

**T. C.**

**İSTANBUL ÜNİVERSİTESİ**

**SOSYAL BİLİMLER ENSTİTÜSÜ**

**ÖZEL HUKUK ANABİLİM DALI**

**DOKTORA TEZİ**

**DİJİTAL ORTAMA İLİŞKİN FARKLI ÜLKE  
DÜZENLEMELERİNİN UYGULANMASI**

**Fatih Burak UZUN**

**2502140507**

**TEZ DANIŞMANI**

**Prof. Dr. Faruk Kerem GİRAY**

**İSTANBUL – 2023**

**ÖZ**

**DİJİTAL ORTAMA İLİŞKİN FARKLI ÜLKE DÜZENLEMELERİNİN**

**UYGULANMASI**

**FATİH BURAK UZUN**

Ekonomik ve sosyal faaliyetler günümüzde çok büyük ölçüde dijital ortama kaymıştır. Kişiler arasındaki hukuki işlem ya da hukuki fiillerin büyük kısmı internet vasıtasıyla ve dijital ortamda iz bırakarak gerçekleşmektedir. Bu durum kara, deniz ve hava ülkesinden bağımsız olan dijital ortama etki edecek hukuk kurallarının getirilmesi ihtiyacını doğurmaktadır. Ancak internetin ülke sınırı tanımayan yapısı, getirilen hukuk kurallarının da ülke sınırları dışında uygulanmasını gerektirmektedir. Farklı devletlerin birbirleri ile çelişen ve sınır ötesi uygulama kapsamına sahip kanunlar çıkarması halinde, “hukukların çatışması” olarak adlandırdığımız olgu meydana gelmektedir. Bu olgu bir kişinin farklı devletlerin birbirleri ile çelişen hukuk kurallarına uymak zorunda kalması halini açıklamaktadır.

Hukukların çatışması olgusunu yaratabilecek örnek düzenlemeler olan GDPR ve CLOUD Act sınır ötesi uygulama kapsamına sahip mevzuat olarak karşımıza çıkmaktadır. Bu düzenlemeler vasıtasıyla AB ve ABD; kendi ülkeleri dışındaki veriler üzerinde de egemenlik yetkisi kullanmaktadırlar.

Hem yabancı devletlerin egemenlik yetkisi kullanmalarını engellemek hem de veriler üzerinde kendi egemenlik yetkilerini rahatça kullanabilmek isteyen devletler ise veri lokalizasyonu yükümlülükleri öngörmektedir. Veri lokalizasyonu yükümlülükleri, belirli tip verilerin ilgili ülke ya da bölge sınırları içerisinde saklanmasını öngören hukuki düzenlemelerdir. Veri lokalizasyonu yükümlülükleri ülkemizde ve dünyada oldukça yaygındır.

Sınır ötesi uygulama kapsamına sahip kanunların etki alanının engellenmesi için tek başına veri lokalizasyonu gerektiren kanunlar yeterli olmamaktadır. Bunun yanında verilerin yurtdışına aktarılmasını sınırlayan ya da engelleyen kanunlara da ihtiyaç

bulunmaktadır. Öte yandan her devletin yabancı ülkelerde bulunan verilere ihtiyacı olacağından sınır ötesi uygulama kapsamına sahip kanunlara ihtiyaç olduğu açıkça ortadadır. İşte bu iki farklı pozisyon, hukukların çatışması olgularının önümüzdeki dönemde daha da yaygınlaşacağını göstermektedir. Dolayısıyla ülkemizin de hukukların çatışması durumlarını düzenleme yönünde gerekli çalışmaları yapması gerektiği düşünülmektedir.

**Anahtar Kelimeler:** Dijital ortam, CLOUD Act, kişisel veriler, veri lokalizasyonu, egemenlik.



**ABSTRACT**  
**IMPLEMENTATION OF VARIOUS NATIONAL LEGISLATIONS ON**  
**DIGITAL ENVIRONMENT**  
**FATİH BURAK UZUN**

Nowadays, economic, and social activities have largely turned to digital media. Most legal transactions or acts between individuals are carried out through the internet, leaving a mark in the digital environment. In this case, it creates the need to introduce legal rules for the digital environment that is independent of land, sea, and air country. However, the borderless nature of the internet requires the implementation of the rules of law outside the borders of the country. A phenomenon called “conflict of legal orders” occurs when different states enact laws that contradict each other and have cross-border applications. This phenomenon explains the situation that a person is forced to comply with the conflicting legal rules of different states.

