1336 sayılı Muhasebe Kanunu (*Kirjanpitolaki*) uyarınca, şirketlerin muhasebesel kayıtlarının bir kopyası ülke içerisinde saklanmalıdır.

6.6.8. Fransa

Fransa'nın da son yıllarda veri lokalizasyonu politikalarına ağırlık veren ülkelerden birisi olduğu söylenebilir. 05 Nisan 2016 yılında İçişleri ile Kültür ve İletişim Bakanlıkları tarafından yayımlanan bir genelgeye göre, kamu kurumları tarafından üretilen verilerin saklanmasında yabancı bulut sağlayıcılarının kullanımının hukuka aykırı olduğu ve kamu kurumları verilerinin Fransa'da muhafaza edilmesi ve işlenmesi gerektiği belirtilmektedir.[93] Ayrıca; Fransız Engelleme Tüzüğü (*Loi de Blocage, Statue No 68-678*) ile, hukuki süreçlerle ilgili bilgilerin bir Fransız mahkeme kararı olmaksızın yurt dışına aktarımı yasaklanmıştır.

6.6.9. Güney Kore

Güney Kore'de Mekânsal Verilerin Oluşturulması ve Yönetilmesi Hakkında Kanun'un (*Act on the Establishment and Management of Spatial Data*) 16'ncı maddesi ile; yüksek çözünürlüklü görüntüler sunan haritaların ve buna ilişkin verilerin milli güvenlik sebebiyle Arazi, Altyapı ve Ulaştırma Bakanlığı izni olmaksızın Güney Kore dışında depolanması yasaklanmıştır. Burada önemle belirtmek gerekir ki, bu düzenleme Güney Kore'de harita hizmeti sunan uluslararası şirketlerin rekabet konusunda dezavantajlı duruma düşmelerine sebep olmasından dolayı eleştirilmesine rağmen milli güvenliğin korunması amacıyla uygulanmaktadır.

Bilgi ve İletişim Ağlarının Kullanımının Teşviki ve Bilginin Korunması Hakkında Kanun (*Act on Promotion of Information and Communicatons Network Utilization and Information Protection*) ile çevrim içi hizmet sağlayıcıların kullanıcıların verilerini yurt dışına aktarabilmeleri için açık rızalarını almaları ve aktarılacak veriler, aktarılan ülke, aktarım tarihi, saati ve yöntemi, aktarılacak kişi/kuruluş bilgisi, kişisel verilerden sorumlu olacak kişinin iletişim bilgileri, aktarım amacı, saklama süresi hakkında detaylı bilgilendirme yapmaları gerektiği düzenlenmiştir.

---

[93] Martina F. Ferracane, "Restrictions on Cross-Border data flows: a taxonomy" *European Centre for International Political Economy* 1 (2017): 14.

Tıbbi Hizmetler Kanunu (*the Medical Services Act*) ile elektronik sağlık kayıtlarının Güney Kore dışında saklanması yasaklanmıştır. Bunun yanında Elektronik Finansın Denetlenmesine İlişkin Yönetmelik (*the Regulation on Supervision of Electronic Finance*) ile finans şirketleri veya elektronik finans işletmecilerinin kimlik ile kredi kartı bilgilerini bulut bilişim hizmetleri aracılığıyla yurt dışında bulunduramayacağı düzenlenmektedir. Son olarak Bulut Bilişim Kanunu (*the Cloud Computing Act*) ile kamu kurumlarınca işlenen verilerin Güney Kore'de muhafaza edilmesine hükmedilmektedir.

6.6.10. Hollanda

Hollanda'da veri lokalizasyonuna ilişkin bir mevzuat olmadığı söylenebilir. Ancak, Arşiv Kanunu'na (*Archiefwet*) göre, kamu kurumu kayıtları fiziksel ve elektronik olarak yalnızca Hollanda'daki belirli konumlarda muhafaza edilebilmektedir.

6.6.11. Japonya

Japonya'da spesifik olarak veri lokalizasyonu kuralları öngören bir mevzuat bulunmamakta, ancak kamu kurumları tarafından sektör bazlı birtakım resmi kılavuzlar yayımlanmaktadır.[94] Bunlara örnek olarak; sağlık verileri ile kamu kurumlarına ilişkin bilgiler gösterilebilir.

6.6.12. Kanada

Kanada'da British Columbia ve Nova Scotia eyaletlerinde veri lokalizasyonu politikaları uygulamaya konmuştur. Bilgi Edinme Özgürlüğü ve Mahremiyetin Korunması Kanunu (*Freedom of Information and Protection of Privacy Act*) ile bu iki eyalette hastaneler, kamu kurumları ve okullar gibi kamu kurumları tarafından işlenen kişisel veriler belirli istisnalar haricinde Kanada'da muhafaza edilmeli ve yalnızca Kanada'dan erişilebilir halde tutulmalıdır.

6.6.13. Meksika

[94] Hiroyuki Tanaka vd., Data Localization Laws: Japan, *Thomson Reuters*, 18 Temmuz 2022. https://www.mhmjapan.com/content/files/00065282/Data%20Localization%20Laws%20Japan.pdf, (21.10.2024).

Meksika'da Milli Güvenlik Kanunu'na (*Ley de Seguridad Nacional*) göre kamu kurumları tarafından işlenen ve milli güvenlik bilgisi olarak sınıflandırılan veriler, kamu kurumlarının tesislerinde saklanmalıdır.

6.6.14. Polonya

Polonya'da belirli sektörlere özel veri lokalizasyonu kuralları düzenlenmiştir. Telekomünikasyon Kanunu (*Telecommunications Acti*) uyarınca, telekomünikasyon ve internet servis sağlayıcıları; iletişimle ilgili konum, cihaz bilgileri, iletişimin zamanı ve türü gibi kılavuz verilerini 12 ay boyunca ülke içerisinde saklamalıdır. Ayrıca 19 Kasım 2009 tarihli Şans Oyunları Kanunu'na (*Ustawa o grach hazardowych*) göre, çevrim içi kumar oyunlarıyla ilgili verilerin işlenmesi ve depolanması için kullanılan cihazlar Avrupa Birliği/Avrupa Ekonomik Alanı içerisinde yer almalıdır.

6.6.15. Rusya Federasyonu

Rusya'nın veri lokalizasyonu konusunda en ağır kuralları benimseyen ülkelerden birisi olduğunu söylemek yanlış olmayacaktır. Şöyle ki, Rusya Kişisel Veriler Hakkında Federal Kanunu'nun 18'inci maddesine göre (*Federal Law No. 152-FZ on Personal Data*) kişisel veriler Rusya Federasyonu sınırları içerisindeki sunucularda depolanmalı ve işlenmelidir. Belirli şartlar dahilinde kişisel veriler yurt dışına aktarılabilse de, ilk olarak Rusya'da depolanmalıdır. Rusya, LinkedIn gibi ziyaret oranı oldukça yüksek internet sitelerini dahi verileri ülke içinde depolama konusunda zorlamakta, aksi takdirde yaptırım uygulamakta veya bu sitelere erişimleri engellemektedir.[95]

Rusya, özellikle telekomünikasyon verileri açısından uyguladığı lokalizasyon politikalarıyla göze çarpmaktadır. İletişim Federal Kanunu'nun (*Federal Law No. 126-FZ on Communications*) 64'üncü maddesiyle, tüm iletişim operatörlerine kullanıcıların elektronik iletişimlerine ilişkin içerik ve kılavuz (metadata) verilerini ülke içerisinde bulundurma zorunluluğu getirilmektedir. Ayrıca; Bilgi Teknolojileri ve Bilginin Korunmasına İlişkin Federal Kanun'un (*Federal Law No. 149-FZ on Information, Informational Technologies and Protection of Information*) 10'uncu maddesi internet siteleri ve yazılımlar gibi bilgi yayılımı sağlayıcılarının kullanıcıların iletişimlerinin içeriklerini ve kılavuz verilerini Rusya içerisindeki sunucularda

[95] Cory, "Cross-Border Data…", 14.

saklanmasını gerektirmektedir. Aynı Kanun ile, 3000'den fazla okuyucusu olan blogların bilgi yayılımı sağlayıcısı olarak kayıt yaptırmaları gerekmektedir. Bu yükümlülüklere uymayan sağlayıcılara Roskomnadzor kurumu tarafından erişim engeli getirilebilmektedir.

İnternet ve bilgi teknolojileri konusunda görece daha sınırlayıcı bir politika izleyen Rusya Federasyonu'nda Dijital Kalkınma, İletişim ve Kitle İletişim Bakanlığı'na bağlı faaliyet gösteren ve Rus kitle iletişim araçlarının denetlenmesi, sansürü ve kontrol edilmesinden sorumlu olan Federal İletişim, Bilgi Teknolojileri ve Kitle iletişim Araçları Denetleme Servisi ("**Roskomnadzor**") bulunmaktadır.[96] Yabancı Kişilerin Rusya Federasyonu Topraklarında Bilgi ve Telekomünikasyon Ağı İnternet Üzerindeki Faaliyetlerine İlişkin Federal Kanunun (Federal Law no. 236-FZ on the Activities of Foreign Persons in the Information and Telecommunication Network "Internet" on the Territory of the Russian Federation) 5'inci maddesi ile; Rus internetinde faaliyet gösteren yabancı şirketlerin Rusya'da şube açması, Rus vatandaşları ile iletişime geçebilmesi için bir mekanizma oluşturması ve Rus kamu kurumu yetkilileriyle etkileşime geçebilmesi için de Roskomnadzor'un internet adresinde bir hesap açması gerekmektedir.

31 Temmuz 2014 tarihli ve 758 sayılı, 12 Ağustos 2014 tarihli ve 801 sayılı Hükümet Kararnamesi ile ile kamuya açık Wi-Fi hesaplarının kullanımı hakkında düzenleme yapılmıştır. Buna göre tüm internet servis sağlayıcılar internet bağlantısının sağlanmasından önce kullanıcıların kimlik belgelerini ve terminal ekipmanını tanımlar. Ayrıca Rusya'daki tüm tüzel kişilikler, kendi ağlarını kullanarak internete bağlanan kişilerin listesini her ay düzenli olarak internet servis sağlayıcılarına bildirmekle yükümlüdür. Bu yükümlülüklere uyulmaması halinde idari para cezaları uygulanmaktadır.

Diğer ülkelere nazaran farklı sektörlerde veri lokalizasyonu politikaları da Rusya Federasyonu'nda uygulanmaktadır. Örneğin, Hava Taşımacılığı İşlemleri İçin Otomatik Bilgi Sistemi Gerekliliklerinin Onaylanmasına İlişin 24 Temmuz 2019 tarihli ve 955 sayılı Hükümet Kararnamesi'nin 9'uncu maddesine göre yurt içi hava

[96] Kurum hakkında detaylı bilgi için bakınız: https://rkn.gov.ru.

taşımacılığı faaliyetlerinde kullanılan veri tabanları ve sunucuların Rusya'da bulunması gerekmektedir.

6.7.Ülkelerin Veri Lokalizasyonu Politikalarına İlişkin Genel Değerlendirme

Veri lokalizasyonu politikaları, ülkeden ülkeye farklılık arz etmekte; ülkeler kendi çıkarları ve stratejik hedefleri doğrultusunda birbirinden tamamen farklı politikalar belirleyebilmektedir. Bu politikalar sertlik, uygulandığı sektör ve uygulama şekli gibi birçok unsura göre çeşitlendirilebilir. Yukarıda incelenen ülkelerin veri lokalizasyonu politikalarını uyguladıkları sektörler Tablo 1'de gösterilmiştir.

Tablo 1-1 Ülkelerin veri lokalizasyonu kuralı düzenlediği sektörler

No	Ülke	Sektör
1	Almanya	Vergi Telekomünikasyon Kişisel veriler
2	ABD	Vergi Milli güvenlik
3	AB	Kişisel veriler
4	Avustralya	Sağlık Kişisel veriler
5	Belçika	Sosyal güvenlik Vergi Şirketler Kişisel veriler
6	Çin	Bankacılık Sağlık Harita yönetimi İnternet Devlet sırrı ve milli güvenliğe ilişkin bilgiler Çevrim içi taksi

		Siber güvenlik Kişisel veriler
7	Finlandiya	Muhasebe Kişisel veriler
8	Fransa	Kamu kurumları tarafından üretilen veriler Hukuki süreçler Kişisel veriler
9	Güney Kore	Harita yönetimi Bilgi iletişim ağları Sağlık Finans Bulut bilişim Kişisel veriler
10	Hollanda	Kamu kurumu kayıtları Kişisel veriler
11	Japonya	Sağlık Kamu kurumu kayıtları Kişisel veriler
12	Kanada	Hastane, kamu kurumları ve okulların kayıtları Kişisel veriler
13	Meksika	Kamu kurumu kayıtları Milli güvenliğe ilişkin bilgiler Kişisel veriler
14	Polonya	Telekomünikasyon Milli güvenliğe ilişkin bilgiler Kişisel veriler
15	Rusya	Telekomünikasyon İnternet Şirketler

		Kamuya açık Wi-Fi bilgileri Hava taşımacılığı Kişisel veriler
16	Türkiye	Kamu kurumları Sağlık Sermaye piyasası Bankacılık ve finans Telekomünikasyon Kişisel veriler

Ülkelerin veri lokalizasyonu politikalarını uyguladıkları sektörler benzerlik gösterse de bu politikaların katılığı oldukça farklılık arz edebilmektedir. İncelenen ülkeler arasında en katı politikaların Çin ve Rusya'nın; en hafif politikaların ise Japonya, Finlandiya, Avustralya ve Hollanda tarafından uygulandığı söylenebilir. Benzer şekilde, Global Data Alliance tarafından gerçekleştirilen bir araştırma sonucunda bir Sınır Ötesi Veri Politikası Endeksi oluşturulmuş; bu endekse göre Rusya ve Çin "Son Derece Kısıtlayıcı" ülkeler olarak 4. seviyede, Türkiye, Hindistan, Suudi Arabistan, Endonezya, Kazakistan ve Vietnam "Oldukça Kısıtlı" ülkeler olarak 3. seviyede, Bangladeş, Güney Afrika, Avrupa Birliği ülkeleri, Güney Kore, Nijerya, Birleşik Arap Emirlikleri ve Senegal "Kısıtlayıcı" ülkeler olarak 2. seviyede, Amerika Birleşik Devletleri ve Japonya ise "Nispeten Açık" olarak 1. seviyede konumlandırılmıştır.[97]

Ayrıca, bu çalışma kapsamında veri lokalizasyonu politikalarının uluslararası uygulamalarını değerlendirebilmek adına IRG (Information Regulators Group) üyesi ülkelere konuya dair bilgi talebi iletilmiştir *(Ek)*. Ülkelere; telekomünikasyon sektörüne özgü veri lokalizasyonu politikalarının bulunup bulunmadığına, milli güvenlik ya da kamu düzeni gibi gerekçelerle hükümetin veya güvenlik birimlerinin verilere erişim talep etmesi durumunda operatörlerin uyması gereken bir prosedürün olup olmadığına ve konu ile ilgili olarak şu an gündemlerinde olan mevzuat ya da politika çalışmasının bulunup bulunmadığına ilişkin sorular yöneltilmiştir. Söz konusu

[97] Global Data Alliance, *Cross-Border Data Policy Index*, Temmuz 2023 13, https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf (07.11.2025).

sorulara Hırvatistan (HAKOM), Çek Cumhuriyeti (CTU), Almanya (BNetzA), İrlanda (ComReg), Malta (MCA), Norveç (NKOM), Polonya (UKE), Portekiz (ANACOM), Slovak Cumhuriyeti (RU), İsviçre (BAKOM) ve Birleşik Krallık (OFCOM UK) geri dönüş yapmıştır. Ülkelerin verdiği yanıtlar, veri lokalizasyonuna ilişkin düzenleme anlayışının ülkeler düzeyinde farklı şekillendiğini ortaya koymuş ve konunun uluslararası bağlamda nasıl ele alındığına dair genel bir çerçeve sunmuştur.

Rusya ve Çin, kişisel verilerin öncelikle ülke içerisinde depolanma şartını katı bir şekilde uygulayarak birçok yatırımcıyı zor bir durum içine sokmakta ve literatürde de sıklıkla otoriter bir rejim kurduğu gerekçesiyle eleştirilmektedir.[98] Ayrıca, katı veri lokalizasyonu politikalarıyla vatandaşlarının mahremiyetinin ve kişisel verilerinin korunduğunu, kolluk ve istihbarat faaliyetleri ile siber güvenliğin sağlandığını, yabancı istihbaratın önlendiğini söylemek pek de mümkün değildir. Zira Oxford Üniversitesinde gerçekleştirilen bir çalışmaya göre siber suç tehdidinin en yüksek olduğu ülkeler sıralamasında Rusya açık ara farkla birinci, Çin de üçüncü olarak konumlanmıştır.[99] Öte yandan izlenen bu katı politikalar, bireylerin mahremiyetinin korunmasına kayda değer bir katkı sağlamazken; bilgiye erişim özgürlüğünün sınırlanmasına ve diğer ülke vatandaşlarının kullandığı teknolojiden mahrum kalmalarına sebep olabilmektedir.[100] Yapılan başka bir çalışmaya göre ise en düşük siber güvenlik risklerine sahip ülkeler sıralamasında Finlandiya birinci, Avustralya dördüncü ve Japonya sekizinci sırada yer almıştır.[101] Çoğu ülkeye nazaran oldukça hafif lokalizasyon politikaları izleyen ülkelerde verilerin yerelleştirilmemesinin tek başına siber güvenlik risklerini artırmadığı görülebilmektedir.

Ferracane tarafından yapılan araştırmaya göre; dünya çapında veri lokalizasyonu politikalarının %49 oranla en sık Asya-Pasifik bölgesinde uygulandığı, bunu %36

---

[98] Alina Polyakova ve Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models", *Foreign Policy at Brookings*, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf, (21.10.2024).

[99] Miranda Bruce vd., "Mapping the global geography of cybercrime with the World Cybercrime Index" *PLoS ONE* 19, sy.4, (Nisan, 2024): 8.

[100] Polyakova ve Meserole, "Exporting Digital Authoritarianism…".

[101] Samara Lynn, "Countries With The Highest Cyber Threat Risk And Ones With The Lowest: Report", *MES Computing*, 16 Mayıs 2024, https://www.mescomputing.com/news/4208968/countries-cyber-threat-risk-ones-lowest-report, (22.10.2024).

oranla Avrupa, %7 ile Kuzey Amerika, %5 ile Latin Amerika ve %3 oranla da Afrika'nın takip ettiği görülmektedir.[102] Aynı çalışma ile dünya genelinde veri lokalizasyonu politikalarının %36'sının kişisel verileri, %14'ünün şirket kayıtlarını, %14'ünün finansal verileri, %9'unun kamu verilerini, %9'unun müşteri verilerini, %5'inin tüm verileri ve %2'sinin sağlık verilerini kapsadığı tespit edilmiştir. Sektör bazında ise politikaların %53'ü yatay bir dağılıma sahipken, %12'sinin finans, %12'sinin çevrim içi hizmet sağlayıcılar, %9'unun kamu ve %5'inin telekomünikasyon sektörlerine odaklandığı görülmüştür.[103]

Politikaların uygulama tarihlerine bakıldığında ise, veri lokalizasyonuna ilişkin kuralların tüm dünyada özellikle son yıllarda arttığı ve genel eğilimin verilerin ülke içerisinde tutulmasına yönelik olduğu görülmektedir. Ülkeler gittikçe daha katı lokalizasyon politikaları benimsemekte, yerel veri merkezlerinin kullanımını teşvik etmekte ve yurt dışına veri aktarımını kısıtlamakta veya yasaklamaktadır. Teknolojinin ise gün geçtikçe verinin global akışına daha çok muhtaç hale gelmesi, çözülmesi zor bir ikilem oluşturmaktadır.

[102] Ferracane, "Restrictions on Cross-Border data…" :8.
[103] Ferracane, "Restrictions on Cross-Border data…" :9.

SONUÇ VE ÖNERİLER

Sanayi ve teknolojinin gelişmesi, çağın gereksinimlerinin değişmesi ve gündelik aktivitelerin giderek farklılaşması ve çeşitlenmesiyle insanların mahremiyet ve özel hayata saygı haklarının da kapsamı zaman geçtikçe genişlemiştir. Hukuk da bu değişime uyum sağlamış; mahremiyet hakkı, kişisel verilerin korunması hakkı ve haberleşmenin gizliliği hakkı gibi temel hak ve hürriyetler ile insanların gelişen özel hayat alanları çerçevesinde koruma kapsamını genişletmiştir. Bireylerin korunması gereken kişiliğinin vazgeçilmez birer göstergesi olan kişisel veriler, AİHS ve Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi gibi birçok uluslararası düzenlemenin yanı sıra yerel mevzuat ile de korunmaya başlamıştır.

Günümüz dünyasında veri kavramı bambaşka bir boyuta ulaşmıştır. İnsanlar, gündelik hayatının neredeyse her anında sürekli olarak veri üretmekte ve üretilen bu veriler birçok bağlantı teknolojisi ve cihaz ile sayısız alıcıya ulaştırılmaktadır. Mobil telefonlardan bağlantılı araçlara, eSIM teknolojili bir buzdolabından çevrim içi taksilere kadar kullanılan her ürün ve hizmet ile sayısız nicelik ve nitelikte veri üretilmeye başlanmış ve birçok farklı kaynaktan toplanan bu veriler büyük veri yığınları oluşturmuştur. Sonrasında bu veriler veri madenciliği, makine öğrenmesi ve derin öğrenme gibi teknolojiler aracılığıyla işlenmeye; heterojen veri yığınlarından çözümleme yapılarak anlamlı bilgiler üretilmeye başlanmıştır. Bu durum, ekonomik gelişmeye katkıda bulunması, bilimsel araştırmaları hızlandırması ve yeni teknolojilerin geliştirilmesi gibi sayısız faydayı beraberinde getirse de bireylerin mahremiyetinin korunması açısından risk oluşturmaktadır. Kişisel verilerin korunmasına yönelik gerekli tedbirlerin alınmaması; bireylerin davranış örüntülerinin tespiti ve mahrem bilgilerinin hukuka aykırı ifşasından iradelerinin sakatlanması ve karar alma mekanizmalarının etkilenmesine kadar birçok olumsuz sonuca sebep olabilmektedir.

Elbette ki devletlerin tek sorumluluğu bireylerin mahremiyet ve kişisel verilerinin korunmasını sağlamak değildir. Örneğin devletler, vatandaşların AİHS'in 2'nci

maddesiyle düzenlenen yaşam haklarını ve 5'inci maddesinde yer alan özgürlük ve güvenlik haklarını korumak ve sağlamakla da yükümlüdür. Bu hakların sağlanması, kamu düzeninin korunması ve suçların soruşturulması ve önlenmesi gibi sorumluluklar, zaman zaman vatandaşların mahremiyet haklarına müdahale edilmesini gerektirebilmektedir. Bu gibi durumlarda mahremiyet hakkına yapılacak meşru bir müdahalenin zamanında gerçekleştirilememesi, insanların can ve mal güvenliğini tehdit edebilmekte ve kamu düzenini bozucu etki oluşturabilmektedir. Gelişen teknolojik imkanlar, mahremiyet hakkına meşru gerekçelerle müdahale edilmesini de zorlaştırmıştır. Örneğin bu imkanlar sayesinde suçlular, delil niteliğindeki verilerin ülkeden çıkarılmasını sağlayabilmekte; bunun sonucunda da soruşturmaların sonuçsuz kalmasına ve kolluk kuvvetleri, yargı makamları ve ilgili kamu kurum ile kuruluşlarının milli güvenliğin sağlanması ve suçların önlenmesi gibi meşru amaçlarla ihtiyaç duyacakları bilgilere erişememesine sebep olabilmektedir. Bu durumlar devletleri kişisel verilerin korunması ve veriler üzerindeki kontrolün sağlanması ile ilgili düzenlemeler yapmaya teşvik etmiştir.

Ülkemizde bazı veri grupları, kişisel veri olup olmadığına bakılmaksızın ayrıca bir korumaya tabi tutulmaktadır. Şöyle ki; işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar, Ulusal Siber Güvenlik Stratejisi kapsamında kritik altyapı olarak adlandırılmaktadır. Kritik altyapılar ise ulaştırma, enerji, elektronik haberleşme, finans, su yönetimi ve kritik kamu hizmetleri olarak belirlenmiştir. Dolayısıyla ülkemizde kişisel veri olup olmadığına bakılmaksızın kritik altyapı verisi olduğu için telekomünikasyon verileri de belirli düzenlemelere tabi tutulmaktadır. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanırken; telekomünikasyon verisi gerçek kişiyle ilişkilendirilebilme niteliğinden bağımsız olarak elektronik haberleşme çerçevesinde işlenen verilerdir. Bu çerçevede her telekomünikasyon verisinin kişisel veri olmadığı teorik olarak söylenebilecektir. Ne var ki günümüzde her türlü verinin gerçek kişilerle ilişkilendirilebileceği düşünüldüğünde, neredeyse her telekomünikasyon verisinin kişisel veri tanımına da girebileceği düşünülebilir.

Kişisel verileri ve telekomünikasyon verileri işlenen ilgili kişiler, mevzuat kapsamında belirli koruma mekanizmalarıyla güvence altına alınmıştır. Örneğin; kişisel veriler ve telekomünikasyon verileri hukuka ve dürüstlük kurallarına uygunluk gibi belirli ilkelere tabi olarak işlenebilmekte, kanunda tanımlanmış hukuki sebeplerden biri olmaksızın işlenememekte, belirli şartlar çerçevesinde aktarılabilmekte ve ilgili kişilerin aydınlatılması gerekmektedir. Devletler zamanla ekonomik, siyasi ve stratejik nedenlerde bu koruma mekanizmalarını yetersiz bulmuş ve mahremiyetin korunması, milli güvenliğin ve kamu düzeninin sağlanması gibi sebeplerle bazı veri gruplarının yurt içinde saklanmasını zorunlu kılmaya başlamıştır.

Veri lokalizasyonu, verilerin doğrudan veya dolaylı olarak belirli bir egemenlik alanı içerisinde münhasıran veya münhasır olmayan bir şekilde depolanmasını veya işlenmesini öngören ya da verinin ulusal sınırlar dışına aktarılmasını zorlaştıran yasal veya idari gereksinimler olarak tanımlanmaktadır. Uygulamaya göre veri lokalizasyonunun katı veri lokalizasyonu, yumuşak veri lokalizasyonu, karma veri lokalizasyonu ve zorlaştırılmış veri aktarımı olmak üzere dört farklı çeşidi bulunmaktadır. Katı veri lokalizasyonu politikaları, verilerin ancak bu kuralları düzenleyen ülkenin sınırları içerisinde işlenebileceğini ve depolanabileceğini öngören kurallar olarak tanımlanırken; verilerin bir kopyasının ülke sınırları içerisinde tutulması şartıyla işleme veya depolama amacıyla yurt dışına aktarımına izin verilmesini öngören kurallar yumuşak veri lokalizasyonu olarak tanımlanır. Hem katı hem de yumuşak veri lokalizasyonu kurallarının özelliklerini barındıran politikalara ise karma veri lokalizasyonu kuralları denir. Son olarak; verilerin doğrudan ülke içerisinde işlenmesi veya depolanması şartını barındırmayan ancak verilerin yurt dışına aktarımı için belirli şartlar düzenleyen politikalar zorlaştırılmış veri aktarımı olarak adlandırılmaktadır. Bu kurallar da yukarıda belirtilen üç veri lokalizasyonu türünde gözlemlenen etkileri doğurduğu için veri lokalizasyonu kapsamında değerlendirilmektedir.

Devletlerin veri lokalizasyonu politikalarını uygularken savunduğu temel gerekçelerden birisi vatandaşların mahremiyetinin ve kişisel verilerinin korunmasıdır. Bireyler; kişisel verilerinin sayısız alıcıya aktarılması ve bilgilerinin yetkisiz kişilere ifşa edilmesi riski altındadır. Bireyin vatandaşı olduğu ülkede güçlü bir kişisel veri

koruma mekanizması geliştirilmiş olsa dahi, verilerin aynı korumayı sunmayan bir ülkeye aktarımı halinde söz konusu risk daha da güçlenecektir. Bu sebeple kişisel verilerin yurt dışına aktarımı belirli şartlara tabi tutulmalı, bu şartlar gerçekleşmeden kişisel verilerin aktarımına izin verilmemelidir. Ancak burada korunan menfaatin bireyin mahremiyeti olduğu ve verisinin geleceğine karar yetkisinin de bireyin kendisinde olduğu unutulmamalıdır. Bu sebeple her ne kadar kişisel veri lokalizasyonu kuralları bireyin mahremiyetinin korunması için gerekli olsa da, bu kuralların gereğinden fazla katı olması; bilgilerin sınırlar arası özgürce dolaşmasını engelleyecek, bireylerin diğer ülke vatandaşlarının sahip olduğu birtakım ürün ve hizmetler ile teknolojik yeniliklerden mahrum kalmasına sebep olabilecek ve bireyleri global şirketlerin ülkeye yatırım yapmaması gibi veri lokalizasyonunun olumsuz etkileriyle baş başa kalmasına sebep olabilecektir. Bu sebeplerle zorlaştırılmış veri aktarımı kurallarının bireylerin mahremiyeti ve kişisel verilerinin korunması için gerekli olduğu; ancak yumuşak, karma veya katı veri lokalizasyon kurallarının bu açıdan ölçülü ve orantılı olmayacağı, dolayısıyla bu lokalizasyon kurallarından kaçınılması gerektiği değerlendirilmektedir.

Veri lokalizasyonu politikalarının diğer gerekçelerinden birisi ise kolluk ve istihbarat faaliyetleridir. Devletler kamu düzeninin sağlanması, milli güvenliğin ve temel hak ve hürriyetlerin korunması amaçlarıyla; suçların tespiti ve önlenmesi ve terörizmin önüne geçilmesi gibi kolluk faaliyetlerinde bulunmaktadır. Doğası gereği bu faaliyetler çerçevesinde devletlerin oldukça büyük nicelik ve nitelikte veriye erişmesi gerekebilmektedir. Günümüzde veri ve iletişim teknolojileri nedeniyle kolluk ve istihbarat makamlarının veriye erişim kapasitesinin oldukça azalması, devletleri veri lokalizasyonu politikalarına başvurmaya itmiştir. Literatürde bu gerekçelere antitez oluşturmak adına devletlerin veriye erişim için halihazırda yeterli düzeyde araçları olduğu ve yurt dışındaki verilere erişim için de ikili anlaşma yönteminin tercih edilebileceği savunulmuştur. Suçların önlenmesi ve soruşturulması kapsamında doğru veriye hızlı erişimin önemi tartışmasız bir şekilde ortadadır. İkili anlaşmalar çerçevesinde yapılacak bir veri erişim talebinin sonuçlanması aylar sürebilmekte, bu süre içerisinde söz konusu talep anlamsız hale gelebilmekte ve soruşturmalar sonuçsuz bir şekilde kapatılabilmektedir. Bu sebeple belirli sınırlar dahilinde kolluk ve istihbarat

faaliyetlerinin sağlanması amacıyla veri lokalizasyonu politikalarının uygulanabileceği değerlendirilmektedir. Zorlaştırılmış veri aktarımı kuralları, birtakım kritik verilere kolluk ve istihbarat makamlarının erişememe riskini oluşturabileceğinden; bu faaliyetler için yumuşak veya karma veri lokalizasyonu kuralları benimsenebilir. Aynı değerlendirme yabancı ülke istihbarat faaliyetlerinin engellenmesi gerekçesiyle uygulamaya konulan veri lokalizasyonu politikaları için de yapılabilir. Tüm dünyanın veri lokalizasyonu politikalarına yönelmesi ve bu yöndeki eğilimin dramatik bir şekilde artması, ABD'de gerçekleşen Snowden ifşaları sonrasında devletlerin yabancı ülke istihbarat faaliyetlerinin engellenmesi için çalışmaya başlaması sebebiyle olmuştur. Yabancı ülke istihbarat faaliyetlerinin engellenmesinin de kolluk faaliyetleri gibi, devletlerin verilere ilişkin düzenleme yapabileceği meşru amaçlardan olduğu değerlendirilir. Elbette ki bu durum, her iki gerekçe için de, tüm verilerin sınırsız bir şekilde yerelleştirilmesine cevaz verildiği anlamına gelmemektedir. Veri lokalizasyon kuralları uygulanırken; tüm verileri kapsayacak geniş kapsamlı bir lokalizasyon politikası tasarlanmamalı, sektör bazlı ve veri bazlı spesifik ayrımlar yapılmalı, süre sınırları tanınmalı ve bireylerin mahremiyeti ile kişisel verilerinin korunmasına yönelik tedbirler alınmalıdır.

Veri lokalizasyonu politikaları her ülke de değişiklik gösterebilmekte, devletler kendi stratejik hedefleri çerçevesinde farklı politikalar izleyebilmektedir. Bu tez kapsamında incelenen ülkeler arasında en katı politikaların Çin ve Rusya tarafından, en hafif politikaların ise Japonya, Finlandiya, Avustralya ve Hollanda tarafından uygulandığı gözlemlenmiştir. Çin ve Rusya, katı veri lokalizasyonu politikalarını uygularken her ne kadar vatandaşlarının mahremiyeti ve kişisel verilerinin korunmasını, siber güvenliğin sağlanmasını ve milli güvenliğin korunmasını hedeflese de; uygulamada bu politikaların bu amaçları sağlamadığı görülmektedir. Nitekim her iki ülke de siber suçların en çok yaşandığı ülkeler arasında yer almakta ve dijital bir otorite kurarak vatandaşlarını dünyadan soyutlama konusunda kamuoyunda sürekli eleştirilmektedir. Veri lokalizasyon politikalarını uygulamayan veya yalnızca birkaç mevzuat ile sınırlı bir şekilde uygulayan ülkelerde ise mahremiyetin korunması açısından riskli durumların daha az olduğu, siber güvenlik risklerinin düşük olduğu ve bireylerin bilgiye erişimde diğer ülkelere nazaran daha avantajlı olduğu tespit edilmektedir. Bu

sebeple katı veri lokalizasyonu politikalarının beklenen faydaları sağlamamakla birlikte vatandaşlar açısından birçok dezavantajlı durumu da beraberinde getirdiği değerlendirilmektedir.

Ülkemizde de farklı sektörlerde birtakım veri lokalizasyonu düzenlemeleri olup, lokalizasyon kurallarının ağırlığının da sektörden sektöre çeşitlilik arz ettiği söylenebilir. Bugüne kadar düzenlenmiş en ağır lokalizasyon kuralının ise KVKK'nin 12 Mart 2024 tarihli ve 32487 sayılı Resmî Gazete'de yayımlanan 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile değişiklik yapılmadan önceki halinin olduğu değerlendirilmektedir. Şöyle ki; değişiklik öncesi KVKK; kişisel verilerin yurt dışına aktarımına ancak ilgili kişilerden açık rıza alınması, verilerin aktarılacağı ülke hakkında Kişisel Verileri Koruma Kurulu tarafından alınmış bir yeterlilik kararı bulunması veya verilerin aktarılacağı veri sorumlusu ya da veri işleyen ile Kurul tarafından onaylanmış bir yazılı taahhütname bulunması şartlarından birinin sağlanmasıyla izin veriyordu. Kişisel Verileri Koruma Kurulunun herhangi bir ülke hakkında yeterlilik kararı vermemiş olması ve yazılı taahhütname onayı sürecinin oldukça yavaş izlemesi her kişisel veri aktarımı için ilgili kişilerin açık rızasının alınmasını zorunlu hale getiriyordu. Bu da özellikle milyonlarca ilgili kişinin verisini işleyen çok uluslu şirketler başta olmak üzere veri sorumluları için bürokratik yük oluşturuyor, kişisel verilerin hukuka aykırı olarak yurt dışına aktarılmasına sebep oluyordu. Bu durum, KVKK'nin değişiklik öncesi döneminde kişisel verilerin yurt dışına aktarılmasını de facto olarak yasaklandığı izlenimine sebep olmuştur. KVKK'de gerçekleştirilen değişiklik sonrasında kişisel verilerin yurt dışına aktarım kuralları GVKT ile uyumlu hale getirilmiş ve ülkemizde kişisel veriler konusunda "zorlaştırılmış veri aktarımı" politikası izlenmeye başlanmıştır.

Kişisel veriler dışında ülkemizde; kamu kurumları tarafından işlenen veriler ve sağlık, sermaye piyasası, bankacılık, finans ve telekomünikasyon sektörlerinde veri lokalizasyonu politikaları bulunmaktadır. Bu politikaların hiçbirinde katı veri lokalizasyonu kuralı benimsenmemiş; çoğunlukla yumuşak veri lokalizasyonu, nadiren de karma veri lokalizasyonu kuralları düzenlenmiştir. Telekomünikasyon verileri için veri lokalizasyonu açısından detaylı düzenlemelere yer verilmiştir. Öncelikle EHK ile trafik ve konum verilerinin yurt dışına aktarılmasında ilgili kişilerin

açık rızalarının alınması şartı getirilerek zorlaştırılmış veri aktarım kuralı benimsenmiştir. Trafik ve konum verileri; ulusal mevzuatımızda her ne kadar özel nitelikli kişisel veri olarak kabul edilmese de, bireylerin yaşantısı hakkında doğru ve detaylı bilgiler sağlayabileceğinden ve davranış örüntülerini gerçeğe yakın bir şekilde ortaya koyabileceğinden birçok ülke mevzuatında hassas veri olarak nitelendirilmektedir. Bu sebeple trafik ve konum verilerinin aktarılması konusunda ilgili kişilerin Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik kapsamında bilgilendirilmeleri ve bu doğrultuda aktarıma kendi iradeleriyle karar vermelerinin düzenlenmesi, bireylerin mahremiyeti ve kişisel verilerinin korunması açısından önem arz eden bir düzenlemedir. Ayrıca söz konusu düzenlemelerde, tüm iletişim verilerinin aktarımına yönelik genel bir yasak getirilmemiş; yalnızca trafik ve konum verileri gibi bazı verilerin aktarımı açık rıza şartına bağlanmıştır. Bu veriler için doğrudan bir veri lokalizasyonu zorunluluğu öngörülmediğinden ve yalnızca aktarım sürecine belli kısıtlamalar getirildiğinden, düzenlemelerin orantılı ve ölçülü olduğu söylenebilir

Bunlara ek olarak 5651 Sayılı Kanun ve 29 Eylül 2020 tarihli ve 2020/DK-İD/274 sayılı Kurul Kararı ile Türkiye'de günlük erişimi bir milyondan fazla olan sosyal ağ sağlayıcıların kullanıcı verileri için karma veri lokalizasyonu, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile imza doğrulama verisi ve elektronik sertifika verisi için yumuşak veri lokalizasyonu, aynı Yönetmelik ile imza oluşturma verisi için karma veri lokalizasyonu, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik ile KEP sistemine ilişkin veriler için yumuşak veri lokalizasyonu, 22 Ocak 2018 tarihli, 2018/DK-YED/27 sayılı ve "112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call)" konulu Kurul Kararı ile bağlantılı araçlardaki e-Call ve katma değerli hizmetlerin sunumuna imkan sağlayan haberleşme sistemlerindeki veriler için karma veri lokalizasyonu, aynı Kurul Kararı ile bu sistemdeki kişisel veriler için zorlaştırılmış veri aktarımı, 12 Şubat 2019 tarihli, 2019/DK-TED/053 sayılı ve "Uzaktan Programlanabilir SIM Teknolojileri (eSIM)" konulu Kurul Kararı ile eSIM süreçlerinde işlenen veriler için karma veri lokalizasyonu kurallarının benimsendiği değerlendirilmektedir.