GDPR and CLOUD Act, which are exemplary regulations that may lead to conflict of legal orders, appear as legislation with a cross-border scope of application. Through these regulations, the EU, and the U.S. exercise their sovereign authorities over data outside their own countries.

States that want to both prevent foreign states from exercising sovereignty and freely exercise their sovereign authority over data, envisage data localization obligations. Data localization obligations are legal regulations stipulating that certain types of data are stored within the borders of the relevant country or region. Data localization obligations are quite common in our country and around the world.

Laws requiring data localization alone are not sufficient to prevent the impact of laws with the cross-border scope of application. In addition, there is also a need for laws that limit or prevent the transfer of data abroad. On the other hand, since every state will need data located in foreign countries, there is clearly a need for laws with a cross-border scope of application. These two different positions indicate that the conflict of

legal orders will become more widespread in the coming period. Therefore, it is considered that our country should also carry out the necessary studies to regulate the conflict of legal orders.

**Keywords:** Digital environment, CLOUD Act, personal data, data localization, sovereignty.



## ÖNSÖZ

Teknoloji ve hukuk birbirleri ile son derece yakın ilişkili iki konudur. Ancak hukuk, kendi doğasına uygun olarak teknolojinin her zaman gerisinden gelmektedir. Teknolojik bir gelişme olan internetin ülke sınırlarını zayıflatan yapısına karşı bir cevap olan sınır ötesi uygulama kapsamına sahip kanunlar ile veri lokalizasyonu yükümlülükleri, beraberlerinde yeni bir hukuki problemi de getirmişlerdir. Bu kişilerin birden çok hukuk düzeninin çelişen yükümlülüklerine uyum sağlamaları hali olup hukukların çatışması kavramı altında çalışmamıza konu edilmiştir.

Çalışmamızın herhangi bir hukuk anabilim dalına ait olduğunu söylemek biraz zordur. Zira çalışmamız boyunca çok sayıda farklı hukuk alanına değinilmektedir. Tezimizin bir diğer yönü de milletlerarası özel hukuk anabilim dalı altında yazılmış olmasına rağmen, genel olarak milletlerarası özel hukukun değinmediği bir konuya değinmiş olmasıdır. Bu yolu bana açan ve çalışmam boyunca oldukça esnek davranan danışmanım Prof. Dr. Faruk Kerem Giray’a, tüm desteklerine ilave olarak bu konudaki yaklaşımı için de özellikle ve içtenlikle teşekkür ederim.

Doktora tez sürecim boyunca benden desteklerini esirgemeyen diğer danışmanlarım Prof. Dr. Leyla Berber Keser ile Doç. Dr. Abdurrahman Savaş’a da teşekkür ve şükranlarımı sunuyorum. Yine çalışmalarım boyunca değerli fikirlerini, desteklerini ve dostluklarını esirgemeyen Ar. Gör. Şehriban İpek Aşıkoğlu ile Stj. Av. Ceren Zeynep Şen’e de oldukça minnettarım. Bu çalışma sebebi ile kendilerine ayırdığım vakti oldukça azaltmak zorunda kaldığım sevgili eşim Kübra Dilara Uzun’a, annem Remziye Uzun’a ve babam Mehmet Uzun’a da yaptıkları fedakarlıklardan dolayı teşekkür etmek isterim. Doktora tezim, bu çalışmanın bitmesinden birkaç hafta önce doğan ve geleceğimiz olan oğlum Utku Alp Uzun ile Kurtuluş Savaşı’nda memleketleri Trabzon’dan İzmir’e kadar vatanın her yerinde savaşmış gazi dedelerim Alaybey, İlyas ve Mustafa’ya ithaf edilmiştir.

İstanbul

Şubat 2023

Fatih Burak Uzun

## İÇİNDEKİLER

|                          |       |
|--------------------------|-------|
| ÖZ .....                 | ii    |
| ABSTRACT .....           | iv    |
| ÖNSÖZ.....               | vi    |
| İÇİNDEKİLER .....        | vii   |
| KISALTMALAR LİSTESİ..... | xviii |
| GİRİŞ .....              | 1     |

### BİRİNCİ BÖLÜM HUKUKLARIN ÇATIŞMASI

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| I. GİRİŞ .....                                                                         | 5  |
| II. DEVLETLERİN EGEMENLİĞİ.....                                                        | 7  |
| A. Egemenlik Kavramının Tanımı.....                                                    | 7  |
| B. Egemenlik Kavramının Mekânsal Sınırları.....                                        | 9  |
| C. Dijital Ortam Üzerinde Egemenlik .....                                              | 11 |
| 1. Dijital Ortam Kavramının Tanımı.....                                                | 11 |
| 2. Dijital Ortamın Bir Egemenlik Alanı Olarak Tanımlanıp Tanımlanamayacağı Sorunu..... | 12 |
| 3. Devletlerin Dijital Ortam Üzerinde Egemenlik Sahibi Olup Olamayacağı Sorunu .....   | 14 |
| III. DEVLETİN ULUSLARARASI YETKİSİ .....                                               | 19 |
| A. Devletin Uluslararası Yetkisi Kavramı .....                                         | 19 |
| B. Devletin Uluslararası Yetkisinin Sınıflandırılması .....                            | 20 |
| 1. Düzenleme Yetkisi .....                                                             | 21 |
| 2. Uygulama Yetkisi.....                                                               | 22 |
| 3. Yargılama Yetkisi .....                                                             | 22 |
| C. Devletin Uluslararası Yetkisini Kendi Ülkesi İçerisinde Kullanması.....             | 24 |

|                                                                                                                                             |    |
|---------------------------------------------------------------------------------------------------------------------------------------------|----|
| D. Devletin Uluslararası Yetkisini Sınır Ötesi Uygulama Kapsamına Sahip Olarak Kullanması .....                                             | 25 |
| 1. Düzenleme Yetkisinin Sınır Ötesi Kullanımı .....                                                                                         | 27 |
| a. Lotus Kararı Çerçevesinde Düzenleme Yetkisinin Sınır Ötesi Kullanımı. ....                                                               | 27 |
| b. Uluslararası Teamül Hukuku Çerçevesinde Düzenleme Yetkisinin Sınır Ötesi Kullanımı .....                                                 | 29 |
| (1) Aktif Kişilik İlkesi.....                                                                                                               | 31 |
| (2) Pasif Kişilik İlkesi .....                                                                                                              | 32 |
| (3) Koruma İlkesi.....                                                                                                                      | 33 |
| (4) Evrensellik İlkesi.....                                                                                                                 | 34 |
| 2. Uygulama Yetkisinin Sınır Ötesi Kullanımı .....                                                                                          | 34 |
| 3. Yargılama Yetkisinin Sınır Ötesi Kullanımı.....                                                                                          | 36 |
| E. Devletlerin Uluslararası Yetkisini Sınır Ötesi Uygulama Kapsamına Sahip Olarak Kullanmasının Yarattığı Sorunlar ve Çözüm Yöntemleri..... | 38 |
| 1. Sorunlar .....                                                                                                                           | 38 |
| 2. Çözüm Yöntemleri .....                                                                                                                   | 39 |
| a. Çözüm Yöntemi Olarak Öne Sürülen Çeşitli Görüşler.....                                                                                   | 39 |
| b. Uluslararası Düzenleme Yetkisinin Makul Kullanımı.....                                                                                   | 40 |
| F. Dijital Ortam Üzerinde Devletlerin Uluslararası Yetkisi.....                                                                             | 44 |
| G. Değerlendirmeler.....                                                                                                                    | 45 |
| IV. DEVLETLERİN ULUSLARARASI YETKİSİ İLE MİLLETLERARASI ÖZEL HUKUK VE USUL HUKUKUNUN İLİŞKİSİ .....                                         | 46 |
| A. Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Temel Bilgiler.....                                                                    | 46 |
| 1. Milletlerarası Özel Hukuk ve Usul Hukuku Alanı Kapsamına Giren Konular .....                                                             | 46 |