Veri lokalizasyonu politikalarının katı bir şekilde uygulanması, internetin yapısına aykırı olarak değerlendirilmekte ve elde edilmesi hedeflenen amaçlar bakımından bu politikaların orantılı ve ölçülü bir yöntem olmadığı kabul edilmektedir. Katı lokalizasyon kurallarının uygulanması, Rusya ve Çin örneğinde görüldüğü gibi, vatandaşların dış dünyadan soyutlanmasına ve bilgiye erişim ve ürün ile hizmetlerden faydalanma konusunda diğer ülke vatandaşlarına göre dezavantajlı konuma düşmelerine sebep olmaktadır.

Literatürde katı veri lokalizasyonu politikalarının yerel ekonomiyi geliştireceğini savunan görüşler mevcuttur. Bu görüşlere göre, veri lokalizasyonu politikaları sayesinde yabancı şirketlerin kuralların uygulandığı ülkeye yatırım yapması zorunlu hale gelecek ve yerel veri merkezlerinin müşteri portföyü genişleyecektir. Ayrıca yerel veri merkezleri barındırdıkları veriyi kullanarak yenilikçi projeler üretebilecek ve çok uluslu şirketlerle rekabet edebilir hale gelme ihtimali yükselecektir. Bu durum kuralların uygulandığı ülkelerde yeni iş imkanlarının oluşmasını sağlayabilecektir. Ancak, yapılan araştırmalara göre veri lokalizasyonu politikaları gayrisafi yurt içi hasılada düşüşe sebep olmakta ve az önce sayılan faydaları öngörülen düzeyde oluşturmamaktadır. Katı veri lokalizasyonu politikaları; uluslararası ticaretin gelişmesinin önünde engel teşkil edebilecek ve özellikle çok uluslu şirketlerin sunduğu ürün ve hizmetlerin kuralların uygulandığı ülkeye yatırım yapmasını engelleyebilecektir. Veri merkezi kiralama veya oluşturma maliyetlerinin yüksek olması, kalifiye personel istihdamının zor olması, kalifiye olmayan personelin veri merkezlerinde çalıştırılamayacak olması ve personel eğitiminin uzun sürecek olması gibi unsurlar, şirketlerin regülasyona uyumluluk maliyetlerini oldukça yükseltecektir.

Tüm bu sebeplerle, yukarıda sayılan önerilere ek olarak;

- Verilerin tümüne tek tip bir lokalizasyon zorunluluğu uygulamak hem teknik hem de ekonomik açıdan sürdürülebilir olmayan sonuçlar doğurabilecektir. Bu nedenle, verilerin mahiyeti, hassasiyeti ve risk düzeyi esas alınarak bir sınıflandırma yapılması, daha dengeli ve etkili bir veri lokalizasyon politikasının temelini oluşturmalıdır. Örneğin; milli güvenlik, kamu düzeni veya kritik altyapılarla doğrudan ilişkili telekomünikasyon verileri “kritik veri”

kategorisine alınarak kesin lokalizasyon yükümlülüğüne tabi tutulabilirken, pazarlama analitiği gibi ikincil kullanım verileri için daha esnek çözümler geliştirilebilir. Böyle bir kademeli yaklaşım, hem güvenlik ve mahremiyet gereksinimlerini karşılayabilecek hem de teknoloji şirketlerinin küresel ağlara entegrasyonunu engellemeden dijital ekonominin gelişmesine katkı sağlayabilecektir. Ayrıca, veri sınıflandırmasının belirli kriterlere ve denetlenebilir standartlara dayanması, uygulamada keyfi kararların önüne geçerek hukuk devleti ilkesini de güçlendirecektir.

- Günümüz dijital ekonomisinde veri, sadece yerel değil aynı zamanda uluslararası düzeyde değer kazanan bir varlık niteliği taşımaktadır. Bu nedenle, verilerin yurt dışına aktarımını mutlak biçimde yasaklayan veya izin süreçlerini belirsiz ve ağır bürokratik engellere tabi tutan bir yaklaşım, hem inovasyonun önünde engel oluşturabilecek hem de küresel rekabet gücünü zayıflatabilecektir. Veri transferinin belirli kriterlere dayalı şekilde, denetlenebilir ve şeffaf bir izin süreciyle yönetilmesi sağlanmalıdır. Bu kapsamda, verilerin aktarılması istenen ülkedeki güvenlik standartları, veri işleme amaçları, yasal koruma seviyesi gibi unsurlar dikkate alınarak risk temelli bir değerlendirme yapılabilir. Bir veri lokalizasyonu politikası tesisinden önce Siber Güvenlik Başkanlığı koordinasyonunda, ilgili sektörün düzenleyici otoritesinin – örneğin telekomünikasyon verileri için BTK'nin – KVKK'nin ve uzman kurum ve kuruluşlardan üyelerin katılımıyla oluşturulacak bir kurul veya komisyonun etraflı değerlendirmelerinin esas alınmasının yerinde olacağı düşünülmektedir. İlave olarak sektör bazlı yapılan veri lokalizasyonu düzenlemelerinde ilgili sektörde faaliyet gösteren aktörlerin -elektronik haberleşme sektörü özelinde işletmecilerin- görüşlerinin de dikkate alınmasının faydalı olacağı değerlendirilmektedir. Türkiye'de, özellikle telekomünikasyon sektörü gibi büyük veri işlenen alanlarda, bu tür esnek ve denetlenebilir mekanizmaların kurulması, hem yasal uyumu kolaylaştıracak hem de dijital dönüşüm süreçlerini hızlandıracaktır.
- Veri lokalizasyonu politikalarında katı kuralların benimsenmesinden kaçınılması önerilmektedir. Kişisel verilerin korunması alanında katı, yumuşak veya karma veri lokalizasyonu politikalarındansa zorlaştırılmış veri aktarımı

kuralları tercih edilmelidir. Zira burada esas olan vatandaşın mahremiyetini korumak olduğundan, bireylerin kişisel verilerinin geleceğine karar verme yetkilerinin de kendilerinde olması gerektiği unutulmamalıdır. Zorlaştırılmış veri aktarımı kuralları düzenlenirken de bu kuralların sağlayacağı faydalar ile beraberinde getireceği risklerin orantılı olup olmadığı tespit edilmelidir. Telekomünikasyon verileri, kritik altyapıya ilişkin bilgiler içerdiğinden ve bireylerin mahremiyeti ile kamu menfaatinin sağlanması ile milli güvenliğin korunması amacını içerdiğinden yumuşak ve karma veri lokalizasyonunun düzenlenmesi makul görülebilir. Veri lokalizasyonu politikası düzenlemeden önce de yukarıda belirtilenlere ek olarak verilerin hassasiyeti, işlemenin amacı ve bağlamı, veri yerelleştirme tedbirlerinin hedeflere ulaşmada ne ölçüde etkili olduğu, yürürlüğe konabilecek daha az kısıtlayıcı bir tedbir olup olmadığı, tedbirlerin doğrudan ve dolaylı, ulusal ve uluslararası etkileri ve diğer ülkelerin de aynı tedbiri benimsemesi halinde ortaya çıkabilecek sonuçlar beraberce değerlendirilmelidir.

- Veri lokalizasyonu kuralları, genel ve global politikaların benimsenmesinden ziyade başta ülkenin, sonrasında ise ilgili sektör ve konunun spesifik ihtiyaçları doğrultusunda tasarlanmalıdır. Veri lokalizasyonu kurallarının düzenlenmesinden önce bu kurallar ile neyin amaçlandığı detaylı bir şekilde tartışılmalıdır. Amaçların belirlenmesinden sonra, bu amaçların sağlanması için lokalizasyon kuralının yürürlüğe konulmasının gerekli olup olmadığı incelenmelidir. Veri lokalizasyon kurallarının gerekli olduğuna kanaat getirilmesi durumunda, amaç ve gereklilik analizinden de faydalanılarak katı, yumuşak ya da karma veri lokalizasyonu gibi politikalardan hangisinin uygulanacağına karar verilmelidir. Tüm bu süreç içerisinde veri lokalizasyonu kurallarının yerel ekonomiye ve bireylerin mahremiyetine, kişisel verilerinin korunmasına ve temel hak ve hürriyetlerine karşı oluşturduğu etki dikkate alınmalı ve ölçülülük ile orantılılık ilkesi çerçevesinde hareket edilmelidir.
- Veri lokalizasyonu politikaları hazırlanırken yalnızca ekonomik ve teknik etkiler değil, bireylerin temel hak ve özgürlükleri üzerindeki etkiler de dikkate alınmalıdır. Özellikle telekomünikasyon verileri gibi kullanıcıların iletişim mahremiyetine ve özel hayatına doğrudan temas eden veri türlerinde,

düzenlemelerin ifade özgürlüğü, haber alma hakkı ve kişisel verilerin korunması gibi hakları nasıl etkilediği mutlaka değerlendirilmelidir. Bu bağlamda, veri lokalizasyonu ile ilgili her yeni mevzuat taslağı için sistematik bir etki analizi yapılması düzenlenebilir. Özellikle yüksek riskli veri işlemede kullanılacak altyapı ve politikalar için yasal düzenlemeler öncesinde hak temelli, nesnel ve uzman görüşlerine dayanan analizlerin zorunlu hale getirilmesi büyük önem taşımaktadır. Böylece yalnızca verinin yerinin değil, veri üzerinde bireylerin sahip olduğu hakların da korunması sağlanarak, güvenlik ve özgürlük arasında daha dengeli bir politika tasarımı mümkün hale gelebilecektir.

Özetle, veri lokalizasyonu politikaları, özellikle telekomünikasyon verisi gibi stratejik öneme sahip veri türlerinde bireylerin mahremiyetini koruma ve milli güvenliği güçlendirme gibi önemli faydalar sunmaktadır. Ancak bu politikaların tek boyutlu ve katı biçimde uygulanması; yüksek altyapı maliyetleri ve küresel teknolojiye erişimde kısıtlamalar gibi ciddi sakıncalar doğurabilir. Bu nedenle, veri lokalizasyonunun faydalarından azami düzeyde yararlanırken dezavantajlarını dengeleyebilmek için risk temelli, şeffaf, esnek ve insan hakları merkezli bir yaklaşım benimsenmelidir. Böylece hem milli çıkarların korunması hem de dijital dönüşümün sürdürülebilirliği arasında sağlıklı bir denge kurulabilecektir.

KAYNAKLAR

Akgül, Aydın. *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, (Beta, 2016).

Article 29 Working Party, *Guidelines on consent under Regulation 2016/679,* 10 Nisan 2008. https://ec.europa.eu/newsroom/article29/items/623051/en, (10.09.2024).

Article 29 Working Party, *Opinion 4/2007 on the concept of personal data,* 20 Haziran 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, (10.09.2024).

Aşıkoğlu, Şehriban İpek. "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-" *Kişisel Verileri Koruma Dergisi* 1, sy. 2 (Aralık 2019): 41-65. https://dergipark.org.tr/en/download/article-file/904836 (13.10.2024).

Atalay, Muhammet ve Çelik, Enes. "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları" *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 9, s.22 (Aralık 2017): 155-172. https://dergipark.org.tr/tr/download/article-file/387269 (19.09.2024).

Atlı, Turan. "Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi." *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* 2, sy.1 (Haziran 2019): 4-22. https://dergipark.org.tr/en/download/article-file/747023 (14.06.2024).

Avrupa Birliği Adalet Divanı Kararı, 1 Ekim 2019 günlü, C-673/17 sayılı karar.

Avrupa Birliği Adalet Divanı Kararı, 20 Eylül 2020 günlü, C-793/10 ve C-794/19 sayılı karar.

Avrupa İnsan Hakları Mahkemesi Kararı, 4 Mayıs 2000 tarihli, 28341/95 başvuru nolu Rotaru/Romanya kararı.

Avrupa İnsan Hakları Mahkemesi Kararı, 5 Eylül 2017 tarihli, 61496/08 başvuru nolu Bărbulescu/Romanya kararı.

Avrupa İnsan Hakları Mahkemesi Kararı, 25 Nisan 1978 tarihli, 5856/72 başvuru nolu Tyrer/Birleşik Krallık kararı.

Azmeh, Shamel ve Foster, Christopher, "The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements" *Working Paper Series* 16, sy.175 (Ocak 2016).

Bilgi Teknolojileri ve İletişim Kurumunun 22 Ocak 2018 tarihli ve 2018/DK-YED/27 sayılı 112 Tabanlı Araç İçi Acil Çağrı Sistemi (E-Call) konulu Kurul Kararı, 2018, https://www.btk.gov.tr/uploads/boarddecisions/112-tabanli-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanli-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf (1.08.2024)

Bilgi Teknolojileri ve İletişim Kurumunun 12 Şubat 2019 tarihli ve 2019/DK-TED/053 sayılı Uzaktan Programlanabilir SIM Teknolojileri (eSIM) konulu Kurul Kararı, 2019, https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf (1.08.2024)

Bilgi Teknolojileri ve İletişim Kurumunun 29 Eylül 2020 tarihli ve 2020/DK-İD/274 sayılı Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar konulu Kurul Kararı, 2020, https://www.btk.gov.tr/uploads/boarddecisions/sosyal-ag-saglayici-hakkinda-usul-ve-esaslar/274-2020-web.pdf (1.08.2024)

Bilir, Faruk. "Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır" *TRT Akademi* 6, sy.11 (Ocak 2021): 172-181. https://dergipark.org.tr/en/download/article-file/1543414 (19.10.2024).

Birleşmiş Milletler, *UN rights chief urges protection for individuals revealing human rights violations*, 12 Temmuz 2013. https://news.un.org/en/story/2013/07/444512, (21.10.2024).
Bowman, Courtney M. "A Primer on Russia's New Data Localization Law", *Proskauer*, 27 Ağustos 2015, https://privacylaw.proskauer.com/2015/08/articles/data-privacy-laws/a-primer-on-russias-new-data-localization-law/ (16.09.2024).

Bruce, Miranda, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair ve Federico Varese. "Mapping the global geography of cybercrime with the World Cybercrime Index" *PLoS ONE* 19, sy.4, Nisan, 2024, 1-16. https://doi.org/10.1371/journal.pone.0297312.
Burman, Anirudh ve Sharma, Upasana. "How Would Data Localization Benefit India?" *Carnegie Endowment for International Peace*, Nisan 2021, https://carnegie-production-assets.s3.amazonaws.com/static/files/202104-Burman_Sharma_DataLocalization_final.pdf, (20.09.2024).

Cadwalladr, Carole ve Graham-Harrison, Emma. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" *The Guardian*, 17 Mart 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, (27.06.2024).

Castro, Daniel ve Mcquinn, Alan. "Cross-Border Data Flows Enable Growth in All Industries" *Information Technology & Innovation Foundation*, Şubat 2015.
Chander, Anupam ve Lê, Uyên P. "Data Nationalism" *Emory Law Journal* 64, sy.3 (2015): 677-739.
https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=elj (21.04.2024).

Chin, Yik-Chan ve Zhao, Jingwu. "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits" *Laws* 11, sy. 4. 2022: 63-85. https://doi.org/10.3390/laws11040063.

Clifford, Daiman ve Ausloos, Jef. "Data Protection and the Role of Fairness" *Yearbook of European Law*, 37 2018: 130-187. https://doi.org/10.1093/yel/yey004.

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*. 2018. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, (11.10.2024).

Cory, Nigel. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" *Information Technology & Innovation Foundation*, Mayıs 2017. https://www2.itif.org/2017-cross-border-data-flows.pdf, (13.10.2024).

Coşlu, Eda. “Veri Madenciliği” *Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri*, Antalya: Akdeniz Üniversitesi, Ocak 2013: 615-619.

Dalkılınç, Sümeyye. “'Kanuna uygun olmadığından PayPal'ın lisans başvurusu onaylanmadı'” *Anadolu Ajansı*, 2 Haziran 2016, https://www.aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825, (19.10.2024).

Digital Europe, *Encryption: finding the balance between privacy, security and lawful data access*, 16 Mart 2020. https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/, (21.10.2024).

Doğan, Ferdi ve Türkoğlu, İbrahim. “Derin Öğrenme Modelleri ve Uygulama Alanlarına İlişkin Bir Derleme” *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi* 10, s.2 (Haziran 2019): 409-445. https://dergipark.org.tr/tr/download/article-file/738321 (23.08.2024).

Doğan, Korcan ve Arslantekin, Sacit. “Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum” *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi* 56, sy. 1 (Ocak 2016): 1-15. https://dergipark.org.tr/tr/download/article-file/2153482 (22.08.2024)

Eker, Remzi, Kamber Can Alkiş, Zennure Uçar ve Abdurrahim Aydın. “Ormancılıkta Makine Öğrenmesi Kullanımı” *Türkiye Ormancılık Dergisi* 24, sy.2 (Haziran 2023): 150-177. https://dergipark.org.tr/tr/download/article-file/3082355 (02.07.2024).

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *Data localisation trends and challenges, Considerations for the review of privacy guidelines,* Aralık 2020, https://www.oecd.org/en/publications/data-localisation-trends-and-challenges_7fbaed62-en.html, (01.07.2024).

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Eylül 1980, https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1729547405&id=id&accname=guest&checksum=3A723BC9D5AE35CECCD8825DD8AECD63, (01.07.2024).

Elitaş, Cemal ve Özdemir, Serkan. “Bulut Bilişim ve Muhasebede Kullanımı” *Muhasebe Bilim Dünyası Dergisi* 16, s.2 (2014): 93-108. https://core.ac.uk/download/pdf/53026209.pdf (04.07.2024).

Erdinç, Göksu Hazar. “Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi”, *Kişisel Verileri koruma Dergisi* 2, sy.1, (Haziran 2020): 1-19. https://dergipark.org.tr/en/download/article-file/1195495 (18.10.2024).
Erdoğdu, Aylin. “Bankacılık Sektöründe Kişisel Verilerin Korunması ve Müşteri İlişkileri Yönetimi.” *Kişisel Verileri Koruma Dergisi* 1, sy.2 (Aralık 2019): 87-94. https://dergipark.org.tr/en/download/article-file/904871 (12.06.2024).