|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| 2. “Milletlerarası Özel Hukuk” ya da “Kanunlar İhtilafı” Terimlerinin Kullanımı.....            | 48 |
| 3. Kanunlar İhtilafı Kurallarının Tarihi Gelişimi.....                                          | 49 |
| 4. Bazı Kanunlar İhtilafı Kavramları .....                                                      | 53 |
| B. Düzenleme Yetkisinin Sınır Ötesi Kullanımı Açısından Milletlerarası Özel Hukukun Etkisi..... | 55 |
| V. YENİ BİR KAVRAM: HUKUKLARIN ÇATIŞMASI .....                                                  | 57 |
| A. Hukukların Çatışması ile Devletlerin Uluslararası Yetkisinin İlişkisi.....                   | 58 |
| B. Hukukların Çatışması ile Kanunlar İhtilafının İlişkisi .....                                 | 59 |
| C. Hukukların Çatışmasından Doğan Sorunların Çözümüne Kavuşturulması Gerekliliği .....          | 61 |
| D. Hukukların Çatışması ile Dijital Ortamın İlişkisi .....                                      | 62 |

## İKİNCİ BÖLÜM

### KİŞİSEL VERİLERİN KORUNMASINA DAİR KANUNLARIN SINIR ÖTESİ UYGULAMA KAPSAMI

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| I. GİRİŞ .....                                                                | 64 |
| II. GDPR’IN SINIR ÖTESİ UYGULAMA KAPSAMI .....                                | 68 |
| A. GDPR Hakkında Genel Bilgiler.....                                          | 68 |
| B. GDPR’ın Sınır Ötesi Uygulama Kapsamına Sahip Olmasının Sebepleri.....      | 71 |
| C. GDPR’ın Sınır Ötesi Uygulama Kapsamına Sahip Olabilmesinin Şartları ...    | 73 |
| 1. Kuruluş Kriteri .....                                                      | 75 |
| 2. AB’ye Yönelik Mal veya Hizmet Sunmayı Hedefleme Kriteri .....              | 79 |
| 3. AB İçerisindeki Bir Kişinin Takip Edilmesi Kriteri .....                   | 82 |
| D. GDPR’ın Sınır Ötesi Uygulama Kurallarının Pratikte Yarattığı Sorunlar..... | 84 |
| III. KVKK’NIN SINIR ÖTESİ UYGULAMA KAPSAMI.....                               | 87 |
| A. KVKK’nın Yurtdışında Bulunan Veri Sorumlularına Uygulandığı Durumlar..     | 87 |

|                                                                                                                                |     |
|--------------------------------------------------------------------------------------------------------------------------------|-----|
| 1. Veri Sorumluları Sicili .....                                                                                               | 88  |
| 2. Veri Güvenliği İhlali Bildirimi.....                                                                                        | 89  |
| B. TCK'nın Yer Bakımından Uygulama Kuralları Çerçevesinde KVKK'nın Sınır Ötesi Uygulama Kapsamına Sahip Olma İmkânı .....      | 91  |
| C. KVKK'nın Sınır Ötesi Uygulama Kapsamına Dair Değerlendirmeler.....                                                          | 95  |
| IV. KVKK'NIN VE GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMI İLE MİLLETLERARASI ÖZEL HUKUK İLİŞKİSİ.....                               | 96  |
| V. KVKK'NIN VE GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMININ DEVLETLERİN ULUSLARARASI YETKİSİ AÇISINDAN DEĞERLENDİRİLMESİ .....      | 100 |
| VI. KVKK'NIN VE GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMININ HUKUKLARIN ÇATIŞMASI KAVRAMI AÇISINDAN DEĞERLENDİRİLMESİ. ....         | 103 |
| A. KVKK ve GDPR'ın Sınır Ötesi Uygulama Kapsamının Hukukların Çatışması Durumu Yaratması .....                                 | 103 |
| B. KVKK ve GDPR'ın Sınır Ötesi Uygulama Kapsamlarının Yarattığı Hukukların Çatışması Durumlarına Yönelik Çözüm Önerileri ..... | 105 |

### ÜÇÜNCÜ BÖLÜM

#### ABD HUKUKUNDA CEZA YARGILAMASI KAPSAMINDA ADLİ MAKAMLARIN DİJİTAL ORTAMDAKİ BİLGİLERE ERİŞMESİ

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| I. GİRİŞ .....                                                                            | 108 |
| A. Dijital Ortamdaki Bilgilere Erişmeye Yönelik İhtiyaçlar ve Karşılaşılan Sorunlar ..... | 108 |
| B. Bölümün İnceleme Konusu ve Kapsamı.....                                                | 110 |
| II. BULUT BİLİŞİM SİSTEMLERİNE GENEL BAKIŞ .....                                          | 111 |
| A. Bulut Bilişimin Tanımı .....                                                           | 111 |
| B. Sunulan Hizmetler Açısından Bulut Bilişim Sistemleri Çeşitleri.....                    | 112 |
| C. Veri Saklama Yöntemleri Açısından Bulut Bilişim Sistemleri Çeşitleri .....             | 115 |

|                                                                                               |     |
|-----------------------------------------------------------------------------------------------|-----|
| 1. Lokal Bulut Bilişim Sistemi.....                                                           | 115 |
| 2. Dağınık Bulut Bilişim Sistemi .....                                                        | 117 |
| 3. Erişim Yetkisi Ayırıştırılmış Bulut Bilişim Sistemi .....                                  | 119 |
| III. ABD HUKUKU ÇERÇEVESİNDE DİJİTAL ORTAMDAKİ BİLGİLERE<br>ERİŞİM İMKANLARI .....            | 120 |
| A. Giriş.....                                                                                 | 120 |
| B. Dördüncü Değişiklik Kapsamında Bilgi Talepleri.....                                        | 122 |
| 1. Dördüncü Değişiklik Hakkında Genel Bilgiler.....                                           | 122 |
| 2. Dördüncü Değişikliğin Özel Hayatın Gizliliği Hakkı (Right to Privacy) ile<br>İlişkisi..... | 124 |
| 3. Dördüncü Değişiklik Kapsamında Arama İşlemi Yapılmasının Şartları. 126                     |     |
| a. Arama İşlemi İçin Mahkeme Kararı Verilmesinin Şartları.....                                | 127 |
| (1) Makul Şüphe Bulunması .....                                                               | 127 |
| (2) Destekleyici Yemin ya da Doğruluk Beyanı Bulunması .....                                  | 128 |
| (3) Aramaya Konu Unsurun Açıkça Belirlenmesi .....                                            | 129 |
| b. Mahkeme Kararı Olmaksızın Arama İşlemi Yapılmasına İmkân Veren<br>İstisnalar .....         | 130 |
| 4. Dördüncü Değişiklik Uygulamasına Teknolojik Gelişmelerin Etkisi .....                      | 131 |
| a. Posta ve Telgrafın Etkisi .....                                                            | 132 |
| b. Telefonun Etkisi .....                                                                     | 133 |
| c. Veri Aktarım Sistemlerinin Etkisi.....                                                     | 135 |
| d. Değerlendirmeler.....                                                                      | 136 |
| 5. Üçüncü Kişi Doktrini .....                                                                 | 138 |
| a. Üçüncü Kişi Doktrini Hakkında Genel Bilgiler.....                                          | 138 |
| b. Üçüncü Kişi Doktrininin Ortaya Çıkışı.....                                                 | 139 |