European Commission, *Adequacy Decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, (20.10.2024).

European Union Agency for Criminal Justice Cooperation, *The CLOUD Act*, 22 Aralık 2022. https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf.

Federal Commissioner for Data Protection and Freedom of Information (BfDI), *Data Retention*, https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Telefon-Internet/Positionen/Vorratsdatenspeicherung.html, (20.10.2024).

Ferracane, Martina F. "The Costs of Data Protectionism" *Big Data and Global Trade Law*, Mira Burri, Londra: Cambridge University Press, 2021: 63-82.

Ferracane, Martina F. "Restrictions on Cross-Border data flows: a taxonomy" *European Centre for International Political Economy* 1 2017: 1-27. https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf, (21.10.2024).

Fraser, Erica. "Data Localisation and The Balkanisation of The Internet" *SCRIPTed* 13, sy.3 (Aralık 2016).

Fratini, Samuele. "Data localization as contested and narrated security in the age of digital sovereignty: the case of Switzerland" Information, Communication & Society 28, sy.8 (Haziran 2024).

Frontier Economics, *The Extent and Impact of Data Localisation*, 1 Haziran 2022, https://assets.publishing.service.gov.uk/media/63a1a2e88fa8f539198d9bb5/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf, (09.10.2024).

Global Data Alliance, *Cross-Border Data Policy Index*, Temmuz 2023, https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf, (07.11.2025).

Greenwald, Gleen, Ewen MacAskill ve Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, 11 Haziran 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, (14.10.2024).

Gök, Murat. "Makine Öğrenmesi Yöntemleri ile Akademik Başarının Tahmin Edilmesi" *Gazi Üniversitesi Fen Bilimleri Dergisi* 5, sy. 3 (2017): 139-148. https://dergipark.org.tr/en/download/article-file/341510 (07.08.2024).

Günal, Ayşe Nida ve Üstün, Yasin. "İş İlişkilerinde Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebebi Olarak "Meşru Menfaat"" *Kişisel Verileri Koruma Dergisi* 4, sy.2 (Aralık 2022): 1-18. https://dergipark.org.tr/en/download/article-file/2434029 (10.10.2024).

Hacker, Philipp. "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things" *International Data Privacy Law* 7, sy.4 (Eylül 2017): 266-286. https://academic.oup.com/idpl/article-abstract/7/4/266/4102081?redirectedFrom=fulltext (28.09.2024).

Hill, Jonah. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders" *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance* (2014).

Hirsch, Dennis D. “The Glass House Effect: Big Data, The New Oil, and The Power of Analogy” *Maine Law Review* 66, sy. 2 (Haziran 2014).

Kang, Cecilia ve Frenkel, Sheera. “Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users” *The New York Times*, 4 Nisan 2018, https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html , (27.06.2024).

Kaynar, Oğuz, Yasin Görmez, Mustafa Yıldız ve Ayşegül Albayrak. “Makine Öğrenmesi Yöntemleri ile Duygu Analizi” *International Artificial Intelligence and Data Processing Symposium (IDAP'16)*, Malatya: İnönü Üniversitesi, Eylül, 2016. 234-241.
Kent, Bülent. “Telekomünikasyon Sektöründe Evrensel Hizmet Kavramı” *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 16, sy.2 (2012): 169-198. https://webftp.gazi.edu.tr/hukuk/dergi/16_2_5.pdf, (01.10.2024).

Kişisel Verileri Koruma Kurulu Kararı, 03/08/2023 tarihli ve 2023/1310 sayılı “Banka mobil uygulamasında dijital parola belirlerken yüz verisinin işlenmesi suretiyle kişisel verilerin işlenmesi” konulu karar.

Kişisel Verileri Koruma Kurulu Kararı, 24.01.2019 tarih ve 2019/10 sayılı karar.

Kişisel Verileri Koruma Kurumu, *“Alenileştirme” Hakkında Kamuoyu Duyurusu*, 16.12.2020, https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU, (22.10.2024).

Kişisel Verileri Koruma Kurumu, *Açık Rıza*, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf, (20.10.2024).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, 4. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf, (19.10.2024).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf, (20.10.2024).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/3a7934b6-406e-4911-a94d-795293aa0e3d.pdf, (20.10.2024).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF, (21.10.2024).

Kokott, Juliane ve Sobotta, Christoph. “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR” *International Data Privacy Law* 3, sy.4 (Eylül 2013): 222-228. https://academic.oup.com/idpl/article/3/4/222/727206 (07.07.2024).

Kösedağ, Elif. “KVKK Tarafından Yurt Dışına Kişisel Veri Aktarımları Onaylanan Şirketler”, *KVKKHaber*, 28 Eylül 2023, https://www.kvkkhaber.net/onaylanan-yurt-disina-kisisel-veri-aktarimi-taahhutnameleri, (19.10.2024).

Küçük, Dilek ve Can, Fazlı. “Hukuki Metinlerin Otomatik İşlenmesinde Yapay Zeka Teknolojilerinin Kullanımı” Bilişim Hukuku Dergisi 6, sy.1 (Haziran 2024).

Lessig, Lawrence. *CODE Version 2.0*. New York, Basic Books, 2006.

Lynn, Samara. “Countries With The Highest Cyber Threat Risk And Ones With The Lowest: Report”, *MES Computing*, 16 Mayıs 2024, https://www.mescomputing.com/news/4208968/countries-cyber-threat-risk-ones-lowest-report, (22.10.2024).

Morphy, Erika. “Google to Comply With Brazilian Court Order” *TechNewsWorld*, 5 Eylül 2006, https://www.technewsworld.com/story/google-to-comply-with-brazilian-court-order-52830.html, (28.09.2024).

Nakashima, Ellen. “Google to Give Data To Brazilian Court” *The Washington Post*, 2 Eylül 2006, https://www.washingtonpost.com/archive/business/2006/09/02/google-to-give-data-to-brazilian-court-span-classbankheadrequest-differs-from-uss-it-saysspan/f0b42222-f508-4185-a2b4-46d215decdf4/, (28.09.2024).

National Health Commission of the People’s Republic of China, *Interpretation on Population Health Information Management Measures (Trial Implementation)*, 15.06.2014, http://en.nhc.gov.cn/2014-06/15/c_46801.htm, (21.10.2024).

Office of the Inspector General U.S. Department of Justice, *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*, Mart 2018. https://oig.justice.gov/reports/2018/o1803.pdf, (06.10.2024).

Özcan, Ali. “Büyük Veri: Fırsatlar ve Tehditler” *TRT Akademi* 6, sy. 11 (Ocak 2021): 11-30. https://dergipark.org.tr/en/download/article-file/1371552 (22.08.2024).

Özlüer Başer, Bilge, Metin Yangın ve E. Selin Sarıdaş. “Makine Öğrenmesi Teknikleriyle Diyabet Hastalığının Sınıflandırılması” *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 25, sy.1 (2021): 112-120. https://dergipark.org.tr/tr/download/article-file/1454072 (22.08.2024).

Polyakova, Alina ve Meserole, Chris. “Exporting Digital Authoritarianism: The Russian and Chinese Models”, *Foreign Policy at Brookings*, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf, (21.10.2024).

Privacy International, *What is Privacy?*, Ekim 2017. https://privacyinternational.org/explainer/56/what-privacy (03.07.2024).

Purtova, Nadezhda. “The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law” *Law, Innovation and Technology* 10, sy.1 (Mart 2018): 1-35. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036355 (07.07.2024).

Reed, Chris. *Internet Law,* London: Cambridge University Press, 2012.
Singh, Nilay Pratap. A dissertation submitted in partial fulfillment of the requirements for the Degree of Master's in Public Policy (MPP). Yüksek lisans tezi, National Law School of India University, 202. http://oldopac.nls.ac.in:8081/xmlui/bitstream/handle/123456789/968/MPP217.pdf?sequence=1&isAllowed=y (06.07.2024).

Rehman, Ikhlaq ur. "Facebook-Cambridge Analytica data harvesting: What you need to know" *Library Philosophy and Practice (e-journal)*, 2497, (2019).

Şeker, Şadi Evren. *İş Zekası ve Veri Madenciliği,* İstanbul: Cinius, 2013.

Taeihagh, Araz ve Lim, Hazel Si Min. "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks" *Transport Reviews* 39, s.1 (2018): 103-128. https://doi.org/10.1080/01441647.2018.1494640.

Tanaka, Hiroyuki, Daisuke Tsuta ve Naoto Shimamura. Data Localization Laws: Japan, *Thomson Reuters*, 18 Temmuz 2022. https://www.mhmjapan.com/content/files/00065282/Data%20Localization%20Laws%20Japan.pdf, (21.10.2024).

The University of California, *Privacy and Information Security Initiative Steering Committee Report to the President,* Ocak 2013. https://www.ucop.edu/privacy-initiative/uc-privacy-and-information-security-steering-committee-final-report.pdf, (14.10.2024).

Tuzcu Ersin, Burcu, Burcu Güray ve Ceylan Necipoğlu. "Türk Veri Koruma Hukuku 2021 İlk 5 Yılda Uygulamadaki Gelişmeler" *Moroğlu Arseven*, (2021). https://www.morogluarseven.com/wp-content/uploads/2021/02/KVKK_RoundUp_TR.pdf (26.09.2024).

Türk Dil Kurumu, "Mahremiyet" *Güncel Türkçe Sözlük,* https://sozluk.gov.tr, (03.07.2024).

Türk Dil Kurumu, "Telekomünikasyon" *Güncel Türkçe Sözlük,* https://sozluk.gov.tr, (03.09.2024).

Türkiye Büyük Millet Meclisi. *Karabük Milletvekili Cem Şahin ve İstanbul Milletvekili Şengül Karslı ile 124 Milletvekilinin Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi (2/2023) ve Adalet Komisyonu Raporu*, 21.02.2024. https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y2/T2/DosyaKomisyonRaporunuVerdi/cfb35b8a-65cc-44e7-b1bc-4764e98175b9.pdf?TSPD_101_R0=08ffcef486ab2000ff6d9063f76177c27189b7e025b25454c512ff820de1d50765a39b27bcd1a0340867382166143000c16a8f07b0ec74cc344efc58244c86db1757365a8b4157994ed518a02274a9b0deaa58622e1d44fd9b2073d0532fa767, (22.10.2024).

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, *Bilgi ve İletişim Güvenliği Rehberi*, 2020. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, (03.10.2024).

Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, *Sektörel SOME Kurulum ve Yönetim Rehberi,* Kasım 2014. https://dsy.usom.gov.tr/usom/19/02/190211090404_Sektorel%20SOME%20Rehberi.pdf (03.10.2024).
Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014*. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/some-2013-2014-eylemplani.pdf, (04.10.2024).

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf (03.10.2024).

Tüzüntürk, Selim. "Veri Madenciliği ve İstatistik" *Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 29, sy. 1 (2010): 65-90. http://www.uludag.edu.tr/dosyalar/iibfdergi/genel-dokuman/2010_1/ASL04.pdf (01.10.2024).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), *Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale*, Şubat 2019. https://www.datenschutzzentrum.de/uploads/projekte/ULD_Location-Service-Tracking.pdf (02.10.2024).

United Nations Conference on Trade and Development, *Data protection regulations and international data flows: Implications for trade and development*, 2016. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (03.10.2024).

Ünver, Akın ve Kim, Grace. "Cross-Border Data Transfers and Data Localization" *EDAM Cyber Policy Paper Series 2016/3*. Haziran 2016. https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf. (09.10.2024).

Warren, Samuel D. ve Brandeis, Louis. "The Right to Privacy", *Harvard Law Review* 4, sy. 5 (Aralık 1890): 193-220. https://docenti.unimc.it/benedetta.barbisan/teaching/2017/17581/files/the-right-to-privacy-warren-brandeis (24.07.2024).

Xiao, Z. ve Xiao, Y. "Security and Privacy in Cloud Computing" *IEEE Communications Surveys & Tutorials* 15, sy. 2 (2013): 843-859. doi: 10.1109/SURV.2012.060912.00182.
Xie, Kun, Di Yang, Kaan Ozbay ve Hong Yang "Use of Real-World Connected Vehicle Data in Identifying High-Risk Locations Based on a New Surrogate Safety Measure" *Accident Analysis and Prevention* 125 (2019): 311-319. https://www.sciencedirect.com/science/article/abs/pii/S0001457518303002 (02.10.2024).

Yatırım Ortamını İyileştirme Koordinasyon Kurulu, "Veri Aktarımına İlişkin Ulusal Politikaların Ticareti Destekleyici Çerçeveye Dönüştürülmesi", Nisan 2022, https://www.akib.org.tr/files/downloads/2024/06/e53a2f00fc734de53a2f00fc734de53a2f00fc734de53a2f00.pdf, (17.05.2025).

Yavuzdoğan Okumuş, Begüm ve Talay, Yalçın Umut. "Verilerin Türkiye'de Depolanması Yönünde Gelişmeler", *Gün+ Partners Avukatlık Bürosu*, Mayıs 2021.

https://gun.av.tr/tr/goruslerimiz/makaleler/verilerin-turkiye-de-depolanmasi-yonunde-gelismeler, (12.09.2024).

Yayboke, Erol, Carolina G. Ramos ve Lindsey R Sheppard. "The Real National Security Concerns over Data Localization" *Center of Strategic & International Studies*, Temmuz 2021, https://www.csis.org/analysis/real-national-security-concerns-over-data-localization (06.08.2024).

Zuboff, Shoshana. *The Age of Surveillance Capitalism* Londra: İngiltere, Profile Books, 2019.

Türk Mevzuatı

1 Aralık 2021 tarihli ve 31676 sayılı Resmi Gazete'de yayımlanan Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik, 2021, https://www.resmigazete.gov.tr/eskiler/2021/12/20211201-1.htm (17.07.2024).

1 Aralık 2021 tarihli ve 31676 sayılı Resmi Gazete'de yayımlanan Türkiye Cumhuriyeti Merkez Bankası'nın Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ, 2021, https://www.resmigazete.gov.tr/eskiler/2021/12/20211201-3.htm (17.07.2024).

1 Kasım 2005 tarihli ve 25983 mükerrer sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 5411 sayılı Bankacılık Kanunu, 2005, https://www.resmigazete.gov.tr/eskiler/2005/11/20051101M1-1.htm 12.07.2024) (22.10.2024).

2 Mart 2024 tarihli ve 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, 2024, https://www.resmigazete.gov.tr/eskiler/2024/03/20240312-1.htm (27.05.2024).

4 Aralık 2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu, 2004, https://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm (13.05.2024).

4 Aralık 2013 tarihli ve 28841 sayılı Resmi Gazete'de yayımlanan Bilgi Alışverişi, Takas, Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ, 2013, https://www.resmigazete.gov.tr/eskiler/2013/12/20131204-9.htm (17.07.2024).

4 Aralık 2020 tarihli ve 31324 sayılı ve Resmi Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik, 2020, https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm (24.05.2024).

5 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu, 2008, https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm (5.06.2024).

5 Ocak 2018 tarihli ve 30292 sayılı Resmi Gazete'de yayımlanan Bilgi Sistemleri Yönetim Tebliği (VII-128.9), 2018, https://www.resmigazete.gov.tr/eskiler/2018/01/20180105-9.htm (12.07.2024).

6 Aralık 2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu, 2012, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6362&MevzuatTur=1&MevzuatTertip=5 (11.07.2024).

6 Nisan 2019 tarihli ve 30737 sayılı Resmi Gazete'de yayımlanan Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ, 2019, https://www.resmigazete.gov.tr/eskiler/2019/04/20190406-6.htm (17.07.2024).

6 Temmuz 2019 tarihli ve 30823 sayılı Resmi Gazete'de yayımlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi, 2019, https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf (5.07.2024).

7 Ağustos 2014 tarih ve 29081 sayılı Resmi Gazete'de yayımlanan Kaydileştirilen Sermaye Piyasası Araçlarına İlişkin Kayıtların Tutulmasının Usul ve Esasları Hakkında Tebliğ, 2014, https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=9&MevzuatNo=19956&MevzuatTertip=5 (11.07.2024).

10 Mart 2007 tarihli ve 26458 sayılı Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmelik, 2007, https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11180&MevzuatTertip=5 (14.06.2024).

10 Mart 2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, 2018, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm (23.05.2024).

10 Mart 2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, 2018, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (23.05.2024).

10 Temmuz 2024 tarihli ve 32598 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2024, https://www.resmigazete.gov.tr/eskiler/2024/07/20240710-2.htm (23.05.2024).

11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 2023, https://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm (27.05.2024).

11 Temmuz 2014 tarihli ve 29057 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, 2014, https://www.resmigazete.gov.tr/eskiler/2014/07/20140711-5.htm (14.06.2024).

15 Ekim 2021 tarih ve 31629 sayılı Resmi Gazete'de yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik,2021, https://www.resmigazete.gov.tr/eskiler/2021/10/20211015-3.htm (29.07.2024).

15 Mart 2020 tarihli ve 31069 sayılı Resmi Gazete'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, 2020, https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm (14.06.2024).

18 Ekim 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası, 1982, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 (20.05.2024).

19 Ekim 2019 tarihli ve 30923 sayılı Resmi Gazete'de yayımlanan Vergi Usul Kanunu Genel Tebliği (Sıra No: 509), 2019, https://www.resmigazete.gov.tr/eskiler/2019/10/20191019-5.pdf (18.07.2024).

19 Eylül 2018 tarihli ve ile 30540 sayılı Resmi Gazete'de yayımlanan Veri Depolama Kuruluşlarının Faaliyet, Çalışma ve Denetim Esasları Hakkında Yönetmelik, 2018, https://www.resmigazete.gov.tr/eskiler/2018/09/20180919-2.htm (5.06.2024).
20 Ekim 2012 tarihli ve 28447 sayılı Resmî Gazete'de yayımlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı, 2012, https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (28.05.2024).

21 Haziran 2019 tarihli ve 30808 sayılı Resmî Gazete'de yayımlanan Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019, https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm (23.05.2024).

22 Kasım 2001 tarihli ve 4721 sayılı Türk Medeni Kanunu, 2001, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4721&MevzuatTur=1&MevzuatTertip=5 (23.05.2024).

22 Mayıs 2003 tarihli ve 4857 sayılı İş Kanunu, 2003, https://www.resmigazete.gov.tr/eskiler/2003/06/20030610.htm#1 (27.05.2024).

23 Mayıs 2007 tarihli ve 26530 sayılı Resmi Gazete'de yayımlanan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007, https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (18.07.2024).

23 Ocak 2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu, 2004, https://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm#1 (29.07.2024).

24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2016, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf (20.05.2024).

25 Ağustos 2011 tarihli ve 28036 sayılı Resmi Gazete'de yayımlanan Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2011, https://www.resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm (29.07.2024).

26 Eylül 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu, 2004, https://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm (20.05.2024).

27 Haziran 2013 tarih ve 28690 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, 2013, https://www.resmigazete.gov.tr/eskiler/2013/06/20130627-14.htm (12.07.2024).

28 Ocak 1981 tarihinde imzalanan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, 1981, https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf (13.05.2024).

28 Ekim 2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim hale Getirilmesi Hakkında Yönetmelik, 2017, https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm (23.05.2024).

28 Haziran 2014 tarih ve 29044 sayılı Resmi Gazete'de yayımlanan Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmelik, 2014, https://www.resmigazete.gov.tr/eskiler/2014/06/20140628-4.htm (17.06.2024).

30 Aralık 2017 tarih ve 30286 sayılı Resmî Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik, 2017, https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=24276&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5 (23.05.2024).

Yabancı Ülke Mevzuatı

Avrupa Parlamentosu ve Konseyi'nin 12 Temmuz 2002 tarihli, elektronik iletişim sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin 2002/58/EC sayılı Direktifi (Gizlilik ve Elektronik İletişim Direktifi) (*Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*), 2002, https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng, (07.11.2025).

Avrupa Parlamentosu ve Konseyi'nin 15 Aralık 1997 tarihli, telekomünikasyon sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin 97/66/EC sayılı Direktifi (*Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*), 1997, https://eur-lex.europa.eu/eli/dir/1997/66/oj/eng, (07.11.2025).

7 Kasım 2016 tarihli Çin Siber Güvenlik Kanunu (*Cybersecurity Law of the People's Republic of China*), 2016, https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3, (22.10.2024).

8 Ağustos 1980 tarihli Kraliyet Kararnamesi (Koninklijk besluit van 8 augustus 1980 betreffende het bijhouden van sociale documenten), 1980, https://www.ejustice.just.fgov.be/img_l/pdf/1980/08/08/1980080803_N.pdf (5.08.2024).

13 Aralık 1995 tarihli 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi, 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 (14.05.2024).

15 Mart 2006 tarihli 2006/24/EC sayılı Direktif, 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (02.06.2024).

16 Mart 1976 tarihli Almanya Vergi Usul Kanunu (*Abgabenordnung*), 1976, https://www.gesetze-im-internet.de/ao_1977/ (3.08.2024).

16 Temmuz 2004 tarihli Polonya Telekomünikasyon Kanunu (Telecommunications Acti), https://www.uke.gov.pl/gfx/uke/userfiles/m-pietrzykowski/telecommunications_act_en.pdf, (22.10.2024).

19 Kasım 2009 tarihli Polonya Şans Oyunları Kanunu (Ustawa o grach hazardowych), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20092011540/U/D20091540Lj.pdf, (22.10.2024).

21 Ocak 2011 tarihli ve 17 numaralı "Bankacılık Finans Kuruluşlarını Kişisel Finansal Bilgileri Korumaya Çağıran Bildiri (*Notice to Urge Banking Financial Institutions to Protect Personal Financial Information*)", 2011, http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid (16.08.2024).

23 Haziran 2021 tarihli Almanya Telekomünikasyon Kanunu (*Telekommunikationsgesetz*), 2021, https://www.gesetze-im-internet.de/tkg_2021/ (3.08.2024).

23 Mart 2018 tarihinde yürürlüğe giren Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Kanunu (The Clarifying Lawful Overseas Use of Data Act, the CLOUD Act), 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943 (4.08.2024).

26 Kasım 1979 tarihli Almanya Katma Değer Vergisi Kanunu (*Umsatzsteuergesetz),* 1979, https://www.gesetze-im-internet.de/ustg_1980/ (3.08.2024).
26 Kasım 2015 tarihli ve 664 numaralı Harita Yönetimi Tüzüğü (*The Regulation on Map Management*), 2015, http://www.lawinfochina.com/display.aspx?id=21392&lib=law (16.08.2024).

27 Nisan 2016 tarihinde kabul edilen 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR),2016, https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-Türkçe-Çeviri-AB-Bakanlığı.pdf (16.05.2024).

27 Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (16.05.2024).

28 Eylül 2015 tarihli ve 36/2015 sayılı Meksika Milli Güvenlik Yasası, https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10389-consolidado.pdf, (22.10.2024).

29 Nisan 2010 tarihli Çin Halk Cumhuriyeti Devlet Sırlarının Korunması Hakkında Kanun (*Law of the People's Republic of China on Guarding State Secrets)*, 2010, http://www.lawinfochina.com/Display.aspx?lib=law&Cgid=129605 (17.08.2024).

31.07.2014 tarihli ve 758 sayılı ve 12.08.2014 tarihli ve 801 sayılı Rusya Hükümet Kararnamesi, https://ciawifi.ru/en/articles/federal-law-on-wi-fi-in-russia, (10.10.2024).

126-FZ Rusya İletişim Federal Kanunu (Federal Law No. 126-FZ on Communications), https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_264.pdf, (10.10.2024).

149-FZ Rusya Bilgi Teknolojileri ve Bilginin Korunmasına İlişkin Federal Kanun (Federal Law No. 149-FZ on Information, Informational Technologies and Protection of Information), https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf, (10.10.2024).

152-FZ Rusya Kişisel Veri Federal Yasası (Federal Law No. 152-FZ on Personal Data), https://pd.rkn.gov.ru/docs/Federal_Law_On_personal_data.doc, (10.10.2024).

236-FZ Yabancı Kişilerin Rusya Federasyonu Topraklarında Bilgi ve Telekomünikasyon Ağı İnternet Üzerindeki Faaliyetlerine İlişkin Federal Kanunu (Federal Law no. 236-FZ on the Activities of Foreign Persons in the Information and Telecommunication Network "Internet" on the Territory of the Russian Federation), https://cis-legislation.com/document.fwx?rgn=133325, (10.10.2024).

2011 tarihli ve 63 sayılı Bireysel Kontrollü Elektronik Sağlık Kaydı Kanunu (Personally Controlled Electronic Health Record Act), 2011, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/r4738_aspassed/0000%22 (4.08.2024).

2016 tarihli ve 60 sayılı Çevrim içi Taksi Rezervasyonu İşletme Faaliyetleri ve Hizmetlerinin İdaresine İlişkin Geçici Tedbirler (*Interim Measures for the Administration of Online Taxi Booking Business Operations and Services*), 2016, http://lawinfochina.com/display.aspx?id=22963&lib=law (16.08.2024).

2016 tarihli Çevrim içi Yayıncılık Hizmetlerinin İdaresine İlişkin Düzenleme (*Provisions on the Administration of Online Publishing Services*), 2016, http://lawinfochina.com/display.aspx?id=21941&lib=law (16.08.2024).

30.12.1997 tarih ve 1336 sayılı Finlandiya Muhasebe Kanunu (Kirjanpitolaki), https://www.finlex.fi/fi/laki/ajantasa/1997/19971336, (20.10.2024).

Arşiv Kanunu (*Archiefwet*), 1995, https://wetten.overheid.nl/BWBR0007376/2024-06-19 Avusturalya Federal Gizlilik Kanunu,1988, https://www-legislation-gov-au.translate.goog/C2004A03712/latest/text?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc&_x_tr_hist=true, (5.08.2024).

Belçika Gelir Vergisi Kanunu (Wetboek van de Inkomstenbelastingen), 1992, https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1992041032&table_name=wet (5.08.2024).

Belçika Şirketler Kanunu (het Wetboek van Vennootschappen en Verenigingen), 2019, https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2019032309&table_name=wet (5.08.2024).

Bilgi ve İletişim Ağlarının Kullanımının Teşviki ve Bilginin Korunması Hakkında Kanun (*Act on Promotion of Information and Communicatons Network Utilization and Information Protection*), 2016, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG Bulut Bilişim Kanunu (*the Cloud Computing Act*), 2018, https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf, (22.10.2024).

Fransız Engelleme Tüzüğü (*Loi de Blocage, Statue n° 68-678*), https://www.entreprises.gouv.fr/files/files/enjeux/securite-economique/loi-de-blocage/guide-identification-donnees-sensibles.pdf, (22.10.2024).

Güney Kore Elektronik Finansın Denetlenmesine İlişkin Yönetmeliği, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=44455&type=part&key=8, (20.10.2024).

Güney Kore'de Mekânsal Verilerin Oluşturulması ve Yönetilmesi Hakkında Kanun, 2014, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG, (22.10.2024).

Kanada Bilgi Edinme Özgürlüğü ve Mahremiyetin Korunması Kanunu, https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00, (22.10.2024).

Sağlık Bilgi Sistemleri Uygulamaları Hakkında 2015/17 sayılı Genelge, 2015, https://dosyasb.saglik.gov.tr/Eklenti/810/0/sbsgmgenelge17pdf.pdf (5.06.2024).

Tıbbi Hizmetler Kanunu (*the Medical Services Act*), 2020, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53532&lang=ENG, (22.10.2024).

Uluslararası Anlaşmalar

1 Ocak 2019 tarihli ABD-Kore Ticaret Anlaşması (*The US-Korea Trade Agreement*), 2019, https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text, (4.08.2024).
1 Temmuz 2020 tarihli Amerika Birleşik Devletleri-Meksika-Kanada Anlaşması (*The United States-Mexico-Canada Agreement, USMCA*), 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between, (22.10.2024).

4 Kasım 1950 tarihinde imzalanan Avrupa İnsan Hakları Sözleşmesi, 1950, https://www.echr.coe.int/documents/d/echr/convention_tur, (08.05.2024).

7 Aralık 2000 tarihinde kabul edilen Avrupa Birliği Temel Haklar Bildirgesi, 2000, https://www.europarl.europa.eu/charter/pdf/text_en.pdf, (10.05.2024).

8 Kasım 2001 tarihinde imzalanan 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol, 2001, https://rm.coe.int/1680080626, (14.05.2024).

10 Aralık 1948 tarihinde kabul edilen Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi, 1948, https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/trk.pdf, (08.05.2024).

14 Aralık 1990 tarihinde yayımlanan Birleşmiş Milletler Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri, 1990, https://digitallibrary.un.org/record/43365?v=pdf, (13.05.2024).

17 Aralık 1992 tarihli Kuzey Amerika Serbest Ticaret Anlaşması (*North America Free Trade Agreement, NAFTA*), 1992, https://www.cbp.gov/trade/north-american-free-trade-agreement, (4.08.2024).

18 Mayıs 2018 tarihinde imzalanan Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması için Sözleşme (108+ Sözleşme), 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1(16.05.2024), (4.10.2024).

EKLER

BTK Veri Lokalizasyonu Anketi

1. **Ülkenizde telekomünikasyon sektöründe veri lokalizasyonuna ilişkin özel bir yasal düzenleme var mı?**

Hırvatistan-HAKOM: Hayır. Doğru anladıysak, elektronik haberleşme mevzuatında öngörülen özel bir gereklilik yoktur; ancak hem kişisel hem de kişisel olmayan veriler için yatay kurallar geçerlidir.

Herhangi bir özel ulusal güvenlik gereksinimi söz konusu olduğunda, konu HAKOM'un kapsam ve yetki alanı dışındadır.

Çek Cumhuriyeti-CTU: Evet.

Almanya-BNetzA (Bundesnetzagentur): BNetzA kapsamında değil – bilgi mevcut değil.

İrlanda-ComReg: Hayır. Kesinlik sağlamak adına, "veri yerelleştirmesi"ni, kişisel veriler veya ulusal stratejik veriler gibi belirli verilerin, üretildikleri ülkenin sınırları içinde saklanması, işlenmesi ve başka şekillerde orada kalması gerektiği anlamına gelen bir yasa veya politika olarak ele alıyoruz.

Malta-MCA: Bu konu, Bilgi ve Veri Koruma Komiserliği Ofisi (Anasayfa - IDPC) tarafından düzenlenen Malta yasalarına tabidir.

Norveç-NKOM: Kesin olarak belirtilmese de, Telekom sağlayıcılarının ulusal GDPR düzenlemelerine uyması gerektiği yasada belirtilmiştir. Ayrıca, risk ulusal güvenlikle bağlantılıysa, denetim kurumu kısıtlamalar uygulayabilir (ekomloven §3-2, §3-3, §3-6 ve sikkerhetsloven §7-1 vedrørende GNF).

Polonya-UKE: Evet.

Portekiz-ANACOM: Evet.

Slovak Cumhuriyeti-RU: Elektronik Haberleşme ve Posta Hizmetleri Düzenleme Kurumu, telekomünikasyon sektöründe veri yerelleştirmeyle ilgili herhangi bir yasal düzenleme getirmemektedir. Bildiğimiz kadarıyla, Slovak Cumhuriyeti Yatırımlar, Bölgesel Kalkınma ve Bilişim Bakanlığı (MIRRI), Avrupa Birliği'nde Kişisel Olmayan Verilerin Serbest Dolaşımı Çerçevesi (Yönetmelik) (AB) 2018/1807 sayılı Tüzük ile bağlantılı olarak veri yerelleştirme sorunlarını ele almaktan sorumludur. MIRRI şunları belirtmiştir: "Mevcut ulusal mevzuatın hukuki analizine dayanarak, kişisel olmayan verilerle ilgili herhangi bir veri yerelleştirme gereksinimi tespit edilmemiştir. Tüzüğün 4 (4) maddesi uyarınca, Slovak mevzuatındaki tüm veri yerelleştirme gereksinimleri bu web sitesinde yayınlanacaktır."

https://mirri.gov.sk/en/sections/informatization/egovernment/free-flow-of-non-personal-data-in-the-eu/

İsviçre-BAKOM: Hayır.

Birleşik Krallık-OFCOM UK: Hayır.

1.1.a. Cevabınız evet ise, yönetmeliğin adını ve kapsamı hakkında kısa bir açıklama belirtebilir misiniz? (Varsa lütfen bağlantıları ekleyin.)

Hırvatistan-HAKOM: -

Çek Cumhuriyeti-CTU: Elektronik iletişimde trafik ve konum verilerinin saklanması, iletilmesi ve imhasını düzenleyen Çek düzenlemesi, 357/2012 sayılı Kararname'dir.

Elektronik İletişim Hakkında 127/2005 sayılı Kanun'un 97(4) maddesini uygular. Şunları belirtir:

- Saklanan verilerin kapsamı (örneğin, IP adresleri, MAC adresleri, IMSI, IMEI),

- Yetkili makamlara aktarım yöntemi,

- Yasal saklama süresinden sonra imha koşulları.

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: -

Malta-MCA: -

Norveç-NKOM: -

Polonya-UKE: 12 Temmuz 2024 tarihli Elektronik Haberleşme Kanunu (2024 Yasalar Dergisi, madde 1221, değişikliklerle). Polonya dilindeki versiyon aşağıdaki bağlantıda mevcuttur: https://dziennikustaw.gov.pl/D2024000122101.pdf

Bu kanun aşağıdakileri düzenler:

1. Elektronik haberleşme faaliyetleri olarak anılacak olan elektronik haberleşme sağlama faaliyetinin yürütülmesi, icrası ve denetlenmesine ilişkin kurallar. Bu faaliyetler şunları kapsar:

a) Halka açık telekomünikasyon hizmetlerinin sunulması, kamu telekomünikasyon şebekelerinin temini, radyo ve televizyon yayınlarının dağıtımı veya yeniden dağıtımı için kullanılan şebeke ve hizmetler dâhil olmak üzere, veya ilgili hizmetlerin sağlanması; bunlar "telekomünikasyon faaliyetleri" olarak anılır.

b) Halka açık, numaradan bağımsız kişiler arası iletişim hizmetlerinin sunulması.

2. Elektronik haberleşme işletmelerinin hak ve yükümlülükleri;

3. Radyo yerel alan ağına erişim ve kullanım kuralları;

4. Elektronik haberleşme alanında savunma, devlet güvenliği, kamu güvenliği ve düzenine ilişkin görev ve sorumluluklar;

5. Avrupa uydu radyonavigasyon sistemi Galileo'nun kamuya düzenlenmiş uydu hizmetine erişim, yönetim ve kullanım kuralları;

6. Frekansların, yörünge kaynaklarının ve numaralandırma kaynaklarının yönetimine ilişkin koşullar;

7. Radyo ekipmanı kullanıcılarının hak ve yükümlülükleri;

8. Son kullanıcıların hak ve yükümlülükleri;

9. Telekomünikasyon erişimine ilişkin kurallar ve elektronik haberleşme pazarlarının düzenlenmesine dair koşullar;

10. Radyo ekipmanının karşılaması gereken gereklilikler;

11. Evrensel hizmet sağlama koşulları;

12. Halka açık elektronik haberleşme hizmetlerinin sunulmasına ve bu hizmetlere engelli son kullanıcıların erişimine ilişkin gereklilikler;

13. Halka açık elektronik haberleşme hizmetlerinin sağlanması kapsamında verilerin (kişisel veriler dâhil) işlenmesi ve elektronik haberleşme gizliliğinin korunmasına ilişkin koşullar;

14. Elektronik haberleşme konularında yetkili makamların işleyişi, ulusal diğer makamlar ve Avrupa Birliği kurumlarıyla iş birliği kuralları.

Telekomünikasyon verilerinin kaydedilmesi ve paylaşılmasına ilişkin hususlar şu maddelerde düzenlenmiştir:

1. Kanunun 43–46. maddeleri – polis, İç Gözetim Ofisi, Sınır Muhafızları, Devlet Koruma Servisi, İç Güvenlik Ajansı, Askeri Kontr-İstihbarat Servisi, Askeri Jandarma, Merkezî Yolsuzlukla Mücadele Bürosu ve Ulusal Gelir İdaresi (bundan sonra "yetkili kurumlar" olarak anılır) ile mahkeme ve savcılık için halka açık telekomünikasyon hizmeti kapsamında gönderilen veya oluşturulan belirli bilgilere erişim sağlama yükümlülüğünü düzenler;

2. Kanunun 47 ve 49. maddeleri – telekomünikasyon işletmesinin halka açık telekomünikasyon hizmetlerine ilişkin verileri saklama, depolama, yetkili kurumlara, mahkemeye ve savcıya sunma ve koruma yükümlülüğünü düzenler. Bu veriler şunlar için gereklidir:

a) Bağlantıyı başlatan son kullanıcıyı, bağlantının yönlendirildiği son kullanıcıyı, şebeke sonlandırma noktasını ve telekomünikasyon terminal ekipmanını açıkça tanımlamak,

b) Bağlantının tarih ve saatini, süresini, bağlantı türünü ve telekomünikasyon terminal ekipmanının konumunu belirlemek;

3. Kanunun 337. maddesi – kamu telekomünikasyon şebekesi işletmecisinin, acil çağrının yapıldığı şebeke sonlandırma noktasının konumuna ilişkin bilgiyi UKE Başkanına iletme yükümlülüğünü düzenler. Bu bilgi, ilgili coğrafi alandaki acil müdahale merkezine, tıbbi sevk merkezine veya yasal olarak yardım sağlamakla görevlendirilmiş birimlere ya da özel düzenlemeler temelinde arama-kurtarma faaliyetleri yürütmeye yetkili kuruluşlara iletilir.