|                                                                                                                 |     |
|-----------------------------------------------------------------------------------------------------------------|-----|
| i. Üçüncü Kişi Doktrininin Kişiler Arası Konuşmalara Uygulanması..                                              | 140 |
| (2) Üçüncü Kişi Doktrininin Büyük Kayıt Sistemlerine Sahip Kişilere Uygulanması .....                           | 141 |
| c. Üçüncü Kişi Doktrininin Dijital Ortamda Bulunan Bilgilere Uygulanması .....                                  | 143 |
| d. Üçüncü Kişi Doktrini Üzerine Değerlendirmeler .....                                                          | 146 |
| C. SCA Kapsamında Bilgi Talepleri.....                                                                          | 147 |
| 1. SCA Hakkında Genel Bilgiler.....                                                                             | 147 |
| 2. SCA'nın Yürürlüğe Konmasının Sebepleri .....                                                                 | 148 |
| 3. SCA'yı Tadil Eden CLOUD Act'in Doğuşuna Sebep Olan Mahkeme Kararları .....                                   | 150 |
| a. Microsoft Corp v. United States Kararı .....                                                                 | 152 |
| b. In re Search Warrant No. 16-960-M-01 and No. 16-1061-M to Google Kararı.....                                 | 157 |
| 4. CLOUD Act ile Tadil Edilen SCA'nın Getirdiği Kurallar .....                                                  | 160 |
| a. SCA'ya Genel Bakış .....                                                                                     | 160 |
| b. SCA'da Yer Alan Önemli Tanımlar .....                                                                        | 161 |
| c. SCA Kapsamında Hizmet Sağlayıcıların Gönüllü Olarak Bilgi Paylaşması.....                                    | 163 |
| d. SCA Kapsamında İddia Makamlarının Bilgi Talepleri.....                                                       | 165 |
| e. SCA'nın Doğurduğu Hukukların Çatışması Sorunları ve Bunların Çözümüne İlişkin Kuralları.....                 | 168 |
| (1) SCA'nın Sınır Ötesi Uygulama Kapsamına İlişkin Kuralları ve Doğurabileceği Hukukların Çatışması Sorunu..... | 168 |
| (2) Hukukların Çatışması Sorununun Çözümlerine Yönelik SCA Kuralları .....                                      | 170 |

|      |                                                                                                                                    |     |
|------|------------------------------------------------------------------------------------------------------------------------------------|-----|
| i.   | SCA Kapsamında Uluslararası Adli İstinabe Sözleşmesi İmzalayan Devletlere İlişkin Hukukların Çatışması Sorunlarının Çözümü .....   | 171 |
| ii.  | SCA Kapsamında Uluslararası Adli İstinabe Sözleşmesi İmzalamayan Devletlere İlişkin Hukukların Çatışması Sorunlarının Çözümü ..... | 175 |
| f.   | SCA Kapsamında İmzalanabilecek Uluslararası Adli İstinabe Sözleşmeleri .....                                                       | 178 |
| (1)  | Uluslararası Adli İstinabe Sözleşmesi İmzalanabilmesine Dair CLOUD Act'in Getirdiği Şartlar.....                                   | 179 |
| i.   | Özel Hayatın Gizliliği ile Temel Hak ve Özgürlüklerin Korunması . .....                                                            | 180 |
| ii.  | Talebe Konu Verilerin Asgari Seviyede Kullanılması İçin Gerekli Prosedürlerin Oluşturulması.....                                   | 182 |
| iii. | Şifrelemenin Kısıtlanmaması ya da Şifre Çözme Zorunluluğu Getirilememesi .....                                                     | 183 |
| iv.  | Adli İstinabe Sözleşmesinin İçermesi Gereken Düzenleme ve Kısıtlamalar .....                                                       | 183 |
| (2)  | ABD ile Birleşik Krallık Arasında İmzalanan Uluslararası Adli İstinabe Sözleşmesinin İncelenmesi.....                              | 187 |
| i.   | Sözleşmenin Amaç, Kapsam ve Uygulanma Hükümleri.....                                                                               | 187 |
| ii.  | Sözleşmenin İç Hukuk ile İlişkisi ve Karşılıklılık İlkesi Açısından Değerlendirilmesi.....                                         | 192 |
| IV.  | SCA'NIN MİLLETLERARASI ÖZEL HUKUK İLE İLİŞKİSİ .....                                                                               | 194 |
| V.   | SCA'NIN SINIR ÖTESİ UYGULAMA KAPSAMININ DEVLETLERİN ULUSLARARASI YETKİSİ AÇISINDAN DEĞERLENDİRİLMESİ .....                         | 196 |
| VI.  | SCA'NIN SINIR ÖTESİ UYGULAMA KAPSAMININ HUKUKLARIN ÇATIŞMASI KAVRAMI AÇISINDAN DEĞERLENDİRİLMESİ.....                              | 197 |