Yukarıdaki 1. noktada belirtilen halka açık telekomünikasyon hizmeti kapsamında gönderilen veya oluşturulan bilgiler şunları içerir:

1. Halka açık telekomünikasyon hizmeti kapsamında iletilen, son kullanıcı veya telekomünikasyon terminal ekipmanı tarafından gönderilen veya alınan elektronik iletiler;

2. Halka açık telekomünikasyon hizmeti kapsamında iletilen elektronik iletilere ilişkin abone verileri; bunlar şunları içerir:

a) Kimlik verileri,

b) Atanmış numara (atanmışsa) ve sabit telekomünikasyon şebekesine bağlantı durumunda şebeke sonlandırma adresi,

c) Yazışma adresi ve abone tarafından verilmişse elektronik haberleşme amaçlı adres;

3. Elektronik haberleşme gizliliği kapsamındaki veriler, bunlar şunlardır:

a) Kullanıcıya ilişkin veriler,

b) Elektronik ileti,

c) İletim verileri: elektronik iletilerin telekomünikasyon şebekelerinde iletilmesi veya elektronik haberleşme hizmetleri için ücretlendirme amacıyla işlenen, konum verilerini içerebilen veriler; konum verileri elektronik haberleşme hizmeti kullanıcısının telekomünikasyon terminal ekipmanının coğrafi konumunu gösteren tüm verilerdir,

d) Elektronik iletinin iletimi veya ücretlendirme için gerekli olanların ötesine geçen konum verileri,

e) Şebeke sonlandırma noktaları arasında bağlantı kurma girişimlerine ilişkin veriler; buna yanıtsız bağlantılar veya bağlantının kurulduktan sonra kesildiği durumlar da dâhildir;

– bunların tümü halka açık telekomünikasyon hizmeti kapsamında iletilen elektronik iletilerle ilgilidir.

4. Diğer bir telekomünikasyon işletmesinin kamu telekomünikasyon şebekesi üzerinde ulusal dolaşım kapsamında oluşturulan veya iletilen ve halka açık telekomünikasyon hizmetiyle bağlantılı konum verileri (3(c) bendinde belirtilen);

5. Hizmet teknolojisinden bağımsız olarak cihazın Polonya topraklarındaki güncel konumunu sağlayan, halka açık telekomünikasyon hizmetiyle bağlantılı olarak oluşturulan 3(d) bendindeki konum verileri.

Slovak Cumhuriyeti-RU: Portekiz'in veri düzenlemesine ilişkin farklı mevzuatı bulunmaktadır. Mevzuatının çoğu Avrupa düzenlemelerinden kaynaklanmaktadır. Kişisel olmayan verilerle ilgili olarak, 4 Kasım tarihli ve 85/2024 sayılı Kanun Hükmünde Kararname (Avrupa Parlamentosu ve Konseyi'nin 018/1807 sayılı Tüzüğünü yürürlüğe koyan) uygulanacaktır. Kişisel verilerin işlenmesi durumunda, öncelikle Genel Veri Koruma Tüzüğü (27 Nisan 2016 tarihli ve 2016/679 sayılı Avrupa Parlamentosu ve Konseyi Tüzüğü'nü uygulayan 8 Ağustos tarihli ve 58/2019 sayılı Kanun) uygulanacaktır.

Telekomünikasyon sektöründeki düzenlemelere ilişkin olarak, öncelikli olarak uygulanabilir mevzuatlar mevcut olup, yalnızca özel olarak düzenlenmeyen konularda sektör dışı mevzuatlar ikincil olarak uygulanacaktır. Telekomünikasyon sektöründe veri korumasına ilişkin özel mevzuatımız ve (12 Temmuz tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi'ni ulusal hukuka aktaran 18 Ağustos tarihli ve 41/2004 sayılı Kanun) mevzuatımız ve meta verilere erişim ve bunların saklanmasına ilişkin özel mevzuatımız (17 Temmuz tarihli ve 32/2008 sayılı Kanun) bulunmaktadır.

Bu nedenle, ilgili veri türüne bağlı olarak sektöre özgü mevzuatlar mevcuttur. (örneğin yukarıda belirtilen meta veri mevzuatı) veya iletişim sektöründeki veri koruma mevzuatı uygulanacaktır.

Portekiz-ANACOM: -

İsviçre-BAKOM: -

Birleşik Krallık-OFCOM UK: -

1.1.b. Cevabınız evet ise, bu düzenlemeler Genel Veri Koruma Tüzüğü'nden (GDPR) farklı mıdır?

Hırvatistan-HAKOM: -

Çek Cumhuriyeti-CTU: Konum verileri, gerçek bir kişiyi tanımlayabiliyorsa GDPR kapsamında kişisel veri olarak kabul edilir. Bu nedenle, işlenmesi aşağıdaki kurallara uygun olmalıdır:

127/2005 Sayılı Kanun, Coll. - Madde 91 ve 88

- Madde 91, konum verilerini, bir kullanıcının cihazının coğrafi konumunu belirleyen veriler olarak tanımlar.

- Trafik verileri dışındaki konum verileri işleniyorsa, bunlar:

- Anonimleştirilmiş veya

- Kullanıcı onayına dayalı olarak işlenmiş olmalıdır.

- Kullanıcı, işlemenin amacı, kapsamı ve süresi hakkında bilgilendirilmeli ve onayını istediği zaman geri çekme hakkına sahip olmalıdır.

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: -

Malta-MCA: -

Norveç-NKOM: -

Polonya-UKE: Evet.

Portugal-ANACOM: Yes. Cevap a)'ya bakınız.

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

1.1.c. Cevabınız evet ise, bu düzenlemeler telekomünikasyon verilerinin yurt dışına aktarılmasına izin veriyor mu? Evet ise, hangi koşullar altında?

Hırvatistan-HAKOM: -

Çek Cumhuriyeti-CTU: No.

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: -

Malta-MCA: -

Norveç-NKOM: -

Polonya-UKE: 12 Temmuz 2024 tarihli Elektronik Haberleşme Kanunu hükümleri, belirli telekomünikasyon verilerine yalnızca 1(a) Sorusunun cevabında listelenen kuruluşların erişmesine izin vermektedir. Daha fazla aktarım konusu bu kanun kapsamında değildir.

Yetkili makamlar tarafından kişisel verilerinin işlenmesinin önlenmesi amacıyla gerçek kişilerin korunmasına ilişkin kurallar, 12 Temmuz 2024 tarihli Elektronik Haberleşme Kanunu hükümleri, belirli telekomünikasyon verilerine yalnızca 1(a) Sorusunun cevabında listelenen kuruluşların erişmesine izin vermektedir. Daha fazla aktarım konusu bu kanun kapsamında değildir.

Yetkili makamlar tarafından kişisel verilerinin işlenmesinin önlenmesi amacıyla gerçek kişilerin korunmasına ilişkin kurallar,Cezai suçların soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı ve bu verilerin serbest dolaşımı ile 2008/977/JHA sayılı Konsey Çerçeve Kararı'nın (OJ L 119, 04.05.2016, s. 89) yürürlükten kaldırılmasına ilişkin karar, aşağıdaki bağlantıdan edinilebilir:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016L0680-20160504

Bu Yönerge, 14 Aralık 2018 tarihli Suçun Önlenmesi ve Suçla Mücadele Kapsamında İşlenen Kişisel Verilerin Korunması Hakkında Kanun (2023 Hukuk Dergisi, madde 1206) ile Polonya hukuk düzenine dahil edilmiştir. Kanunun Lehçe versiyonuna aşağıdaki bağlantıdan (s. 48-68) ulaşılabilir:

https://dziennikustaw.gov.pl/D2023000120601.pdf

Portekiz-ANACOM: Meta veri düzenlemesi, bazı veri kategorilerinin diğer Devletlerin makamlarına aktarılmasına izin verir, ancak bu yalnızca cezai konularda uluslararası adli iş birliği çerçevesinde, ilgili yasalarında belirlenen kurallara uygun olarak ve bu Devletlerin Avrupa Birliği topraklarında yürürlükte olan kişisel verilerin aynı düzeyde korunmasını garanti etmeleri koşuluyla mümkündür (9. maddenin 9. maddesi).

İzin verilen veri kategorileri şunlardır (9. maddenin 1. maddesi): a) Bir iletişimin kaynağını bulmak ve tanımlamak için gerekli veriler;

b) Bir iletişimin hedefini bulmak ve tanımlamak için gerekli veriler;

c) Bir iletişimin tarihini, saatini ve süresini belirlemek için gerekli veriler;

d) İletişimin türünü belirlemek için gerekli veriler;

e) Kullanıcıların telekomünikasyon ekipmanlarını veya bunların ekipmanı olarak kabul edilenleri tanımlamak için gerekli veriler.

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: -

Birleşik Krallık-OFCOM UK: -

1.1.d. Cevabınız evet ise, telekomünikasyon verisi aktarımında hedef ülkenin AB üyesi olması fark yaratıyor mu?

Hırvatistan-HAKOM: -

Çek Cumhuriyeti-CTU: -

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: -

Malta-MCA: -

Norveç-NKOM: -

Polonya-UKE: (AB) 2016/680 sayılı Direktifin 35 ila 40. maddeleri, verilerin üçüncü ülkelere aktarılmasına ilişkin ayrı kurallar koymaktadır.

Portekiz-ANACOM: Hayır. Bu Devletler, Avrupa Birliği topraklarında yürürlükte olan kişisel verilerin korunmasına ilişkin aynı düzeyde korumayı garanti altına aldıkları takdirde veri aktarımına izin verilmektedir.

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: -

Birleşik Krallık-OFCOM UK: -

1.2.a. Cevabınız hayır ise, ülkenizde bu konuda benimsenen yaklaşım hakkında bilgi verebilir misiniz? Zorunlu veri yerelleştirmesinin olmaması, hükümet/kamu politikası ve sektör açısından nasıl değerlendiriliyor?

Hırvatistan-HAKOM: Daha önce 1) numaralı maddede belirtildiği gibi, AB'de kişisel olmayan verilerin serbest dolaşımına ilişkin yatay kurallar ve kişisel veriler için yatay hukuk olarak GDPR bulunmaktadır.

Öncelikle, AB'de kişisel olmayan verilerin serbest dolaşımına ilişkin çerçeveye ilişkin 2018/1807 sayılı Tüzük, 4. Maddede öngörülen orantılılık ilkesine uygun olarak kamu güvenliği gerekçesiyle gerekçelendirilmediği sürece veri yerelleştirme gerekliliklerini yasaklamaktadır. AB içinde kişisel olmayan verilerin serbest dolaşımını sağlamak amacıyla, Tüzük, veri yerelleştirme gerekliliklerine (verilerin AB'nin herhangi bir yerinde ücretsiz olarak depolanması ve işlenmesi) ilişkin kuralları belirlemektedir,Yetkili makamlar için verilerin erişilebilirliği (yetkili makamların verilere erişimi, verilerin başka bir Üye Devlette işlendiği gerekçesiyle reddedilemez) ve profesyonel kullanıcılar için veri aktarımı (bulut hizmeti sağlayıcıları arasında geçişi ve bireysel sağlayıcılar arasında veri aktarımını kolaylaştırma).

Üye Devletler, kanun/yönetmeliklerde belirtilen gerekçesiz veri yerelleştirme gerekliliklerini kaldırmakla yükümlüdür. Tüm gerekçeli veri yerelleştirme talepleri, Ulusal Tek Bilgi Noktası aracılığıyla kamuya açık hale getirilmeli ve Avrupa Komisyonu'na bildirilmelidir.

İkinci olarak, (yeni) Ulusal Bilgi Altyapısı Yasası (Resmi Gazete no. 72/2025) bağlantısı: https://narodne-novine.nn.hr/clanci/sluzbeni/2025_04_72_934.html 1 Mayıs 2025 tarihinde yürürlüğe girdiğinden, yürürlüğe girmesinden itibaren altı ay içinde devlet bilgi altyapısının kullanım koşulları ve yöntemleri hakkında yeni bir kararname çıkarılmalı ve veri yerelleştirme gerekliliği kaldırılmalıdır.

Ancak kişisel verileri içeren Siciller, Hırvatistan Cumhuriyeti sınırları içerisinde bulunan veri merkezlerinde saklanmalıdır.

Çek Cumhuriyeti-CTU: -

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: İrlanda'da faaliyet gösteren tüm işletmeler ve kuruluşlar, doğrudan yürürlükte olan GDPR'ye tabidir; ancak bu düzenleme, 2018 tarihli Veri Koruma Yasası ile İrlanda hukukunda da uygulanmaktadır. GDPR, kişisel verilerin nasıl toplanabileceği, saklanabileceği, işlenebileceği ve işlenebileceği konusunda AB genelinde açık kurallar koymaktadır. Bu kurallar, kişisel verilerin, kişisel verileri koruma yasalarının AB'dekinden daha zayıf olduğu üçüncü ülkelere gönderilemeyeceğini de içermektedir.

GDPR, kişisel verileri kapsar. İrlanda ayrıca kişisel olmayan verileri kapsayan AB mevzuatına da tabidir. "Avrupa Birliği'nde Kişisel Olmayan Verilerin Serbest Dolaşımı Çerçevesine

İlişkin AB Tüzüğü" (Tüzük 2017/1807). Bu Tüzük, işletmeler ve bireyler için çevrimiçi faaliyetlere erişimi artırarak rekabeti teşvik etmeyi ve dijital tek pazar hedefini desteklemeyi amaçlamaktadır. 30 Mayıs 2021 tarihinden itibaren, tüm AB Üye Devletleri, AB içinde kişisel olmayan verilerin serbest dolaşımını engelleyen tüm önlemleri yürürlükten kaldırmakla yükümlüdür.

Bu nedenle GDPR, kişisel verilerin, en azından koruma düzeyinin daha düşük olduğu yargı bölgelerine gönderilemeyeceği ölçüde yerelleştirilmesini şart koşarken, Kişisel Olmayan Verilerin Serbest Dolaşımı Tüzüğü, kişisel olmayan verilerin AB içinde yerelleştirilemeyeceğini şart koşar. Herhangi bir AB üye devletinin hükümeti tarafından benimsenen herhangi bir politika, bu Tüzüğün her ikisine de tabidir.

Malta-MCA: -

Norveç-NKOM: 1. soruya bakın, yönetmelik verilerin nerede saklanması gerektiğini belirtmiyor ancak nasıl saklanacağına dair kısıtlamalar getiriyor. Bu kısıtlamalar, verilerin Norveç dışında saklanmasını pratikte zorlaştırıyor.

Polonya-UKE: -

Portekiz-ANACOM: -

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: Telekomünikasyon altyapımızın güvenliğine ilişkin tartışmalar da göz önünde bulundurularak bu konuda görüşmeler sürdürülüyor.

Birleşik Krallık-OFCOM UK: Birleşik Krallık, genel olarak veri yerelleştirmesini zorunlu kılmaz ve ticaret anlaşmaları ve G7 Yol Haritası gibi taahhütlerde belirtildiği gibi serbest veri akışını destekler. ICO'nun sorumluluklarıyla ilgili son mevzuat olan 2015 Veri (Kullanım ve Erişim) Yasası, belirli amaçlar için veri saklamayı zorunlu kılar; özellikle de kolluk kuvvetleri ve ulusal güvenlik amaçlarıyla 12 aya kadar veri saklamak zorunda olan iletişim sağlayıcıları için. Ayrıca bkz.: VERİ YERELLEŞTİRMESİNİN KAPSAMI VE ETKİSİ.

1.2.b. Cevabınız hayır ise siber saldırı veya doğal afet gibi kriz durumlarında verilere erişim nasıl sağlanıyor?

Hırvatistan-HAKOM: NIS2 Direktifi (AB) 2022/2555, 7 Şubat 2024 tarihinde yürürlüğe giren Siber Güvenlik Yasası (Resmi Gazete no. 14/2024) ile Hırvatistan mevzuatına tamamen aktarılmıştır. Ayrıca, Siber Güvenlik Yasası'nı ikincil mevzuat olarak tamamlayan Siber Güvenlik Yönetmeliği (Resmi Gazete no. 135/2024) 30 Kasım 2024 tarihinde yürürlüğe girmiştir.

Siber saldırılar veya doğal afetlerden kaynaklanan olaylar durumunda, kriz müdahale mekanizması, https://ncsc.hr/hr/nacionalni-program-upravljanja-kibernetickim-krizama

adresinden ulaşılabilen Ulusal Siber Kriz Yönetimi Programı'na uygun olarak ulusal irtibat noktası aracılığıyla etkinleştirilecektir.

Çek Cumhuriyeti-CTU: -

Almanya-BNetzA (Bundesnetzagentur): -

İrlanda-ComReg: Bu geniş kapsamlı bir sorudur ve krize ve verilere bağlı olacaktır. Örnek olarak, İrlandalı bir elektronik iletişim hizmeti sağlayıcısına yönelik bir siber güvenlik saldırısı tehdidini ele alalım. Tarihsel olarak, İrlandalı ECS sağlayıcıları, her Ulusal Düzenleme Kurumu'nun (NRA) "kamu iletişim ağlarının bütünlüğünün ve güvenliğinin korunmasını sağlamak" da dahil olmak üzere bir dizi hedefe ulaşmayı amaçlayan tüm makul önlemleri almasını gerektiren 2002/21/EC sayılı Çerçeve Direktifi'nin (değiştirildiği ve İrlanda yasalarına aktarıldığı şekliyle) 8. Maddesine tabiydi. Bu gereklilikler, Üye Devletlerin ECS/N sağlayıcılarının "ağların ve hizmetlerin güvenliğine yönelik riskleri uygun şekilde yönetmek için uygun ve orantılı teknik ve organizasyonel önlemler almasını" sağlamasını gerektiren EECC'nin 40. Maddesi'ne de taşınmıştır. NIS Direktifi (AB 2016/1148), telekomünikasyon da dahil olmak üzere kritik sektörlerde güvenlik ve raporlama yükümlülükleri belirlerken, NIS2 Direktifi (AB 2022/2555) siber güvenlik düzenlemesinin kapsamını ve derinliğini genişletmektedir. NIS2 kapsamında, ComReg, tüm sektörleri kapsayan ve Ulusal Siber Güvenlik Merkezi tarafından koordine edilen ulusal bir siber güvenlik çerçevesine entegre edilmiş olsa da, telekom sektörü için yetkili makam olarak kalacaktır.

Doğal afetler veya şiddetli hava olayları söz konusu olduğunda, Kritik Kuruluşların Dayanıklılık Direktifi (CER) (2008/14/EC), kritik kuruluşların bu tür olaylara karşı dayanıklı olmaları için uygun önlemleri almalarını sağlamayı amaçlamaktadır.

Siber saldırılar ve doğal afetler söz konusu olduğunda, kilit noktanın sürekli proaktif hazırlık olduğunu söyleyebiliriz. Telekom operatörlerinin, teknik ve operasyonel olmak üzere tüm makul, gerekli ve orantılı önlemleri önceden almaları gerekmektedir. Bunu yaparken iki temel hedefimiz vardır: (a) yıkıcı olayların olasılığını önlemek ve (2) bir olay meydana gelirse, mümkün olan en büyük ölçüde etkisinin en aza indirilmesini sağlayarak hizmetlerin kesintiye uğramamasını veya mümkün olan en kısa sürede yeniden sağlanmasını garantilemek.

Malta-MCA: -

Norveç-NKOM: Telekom sağlayıcılarının risk yönetimi, felaket kurtarma ve yedeklilik konusunda ulusal ve AB düzenlemelerine uymaları beklenmektedir.

Polonya-UKE: -

Portekiz-ANACOM: -

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: Telekomünikasyon işletmecileri, gerektiğinde yetkililere bilgi vermek zorundadır (özellikle Telekomünikasyon Kanunu'nun 59. maddesine bakınız [SR 784.10 - 30 Nisan 1997 tarihli Telekomünikasyon Kanunu (TCA) | Fedlex]).

Birleşik Krallık-OFCOM UK: Bu, esas olarak veri sorumlularının ve veri işleyicilerinin sorumluluğundadır. Birleşik Krallık Hükümeti'nin 2030 yılına kadar bir Siber Güvenlik Stratejisi bulunmaktadır - bkz.: https://www.gov.uk/government/publications/national-cyber-strategy-2022

2. Devlet veya güvenlik yetkililerinin ulusal güvenlik veya kamu düzeni gibi nedenlerle verilere erişim talep etmesi durumunda, operatörlerin uyması gereken bir prosedür var mı? Evet ise, bu prosedürler nelerdir?

Hırvatistan-HAKOM: Hırvatistan Cumhuriyeti Telekomünikasyon Sektöründeki Tüzel ve Gerçek Kişilerin Ulusal Güvenlik Alanındaki Yükümlülüklerine Dair Yönetmelik (Resmi Gazete no. 64/2008 ve 76/2013), operatörlerin ulusal güvenlik gerekliliklerine ilgili veri saklama yükümlülüklerini düzenlemektedir.

1) Maddede belirtildiği gibi, herhangi bir özel ulusal güvenlik gerekliliği HAKOM'un kapsamı ve yetkileri dışındadır.

Çek Cumhuriyeti-CTU: -

Almanya-BNetzA (Bundesnetzagentur): "Veri yerelleştirmesi"nin dikkate alınmasının yanı sıra, Telekomünikasyon Kanunu (TKG), § 170 vd. TKG'de aşağıdakileri düzenlemektedir: Almanya'da, yükümlü telekomünikasyon şirketleri, güvenlik ve kolluk kuvvetlerine verilere erişim izni vermek için çeşitli prosedürler sağlamak zorundadır.

Söz konusu veriler, telekomünikasyonların yasal olarak dinlenmesi sırasında üretilen içerik verileri, abone verileri, envanter verileri veya trafik verileridir.

Yasal olarak dinlenme ve trafik verileri hakkında bilgi sağlama yöntemleri yalnızca özellikle ciddi suçlarda kullanılabilir. Bu, yalnızca olayın gerçeklerinin araştırılmasının başka türlü faydasız veya önemli ölçüde daha zor olacağı durumlarda mümkündür. Bu tür yasalardan biri Ceza Muhakemeleri Usulü Kanunu'dur (StPO). Bu kanun, özellikle yasal olarak dinlenmenin veya bilgi sağlanmasının izin verildiği cezai suçları belirtir. StPO'ya göre, yasal olarak dinlenme ve trafik verilerinin sağlanması genellikle bir mahkeme tarafından emredilir. Telekomünikasyonların izlenmesinin veya trafik verilerinin ifşa edilmesinin emredilebileceği diğer yasalar, Madde 10 Kanunu (G 10), Gümrük Soruşturma Hizmetleri Kanunu (ZFdG), Federal Kriminal Polis Teşkilatı Kanunu (BKAG), Federal Anayasa Koruma Kanunu (BVerfSchG) ve önleyici polis telekomünikasyon gözetimine ilişkin ilgili eyalet düzenlemeleridir. Bağlantı sahiplerine ve envanter verilerine ilişkin bilgi talepleri, talep eden makamlarca hukuki dayanakları belirtilerek yapılır.

Kamuya açık telekomünikasyon hizmetleri sunan bir telekomünikasyon sistemini işleten herkes, TKG'nin 170(1) maddesi uyarınca, faaliyete başladığı andan itibaren, hukuka uygun dinleme için kanunla öngörülen tedbirleri uygulamak üzere teknik donanıma sahip olmak ve bunların derhal uygulanmasını sağlamak için örgütsel tedbirleri almak zorundadır.

Telekomünikasyon hizmetleri sağlayan veya bu hizmetlere katılan herkes, Telekomünikasyon Kanunu'nun (TKG) 174. maddesinin (1) numaralı cümlesinin 1. cümlesi uyarınca, topladıkları envanter verilerini ve 172. madde uyarınca toplanan bağlantı sahibi verilerini, güvenlik ve kolluk kuvvetlerine karşı bilgi yükümlülüklerini yerine getirmek amacıyla kullanabilir. Yasal dinleme ve bilgi sağlama için, Telekomünikasyon Dinleme Yönetmeliği (TKÜV) ve Telekomünikasyon Dinleme ve Bilgi Sağlama Tedbirlerinin Uygulanmasına İlişkin Teknik Kılavuz (TR TKÜV) uyarınca güvenli elektronik arayüzler sağlanmalıdır. Bu kılavuzlar, yetkisiz kişilerin erişimine karşı verilerin güvenli bir şekilde iletilmesini de sağlar (TKG'nin 174. maddesinin (7) numaralı cümlesinin 1. cümlesi). TKG'nin 174. maddesinin (2) numaralı fıkrasının 1 ve 2 numaralı cümleleri uyarınca, bilgi yalnızca TKG'nin 174. maddesinin 3 ila 5. fıkraları uyarınca ve bilgiyi talep eden makamın, söz konusu verileri toplamasına izin veren bir yasal düzenlemeye dayanarak, bunu bireysel durumlarda talep etmesi halinde sağlanabilir. Bilgi talebi yazılı veya elektronik ortamda yapılmalıdır.

Abone ve envanter verilerine ilişkin bilgi taleplerine TKG'nin 174(7) maddesi ve TKÜV'nin 4. Kısmı ile bağlantılı olarak 170 TKG maddesi uyarınca ticari olarak depolanan trafik verilerine yanıt vermek için, yükümlü şirketler, Telekomünikasyon Dinleme Yönetmeliği (TKÜV) ve Telekomünikasyon Dinleme Yönetmeliği Teknik Kılavuzu (TR TKÜV) hükümlerine uygun olarak teknik ve organizasyonel önlemler almak zorundadır. Bu yükümlülük, şirketin Almanya'da faaliyete başladığı tarihten itibaren geçerlidir.

Bu bağlamda, telekomünikasyon hizmet sağlayıcıları da müşteri verilerinin toplanması ve sağlanmasıyla ilgili belirli gerekliliklere uymakla yükümlüdür. Bu, Alman Telekomünikasyon Kanunu'nun (TKG) 172. maddesi ve devamında belirtilmiştir. Ayrıntılar için lütfen eke bakınız

İrlanda-ComReg: Bu alan, 2022 tarihli İletişim (Veri Saklama) Değişiklik Yasası ile değiştirilen 2011 tarihli İletişim (Veri Saklama) Yasası tarafından yönetilmektedir. Bu yasalar uyarınca, Veri erişimi ve saklama

Standart saklama: Telekomünikasyon şirketleri, kullanıcı ve internet kaynak verilerini bir yıl boyunca saklamak zorundadır. İlgili Bakan, suç veya ulusal güvenlik gibi nedenlerle bu süreyi iki yıla çıkarabilir. İrlanda polisi (An Garda Síochána), verileri dondurmak ve saklamak için bir Saklama Emri veya verileri toplamak ve göndermek için bir Üretim Emri gibi uygun bir emir için İrlanda Yüksek Mahkemesi'ne başvurmalıdır.

Malta-MCA: -

Norveç-NKOM: Evet, bu bilgilere kimlerin ve nasıl erişebileceği ve kullanabileceği konusunda ayrıntılı düzenlemeler mevcuttur.

Polonya-UKE: 24 Temmuz 2024 tarihli Elektronik Haberleşme Kanunu'nun 43 (4) maddesi uyarınca, uygun bir kuruluş, bir telekomünikasyon işletmesiyle birlikte, uygun kuruluşun yazılı veya elektronik ortamda talepte bulunmasından itibaren 24 saat içinde, telekomünikasyon işletmesinin teknik ve mali imkânları ile Kanunun 46 (1) maddesi uyarınca çıkarılan hükümlerde belirtilen şartları dikkate alarak, telekomünikasyon işletmesinin Kanunun 43 (1) maddesinin (1) (a) ve (b) maddelerinde belirtilen verilere erişim ve kayıt koşullarını uygulama biçimini belirler. Kanunun 45 inci maddesinin (1) numaralı fıkrası

uyarınca, telekomünikasyon işletmecileri, kendileri tarafından işlenen belirli telekomünikasyon verilerinin erişilebilirliğini sağlamak ve bu verileri (Kanunun 46 ncı maddesinin (1) numaralı fıkrasına dayanılarak çıkarılan hükümlere uygun olarak) hak sahibi kuruluşlara, mahkemeye ve savcılığa, ayrı hükümlerde belirtilen esas ve usullere uygun olarak erişilebilir kılmak için teknik ve organizasyonel şartları hazırlamakla yükümlüdür.

Kanun'un 46(1) maddesi uyarınca çıkarılacak düzenlemeler üzerinde çalışmalar devam etmektedir. Bu düzenlemeler, verilere erişim ve kayıt koşullarının sağlanmasına ilişkin şartları ve yöntemleri, belirli telekomünikasyon verilerinin erişilebilir kılınması için teknik ve organizasyonel koşulların hazırlanmasını ve bunların erişilebilir kılınmasını öngörmektedir.

Kanunun 47(1) maddesinde belirtilen verilerin erişilebilir kılınma şekli ve erişilebilir kılınan verilerin türü, yapısı, kayıt yöntemi ve elektronik formata ilişkin şartlar, Kanun'un 49 (3) maddesi uyarınca çıkarılacak ve halen hazırlık aşamasında olan düzenlemelerde belirtilecektir.

Portekiz-ANACOM: Veri türüne bağlı olarak, daha önce atıfta bulunulan Meta Veri Mevzuatı'nda düzenlenen meta verilere erişim için belirli bir prosedür bulunmaktadır. Erişim yalnızca bir ceza soruşturması kapsamında izin verilmekte olup, verilere erişim yetkisi için bir hâkimin onayı gerekmektedir.

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: Telekomünikasyon işletmecilerinin gerektiğinde yetkililere bilgi verme yükümlülüğü dışında özel bir prosedür bulunmamaktadır.

Birleşik Krallık-OFCOM UK: 2016 tarihli Soruşturma Yetkileri Yasası (IPA), diğer hususların yanı sıra, Birleşik Krallık Dışişleri Bakanlığı'ndan (yani Hükümet) bir Veri Saklama Bildirimi (DRN) alan bir telekomünikasyon operatörünü, ilgili iletişim verilerini belirli amaçlar doğrultusunda saklamaya zorlayan yasal bir çerçeve sunmaktadır. Ancak bu, doğrudan bir hukuk olup genel telekomünikasyon yasaları/düzenlemelerinin kapsamı dışındadır.

3. **Bu konuyla ilgili olarak şu anda geliştirilmekte olan herhangi bir mevzuat veya politika var mı? Varsa, kısaca bilgi verebilir misiniz?**

Hırvatistan-HAKOM: -

Çek Cumhuriyeti-CTU: -

Almanya-BNetzA (Bundesnetzagentur): BNetzA kapsamında değil – bilgi mevcut değil.

İrlanda-ComReg: Bekleyen herhangi bir mevzuat veya politikadan haberdar değiliz, ancak aşağıda İrlandalı hukuk firması McCann FitzGerald'ın, eGizlilik Direktifi (Değişikliklerle birlikte 2002/58/EC sayılı Direktif) bağlamında 2002 yılında yasada yapılan değişikliğin karmaşık geçmişini anlatan bir web sayfasına bağlantı bulunmaktadır.

https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/overhaul-of-irish-data-retention-laws

Malta-MCA: -

Norveç-NKOM: Hayır, telekomünikasyon sağlayıcılarının dahil olduğu bir şey değil.

Polonya-UKE: 2. sorunun cevabında belirtilen hükümler üzerinde çalışmalar devam etmektedir.

Portekiz-ANACOM: Gerçek ve tüzel kişilere ilişkin trafik ve konum verileri ile abone veya kayıtlı kullanıcıyı tespit etmeye yönelik ilgili verilerin iletimi amacıyla elektronik haberleşmenin işlenmesine ilişkin teknik ve güvenlik şartlarının esas alındığı meta veri düzenlemelerine ilişkin bir inceleme bulunmaktadır.

Slovak Cumhuriyeti-RU: -

İsviçre-BAKOM: OFCOM, telekomünikasyon operatörlerinin telekomünikasyon verilerini yalnızca İsviçre'de veya veri koruma açısından mevzuatı İsviçre'ninkine eşdeğer olan bir ülkede işlemesi zorunluluğu getirmesinin uygunluğunu inceliyor.

Birleşik Krallık-OFCOM UK: Evet, yeni mevzuat değerlendiriliyor, buradan inceleyin:

Siber Güvenlik ve Dayanıklılık Yasa Tasarısı - GOV.UK

4. İlgili gördüğünüz ek bilgi veya belgeleri bize iletmeniz durumunda memnun oluruz.

Hırvatistan – HAKOM: -

Çek Cumhuriyeti – CTU: -

Almanya – BnetzA (Bundesnetzagentur): BNetzA kapsamında değil – bilgi mevcut değil.

İrlanda – ComReg: Şu anda bize ulaşan başka bir bilgi veya belge bulunmamaktadır.

Norveç – NKOM: -

Polonya – UKE: -

Slovak Cumhuriyeti – RU: -

İsviçre – BAKOM: -

Birleşik Krallık – OFCOM UK: -

BTK Questionnare on Data Localisation

1. **Does your country have any legal regulation specifically concerning data localization in the telecommunications sector?**

Croatia-HAKOM: No. If we understand correctly there is no specific requirements prescribed by electronic communications legal framework but horizontal rules apply to both non-personal and personal data.

In case of any specific national security requirements, then the matter is outside of the scope and competences of HAKOM.

Czech Republic-CTU: Yes.

Germany-BNetzA (Bundesnetzagentur): BNetzA (Bundesnetzagentur)

Ireland-ComReg: No. For the sake of certainty, we take "data localisation" to mean a law or policy under which certain data – such as personal data or national strategic data – must be stored, processed and otherwise remain within the borders of the country in which it was generated.

Malta-MCA: This subject is under Maltese law regulated by the office of Information and Data Protection Commissioner (Home - IDPC)

Norway-NKOM: Not specifically, but it is stated in law that Telecom providers must adhere to national GDPR regulations. In addition, the supervisory body can enforce restrictions if it the risk is tied to national security (ekomloven §3-2, §3-3, §3-6, og sikkerhetsloven §7-1 vedrørende GNF)

Poland-UKE: Yes.

Portugal-ANACOM: Yes.

Slovak Republic-RU: The Regulatory Authority for Electronic Communications and Postal Services does not impose any legal regulations concerning data localization in the telecommunications sector. As far as we know, the Ministry of Investments, Regional Development and Informatization of the Slovak Republic (MIRRI) is responsible for addressing data localizations issues in connection with the Regulation (EU) 2018/1807 on a Framework for the Free Flow of Non – Personal Data in European Union (Regulation). MIRRI has stated: "Based on legal analysis of currently applicable national legislation, no data localisation requirements on non – personal data have been identified. Per art. 4 (4) of the Regulation, all requirements for data localization in the Slovak legislation will be published on this website."

https://mirri.gov.sk/en/sections/informatization/egovernment/free-flow-of-non-personal-data-in-the-eu/

Switzerland-BAKOM: No.

United Kingdom-OFCOM UK: No.

1.1.a. If your answer is yes, could you please provide the name of the regulation and a brief description of its scope? (If available, please include links.)

Croatia-HAKOM: -

Czech Republic-CTU: The Czech regulation that governs the retention, transmission, and disposal of traffic and location data in electronic communications is Decree No. 357/2012 Coll.

- Implements Section 97(4) of Act No. 127/2005 Coll., on Electronic Communications.

- Specifies:

- Scope of retained data (e.g., IP addresses, MAC addresses, IMSI, IMEI),

- Method of transmission to authorized authorities,

- Conditions for disposal after the statutory retention period.

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: -

Malta-MCA: -

Norway-NKOM: -

Poland-UKE: Electronic Communications Law Act of 12 July 2024 (Journal of Laws of 2024, item 1221, as amended)

The Polish version is available under the following link:

https://dziennikustaw.gov.pl/D2024000122101.pdf

This law specifies:

1) the rules governing the taking-up, pursuit and control of the activity of providing electronic communications, hereinafter referred to as ‘electronic communications activities’, comprising:

a) the supply of publicly available telecommunications services, the supply of public telecommunications networks, including networks and services for the distribution or re-distribution of radio and television broadcasts, or the provision of related services, hereinafter referred to as "telecommunications activities", and

b) the provision of publicly available number-independent interpersonal communications services;

2) rights and obligations of electronic communications undertakings;

3) the rules for providing access to and use of the radio local area network;

4) tasks and responsibilities for defence, state security and public security and order, in the field of electronic communications;

5) the rules for accessing, managing and using the public regulated satellite service of the European satellite radionavigation system Galileo;

6) conditions for the management of frequencies, orbital resources and numbering resources;

7) rights and obligations of users of radio equipment;

8) the rights and obligations of end-users;

9) rules for telecommunications access and conditions for regulating electronic communications markets;

10) the requirements to be met by radio equipment;

11) conditions for the provision of universal service;

12) requirements for the provision of publicly available electronic communications services and facilities for access to those services to end-users with disabilities;

13) conditions for the processing of data, including personal data, as part providing publicly available electronic communications services and the protection of electronic communications confidentiality;

14) functioning of authorities competent in matters of electronic communications, rules of their cooperation with other national authorities and European Union institutions in the field of electronic communications regulation.

Issues relating to the recording and sharing of telecommunications data are defined in:

1) Articles 43-46 of the Act – regulating the obligation for telecommunications undertakings to ensure access to specific information sent or created as part of the publicly available telecommunications service for the Police, the Internal Surveillance Office, the Border Guard, the State Protection Service, the Internal Security Agency, the Military Counterintelligence Service, the Military Gendarmerie, the Central Anti-Corruption Bureau and the National Revenue Administration, hereinafter referred to as ‘eligible entities’, as well as for the court and prosecutor;

2) Articles 47 and 49 of the Act – regulating the obligation of a telecommunications undertaking to retain, store, make available to eligible entities, the court and the prosecutor and to protect data concerning publicly available telecommunications services necessary to:

a) unambiguously identify the termination of the network, the telecommunications terminal equipment and the end-user initiating the connection and the end-user to whom the connection is directed,

b) specify the date and time of the connection and its duration, the type of connection and the location of the telecommunications terminal equipment;

3) Article 337 of the Act – regulating the obligation of the operator of the public telecommunications network to make available to the President of UKE information on the location of the network termination point from which the call to the emergency number was made, in order to make this data available to the relevant, in territorial terms, emergency response centre, medical dispatch centre or units of services legally appointed to provide assistance or entities authorised to carry out rescue operations on the basis of specific provisions.