|                                                                                                                                                                               |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| A. SCA'nın Sınır Ötesi Uygulama Kapsamının Hukukların Çatışması Durumu Yaratması .....                                                                                        | 197 |
| B. SCA'nın Yarattığı Hukukların Çatışması Durumlarına Yönelik Çözüm Önerileri ve Ülkemizin Dijital Ortamdaki Bilgilere Erişime Dair Hukuk Politikasına İlişkin Öneriler ..... | 199 |

## **DÖRDÜNCÜ BÖLÜM**

### **VERİ LOKALİZASYONU**

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| I. GİRİŞ .....                                                                    | 202 |
| II. VERİ LOKALİZASYONU KAVRAMI HAKKINDA GENEL BİLGİLER ... ..                     | 205 |
| A. Veri Lokalizasyonu Kavramının Tanımı .....                                     | 205 |
| B. Veri Lokalizasyonu Yükümlülüğü Tipleri .....                                   | 207 |
| C. Veri Lokalizasyonu Yükümlülüğünün Gündeme Gelmesine Sebep Olan Olaylar.....    | 209 |
| D. Veri Lokalizasyonu Yükümlülüğünü Getirilmesinin Amaçları ve Etkileri .         | 212 |
| 1. Güvenlik Amaçları .....                                                        | 213 |
| a. Veri Güvenliği ve Gizliliğinin Sağlanması .....                                | 213 |
| b. Devlet Kurumlarının Veriye Erişiminin Sağlanması .....                         | 215 |
| c. Yabancı Devletlerin Verilere Erişiminin Engellenmesi.....                      | 216 |
| 2. Ekonomik Amaçlar .....                                                         | 217 |
| E. Veri Lokalizasyonu Yükümlülüğüne Dair Farklı Devletlerin Bakış Açıkları        | 219 |
| III. TÜRKİYE VE DÜNYADA VERİ LOKALİZASYONU YÜKÜMLÜLÜKLERİ .....                   | 221 |
| A. Türkiye’de Veri Lokalizasyonu Yükümlülüğü Getiren Mevzuat .....                | 221 |
| 1. Bankacılık ve Finans Sektörüne Yönelik Veri Lokalizasyonu Yükümlülükleri ..... | 222 |
| a. Bankacılık Kanunu ve İkincil Düzenlemeleri .....                               | 222 |

|                                                                                                                                              |     |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----|
| b. Banka Kartları ve Kredi Kartlarına İlişkin İkincil Düzenlemeler.....                                                                      | 226 |
| c. Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ve İkincil Düzenlemeleri..... | 227 |
| d. Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin İkincil Düzenlemeler.....    | 229 |
| e. Sermaye Piyasası Kanunu ve İkincil Düzenlemeleri .....                                                                                    | 230 |
| f. Sigortacılığa İlişkin İkincil Düzenlemeler .....                                                                                          | 232 |
| 2. Kamu Kurum ve Kuruluşları ile Kritik Altyapılara Yönelik Veri Lokalizasyonu Yükümlülükleri.....                                           | 233 |
| 3. Telekomünikasyon Sektörüne Yönelik Veri Lokalizasyonu Yükümlülükleri .....                                                                | 235 |
| 4. Fatura ve Ticari Defterlere Yönelik Veri Lokalizasyonu Yükümlülükleri....                                                                 | 237 |
| 5. Elektrikli Skuterlere Yönelik Veri Lokalizasyonu Yükümlülüğü .....                                                                        | 238 |
| 6. Sosyal Ağ Sağlayıcılarının Veri Lokalizasyonunu Sağlamaya Yönelik Tedbirler Alma Yükümlülüğü.....                                         | 239 |
| 7. Kişisel Verilere Dair De Facto Veri Lokalizasyonu Yükümlülüğü .....                                                                       | 241 |
| B. Çeşitli Ülkelerin Veri Lokalizasyonu Yükümlülüğü Getiren Hukuki Düzenlemeleri .....                                                       | 245 |
| 1. Batı Bloğu Ülkelerinde Veri Lokalizasyonu Yükümlülükleri .....                                                                            | 246 |
| a. Avrupa Birliği .....                                                                                                                      | 246 |
| (1) AB Nezdinde Veri Lokalizasyonu Yaklaşımı.....                                                                                            | 246 |
| (2) Bazı AB Ülkelerinde Veri Lokalizasyonu Yükümlülükleri.....                                                                               | 249 |
| b. Kanada.....                                                                                                                               | 251 |
| 2. Doğu ve Güneydoğu Asya Ülkelerinde Veri Lokalizasyonu Yükümlülükleri .....                                                                | 253 |
| a. Çin Halk Cumhuriyeti .....                                                                                                                | 253 |