The information sent or created as part of the publicly available telecommunications service referred to in point 1 above include:

1) electronic messages transmitted as part of a publicly available telecommunications service, transmitted or received by an end-user or telecommunications terminal equipment;

2) subscriber data relating to electronic messages transmitted as part of a publicly available telecommunications service, including:

a) identification data,

b) assigned number, if assigned, and in the case of connection to a fixed telecommunications network also the address of the network termination,

c) correspondence address and address indicated for the purposes of electronic communications, if provided by the subscriber;

3) data covered by the confidentiality of electronic communications, which include:

a) data concerning the user,

b) electronic message,

c) transmission data, which means data processed for the purpose of transmitting electronic messages in telecommunications networks or charging for electronic communications services and may include location data, which means any data processed in a telecommunications network or as part of electronic communications services indicating the geographical location of the telecommunications terminal equipment of electronic communications services' user,

d) location data, which means location data that goes beyond the data necessary for the transmission of an electronic message or billing,

e) data on attempts to establish a connection between network termination points, including data on unsuccessful connection attempts, meaning connections between telecommunications terminal equipment or network termination points that have been set up and have not been answered by the end-user, or where the set up connections have been interrupted

– related to electronic messages transmitted as part of a publicly available telecommunications service provided;

4) location data referred to in point 3(c), created or transmitted on the public telecommunications network of another telecommunications undertaking as part of domestic roaming, created in connection with a publicly available telecommunications service provided;

5) location data referred to in point 3(d) in a way that ensures the current location of the device on the territory of Poland, regardless of the technology of the service provided, created in connection with the publicly provided telecommunications service.

Portugal-ANACOM: Portugal has different legislation that concerns data regulation. Most of its legislation derives from European regulations. If non personal data is evolved Decree-Law No. 85/2024, of November 4 (that executes Regulation (EU) 018/1807 of the European parliament and of the council) shall apply. If personal data is evolved, primarily shall be applied General Data Protection Regulation (Law No. 58/2019, of August 8 that executes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Concerning regulation in the telecommunication sector, there is legislation that is primarily applicable and only in matters that are not specifically regulated will non-sectoral legislation be subsidiarily applicable. We have specific legislation regarding data protection on the telecommunication sector and legislation (Law No. 41/2004, of August 18, that transposes into national law Directive No. 2002/58/EC of the European Parliament and of the Council of 12 July on the processing of personal data and the protection of privacy in the electronic communications sector), and specific legislation regarding the access and conservation of metadata (Law No. 32/2008, of July 17).

So, depending on the type of data concerned, sector-specific legislation (e.g. the above referred metadata legislation) or data protection legislation on te communications sector will apply

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

1.1.b. If your answer is yes, do these regulations differ from the General Data Protection Regulation (GDPR)?

Croatia-HAKOM: -

Czech Republic-CTU: Location data are considered personal data under the GDPR if they can identify a natural person. Therefore, their processing must comply with the following rules:

Act No. 127/2005 Coll. – Sections 91 and 88

- Section 91 defines location data as data determining the geographical position of a user's device.

- If location data other than traffic data are processed, they must be:

- Anonymized, or

- Processed based on user consent.

- The user must be informed about the purpose, scope, and duration of processing and has the right to withdraw consent at any time.

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: -

Malta-MCA: -

Norway-NKOM: -

Poland-UKE: Yes.

Portugal-ANACOM: Yes. Se answer a).

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

1.1.c. If your answer is yes, do these regulations permit the transfer of telecommunications data abroad? If yes, under what conditions?

Croatia-HAKOM: -

Czech Republic-CTU: No.

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: -

Malta-MCA: -

Norway-NKOM: -

Poland-UKE: The provisions of the Electronic Communications Law Act of 12 July 2024 allow access to certain telecommunications data only to the entities listed in the answer to Question 1(a). The issue of further transfers is not governed by this law.

The rules for the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, are laid down in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, p. 89), available at the following link:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016L0680-20160504

This Directive has been implemented into the Polish legal order by the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime (Journal of Laws of 2023, item 1206). The Polish language version of the Act is available at the following link (p. 48-68):

https://dziennikustaw.gov.pl/D2023000120601.pdf

Portugal-ANACOM: Metadata regulation permits the transfer of some categories of data to authorities of other States but only within the framework of international judicial cooperation in criminal matters, in accordance with the rules established in their respective laws and provided that these States guarantee the same level of protection of personal data in force in the territory of the European Union (number 9 of article 9).

The categories of data that is permitted are (number 1 of article 9): a) Data necessary to locate and identify the source of a communication;

b) Data necessary to locate and identify the destination of a communication;

c) Data necessary to identify the date, time, and duration of a communication;

d) Data necessary to identify the type of communication;

e) Data necessary to identify users telecommunications equipment, or what is considered to be their equipment.

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

1.1.d. If your answer is yes, does it make a difference whether the destination country is an EU member state when transferring telecommunications data?

Croatia-HAKOM: -

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: -

Malta-MCA: -

Norway-NKOM: -

Poland-UKE: Articles 35 to 40 of Directive (EU) 2016/680 lay down separate rules for the transfer of data to third countries.

Portugal-ANACOM: No. Provided that these States guarantee the same level of protection of personal data in force in the territory of the European Union data transmission is allowed.

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

1.2.a. If your answer is no, could you provide information on the approach adopted in your country regarding this matter? How is the absence of mandatory data localization evaluated from the perspective of government/public policy and the sector?

Croatia-HAKOM: As previously stated under 1) there are horizontal rules concerning free flow of non-personal data in the EU and GDPR as horizontal law for personal data.

Firstly, Regulation (EU) 2018/1807 on the framework for the free flow of non-personal data in the EU prohibits data localization requirements unless they are justified on grounds of public security in compliance with the principle of proportionality as prescribed in Article 4. In order to ensure the free flow of non-personal data within the EU, the Regulation lays down rules concerning data localisation requirements (free storage and processing of data anywhere in the EU), the availability of data for competent authorities (competent authorities cannot be refused access to data on the grounds that they are processed in another Member State) and the transfer of data for professional users (facilitating switching between cloud service providers and transferring data between individual providers).

Member States are required to remove any unjustified data localisation requirements laid down in laws/regulations. All justified data localisation requests shall be made publicly available via the National Single Information Point and notified to the European Commission.

Secondly, asthe (new) National Information Infrastructure Act (Official Gazette no. 72/2025) link: https://narodne-novine.nn.hr/clanci/sluzbeni/2025_04_72_934.html entered into force on 1 May 2025, a new decree on the conditions and methods of use of the government information infrastructure should be adopted within six months of the entry into force, removing the data localisation requirement.

However, Registers containing personal data should be stored in data centres located within the territory of the Republic of Croatia.

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: All businesses and organisations operating in Ireland are subject to the GDPR which has direct effect though it has also been implemented in Irish law by the Data Protection Act 2018. The GDPR sets out a clear set of EU-wide rules on how personal data may be collected, stored, processed and handled. This includes that personal data may not be sent to any third country where the laws on protecting personal data are weaker than in the EU.

The GDPR covers personal data. Ireland is also subject to EU law covering non-personal data. The "EU Regulation on a framework for the free flow of non-personal data in the European Union" (Regulation 2017/1807). This Regulation aims to promote competition and support the objective of a digital single market, by enhancing access to online activities for businesses and individuals. From 30 May 2021, all EU Member States were **required to repeal any measures that inhibited the free flow of non-personal data within the EU.**

The GDPR therefore requires that personal data be localised, at least to the extent that it may not be sent to jurisdiction where the level of protection is lower, while Regulation on the free flow of non-personal data mandates that non-personal data may not be localised within the EU. Any policy adopted by the government of any EU member state is subject to both of these Regulations.

Malta-MCA: -

Norway-NKOM: See question 1, the regulation doesn't specify where it should be stored but puts restrictions on how it is stored. These restrictions make it difficult in practice to store data outside of Norway.

Poland-UKE: -

Portugal-ANACOM: -

Slovak Republic-RU: -

Switzerland-BAKOM: Discussions are underway on this matter, taking into account the debates concerning the security of our telecommunications infrastructure.

United Kingdom-OFCOM UK: The UK, in general, does not mandate data localisation and supports free data flow, as outlined in trade agreements and commitments like the G7 Roadmap. Recent legislation relating to the ICO's responsbilities, in the Data (Use and Access) Act 2015, mandates data retention for specific purposes, specfically for communications providers who must store data for up to 12 months for law enforcement and national security purposes. See also: THE EXTENT AND IMPACT OF DATA LOCALISATION.

1.2.b. If your answer is no, in cases of crises such as cyberattacks or natural disasters, how is access to data ensured?

Croatia-HAKOM: NIS2 Directive (EU) 2022/2555 has been fully transposed into Croatian legislation by the Cybersecurity Act (Official Gazette no.14/2024) entering into force on February 7, 2024. In addition, Cybersecurity Regulation (Official Gazette no. 135/2024)

entered into force on November 30, 2024 complimenting Cybersecurity Act as secondary legislation.

In cases of cyberattacks or incidents resulting from natural disasters, the crisis response mechanism shall be activated through the national contact point according to the National Program for Cyber Crisis Management publicly available on link: https://ncsc.hr/hr/nacionalni-program-upravljanja-kibernetickim-krizama.

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): -

Ireland-ComReg: This is a broad question and it would depend on the crisis and the data. We will take, as an example, the threat of a cybersecurity attack on an Irish provider of an electronic communications service. Historically, Irish ECS providers were subject to Article 8 of the Framework Directive 2002/21/EC (as amended and as transposed into Irish law) which required each NRA to take all reasonable measures aimed at achieving a number of objectives, including "ensuring that the integrity and security of public communications networks are maintained." These requirements were carried over in Article 40 of the EECC which requires Member States to ensure that ECS/N providers "take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services". The NIS Directive (EU 2016/1148) also set security and reporting obligations across critical sectors, including telecommunications, and the NIS2 Directive (EU 2022/2555) expands the scope and depth of cybersecurity regulation. Under NIS2, ComReg will remain the designated Competent Authority for the telecom sector, though embedded within a national cybersecurity framework that covers all sectors, and that is coordinated by the National Cyber Security Centre.

As for natural disasters or severe weather events, the Critical Entities Resilience Directive (CER) (2008/14/EC) aims to ensure that critical entities take appropriate measures so that they are resilient to such events.

We would say that the key point, in the case of cyberattacks and natural disasters, is ongoing proactive preparation. Telecom operators are required to take all reasonable, necessary and proportionate measures in advance – technical and operational. In doing so, the two main goals are (a) to prevent the likelihood of disruptive events, and (2) if an event does occur, to ensure that its impact minimised, to the greatest extent possible, so that services are not interrupted or are restored as quickly as possible.

Malta-MCA: -

Norway-NKOM: Telecom providers are expected to to adhere to national and Eu regulation regarding risk management, disaster recovery and redundancy.

Poland-UKE: -

Portugal-ANACOM: -

Slovak Republic-RU: -

Switzerland-BAKOM: Telecommunications operators are required to provide information to the authorities when necessary (see in particular Article 59 of the Telecommunications Act [SR 784.10 - Telecommunications Act of 30 April 1997 (TCA) | Fedlex]).

United Kingdom-OFCOM UK: This is the responsibility of data controllers and processors in the main. The UK Government has a Cyber Security Strategy through to 2030 – see here: https://www.gov.uk/government/publications/national-cyber-strategy-2022

2. **In cases where the government or security authorities request access to data for reasons such as national security or public order, is there a procedure that operators are required to follow? If yes, what are the procedures?**

Croatia-HAKOM: Regulation on Obligations in the Area of National Security of the Republic of Croatia for Legal and Natural Persons in Telecommunications (Official Gazette no. 64/2008 and 76/2013) prescribes operators' data retention obligation related to national security requirements.

As stated under 1) any specific national security requirements are outside of the scope and the competences of HAKOM.

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): Apart from the consideration of "data localization," the Telecommunications Act (TKG) regulates the following in § 170 ff. TKG: In Germany, obligated telecommunications companies must provide security and law enforcement authorities with various procedures to grant access to data.

The data in question is either content data generated during the lawful interception of telecommunications, subscriber data, inventory data, or traffic data.

The means of lawful interception and providing information on traffic data may only be used in cases of particularly serious crime. This is only permissible if investigating the facts of the case would otherwise be futile or significantly more difficult. One such law is the Code of Criminal Procedure (StPO). It specifies in particular the criminal offenses for which lawful interception or the provision of information is permissible. According to the StPO, lawful interception and the provision of traffic data are usually ordered by a court. Other laws on the basis of which the monitoring of telecommunications or the disclosure of traffic data may be ordered are the Article 10 Law (G 10), the Customs Investigation Service Act (ZFdG), the Federal Criminal Police Office Act (BKAG), the Federal Constitution Protection Act (BVerfSchG), and corresponding state regulations on preventive police telecommunications surveillance. Requests for information on connection owners and inventory data are made by the requesting authorities, stating their legal basis.

Anyone who operates a telecommunications system that provides publicly accessible telecommunications services must, in accordance with Section 170 (1) TKG, have technical

equipment in place from the time of commencement of operations to implement legally prescribed measures for the lawful interception and must take organizational precautions to ensure their immediate implementation.

Anyone who provides telecommunications services or participates in such services may, pursuant to Section 174 (1) sentence 1 of the Telecommunications Act (TKG), use inventory data collected by them and connection owner data collected pursuant to Section 172 to fulfill information obligations toward security and law enforcement authorities. For lawful interception and the provision of information, secure electronic interfaces must be provided in accordance with the Telecommunications Interception Ordinance (TKÜV) and the Technical Guideline for the Implementation of Legal Measures for Telecommunications Interception, Provision of Information (TR TKÜV), which also ensure secure transmission of the data against access by unauthorized persons (Section 174 (7) sentence 1 TKG).

Pursuant to Section 174 (2) sentences 1 and 2 TKG, information may only be provided in accordance with paragraphs 3 to 5 of Section 174 TKG and insofar as the authority requesting the information requires this in individual cases, citing a legal provision that allows it to collect the data referred to. The request for information must be made in writing or electronically.

In order to respond to requests for information on subscriber and inventory data in accordance with Section 174 (7) TKG and on commercially stored traffic data in accordance with Section 170 TKG in conjunction with Part 4 of the TKÜV, the obligated companies must take technical and organizational precautions in accordance with the provisions of the Telecommunications Interception Ordinance (TKÜV) and the Technical Guideline for the Telecommunications Interception Ordinance (TR TKÜV). This obligation applies from the time the company commences operations in Germany.

In this context, telecommunications service providers are also obliged to comply with certain requirements regarding the collection and provision of customer data. This is stipulated in Sections 172 ff. of the German Telecommunications Act (TKG). For details, please refer to the appendix.

Ireland-ComReg: This area is governed by the Communications (Retention of Data) Act 2011 as amended by the Communications (Retention of Data) Amendment Act 2022. Under these laws, Data access and retention

Standard retention: Telecoms firms must retain user and internet source data for one year, which the relevant Minister can increase to two years for reasons like crime or national security. The Irish police (An Garda Síochána) must apply the apply to the Irish High Court for an appropriate order, being a Preservation Order to freeze and hold data, or a Production Order to gather and submit data.

Malta-MCA: -

Norway-NKOM: Yes, there are strict legislations in place detailing who and how this information can be accessed and used.

Poland-UKE: In accordance with Article 43 (4) of the Electronic Communications Law Act of 24 July 2024, an eligible entity jointly with a telecommunications undertaking, within 24

hours of the eligible entity submitting a written demand in paper or electronic form, taking into account the technical and financial capabilities of the telecommunications undertaking and the requirements laid down in the provisions issued pursuant to Article 46 (1) of the Act, determine the manner in which the telecommunications undertaking shall implement the conditions for access and recording of data referred to in Article 43 (1) (1) (a) and (b) of the Act.

Pursuant to Article 45 (1) of the Act, telecommunications undertakings are obliged to prepare technical and organizational conditions for making certain telecommunications data processed by them available and making these data available (in accordance with the provisions issued on the basis of Article 46 (1) of the Act) to eligible entities, as well as the court and the prosecutor, under the principles and in accordance with the procedures specified in separate provisions.

Work on the provisions to be issued pursuant to Article 46 (1) of the Act, which will specify the requirements and methods of ensuring the conditions for access to and recording of data and the preparation of technical and organizational conditions for making certain telecommunications data available, as well as for making them available, is in progress.

The detailed manner of making the data available and the requirements regarding the type, structure, method of recording and electronic format of the data made available, referred to in Article 47 (1) of the Act, will be specified in the provisions issued pursuant to Article 49 (3) of the Act, which is also under preparation.

Portugal-ANACOM: Depending on the type of data there is a specific procedure to access metadata regulated by the already referred Metadata Legislation. The access is only allowed regarding a criminal investigation and requires the authorization of a judge to grant the access to the data.

Slovak Republic-RU: -

Switzerland-BAKOM: There is no specific procedure in place, other than that based on the obligation of telecommunications operators to provide information to the authorities when necessary.

United Kingdom-OFCOM UK: The Investigatory Powers Act 2016 (the IPA) provides, amongst other things, a legal framework compelling a telecommunications operator in receipt of a Data Retention Notice (DRN) from the UK Secretary of State (i.e. Government) to retain relevant communications data for a set of purposes. However, this is direct law and sits outside general telecommunications laws/regulations.

3. Is there currently any legislation or policy under consideration related to this topic? If yes, could you provide a brief overview?

Croatia-HAKOM: -

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): Not within the scope of BNetzA – no information available.

Ireland-ComReg: We are not aware of any pending legislation or policy but below is a link to a webpage by Irish law firm McCann FitzGerald, which sets out the complex history to the amending of the law in 2002,, in the context of the ePrivacy Directive (Directive 2002/58/EC, as amended).

https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/overhaul-of-irish-data-retention-laws

Malta-MCA: -

Norway-NKOM: No, not that the Telco providers are involved in.

Poland-UKE: Work is currently underway on the provisions indicated in the answer to question 2.

Portugal-ANACOM: There is a review in course related to metadata regulations that focuses mainly on the terms of the technical and safety conditions under which electronic communication is processed for the purposes of transmitting traffic and location data relating to natural persons and legal entities, as well as related data necessary to identify the subscriber or registered user.

Slovak Republic-RU: -

Switzerland-BAKOM: OFCOM is currently examining the advisability of introducing an obligation for telecommunications operators to process telecommunications data only in Switzerland or in a country whose legislation is equivalent to that of Switzerland in terms of data protection.

United Kingdom-OFCOM UK: Yes, new legislation is under consideration, see here:

Cyber Security and Resilience Bill - GOV.UK

4. **We would appreciate if you could provide any additional information or documents that you deem relevant.**

Croatia-HAKOM: -

Czech Republic-CTU: -

Germany-BNetzA (Bundesnetzagentur): Not within the scope of BNetzA – no information available.

Ireland-ComReg: No further informartion or documents occur to us at this time.

Malta-MCA: -

Norway-NKOM: -

Poland-UKE: -

Portugal-ANACOM: -

Slovak Republic-RU: -

Switzerland-BAKOM: -

United Kingdom-OFCOM UK: -

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

2.12.2025

Fatmanur BEYTEKİN

ÖZGEÇMİŞ

1994 yılında Samsun'da doğdu. İlk ve orta öğretimi ile lise öğrenimini Samsun Bafra'da tamamladı. 2016 yılında Selçuk Üniversitesi Hukuk Fakültesi bölümünden mezun oldu. 2017 yılında Samsun Barosunda yasal avukatlık stajını tamamladı. Aralık 2020'de Bilgi Teknolojileri ve İletişim Kurumunda İnternet Dairesi Başkanlığında Bilişim Uzman Yardımcısı olarak göreve başladı. Şubat 2021'de Hukuk Müşavirliğine geçiş yaptı. Nisan 2024'ten beri Bursa Bölge Müdürlüğünde görevine devam etmektedir.