|                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------|-----|
| b. Hindistan .....                                                                                                          | 257 |
| c. Endonezya .....                                                                                                          | 259 |
| d. Vietnam .....                                                                                                            | 261 |
| e. Güney Kore .....                                                                                                         | 263 |
| 3. Diğer Bazı Ülkelerde Veri Lokalizasyonu Yükümlülükleri .....                                                             | 265 |
| a. Rusya.....                                                                                                               | 265 |
| b. Kazakistan.....                                                                                                          | 266 |
| c. Brezilya .....                                                                                                           | 267 |
| d. Suudi Arabistan.....                                                                                                     | 268 |
| IV. VERİ LOKALİZASYONU KURALLARININ MİLLETLERARASI ÖZEL HUKUK VE USUL HUKUKU AÇISINDAN ÖNEMİ .....                          | 269 |
| A. Milletlerarası İstinabe ile Veri Lokalizasyonu Yükümlülüğü Kurallarının İlişkisi.....                                    | 270 |
| B. Serbest Ticaret Anlaşmaları ve Doğrudan Yabancı Yatırımlar ile Veri Lokalizasyonu Yükümlülüğü Kurallarının İlişkisi..... | 272 |
| 1. Serbest Ticaret Anlaşmaları ile Veri Lokalizasyonu Yükümlülükleri İlişkisi .....                                         | 273 |
| 2. Serbest Ticaret Anlaşmaları İçerisinde Veri Lokalizasyonu Yükümlülüklerinin Ele Alınışı.....                             | 274 |
| 3. Veri Lokalizasyonu Yükümlülüklerinin Doğrudan Yabancı Yatırımlar Açısından Etkileri.....                                 | 279 |
| V. VERİ LOKALİZASYONU KURALLARININ HUKUKLARIN ÇATIŞMASI AÇISINDAN ÖNEMİ.....                                                | 282 |
| VI. ÜLKEMİZİN VERİ LOKALİZASYONU HAKKINDAKİ HUKUK POLİTİKASININ DEĞERLENDİRİLMESİ VE ÖNERİLER .....                         | 284 |
| A. Türkiye’de Veri Lokalizasyonu Yükümlülükleri Getirilmesinin Amaçları.                                                    | 284 |
| B. Türkiye’de Veri Lokalizasyonu Konusunun Ele Alınışına Dair Öneriler ...                                                  | 285 |



|                |     |
|----------------|-----|
| SONUÇ .....    | 290 |
| KAYNAKÇA.....  | 295 |
| ÖZGEÇMİŞ ..... | 351 |



## KISALTMALAR LİSTESİ

|                  |                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------|
| <b>a.g.e.</b>    | : Adı Geçen Eser                                                                                  |
| <b>A.Ş.</b>      | : Anonim Şirketi                                                                                  |
| <b>a.y.</b>      | : Yazara Ait Son Zikredilen Yer                                                                   |
| <b>AB</b>        | : Avrupa Birliği                                                                                  |
| <b>ABAD</b>      | : Avrupa Birliği Adalet Divanı                                                                    |
| <b>ABD</b>       | : Amerika Birleşik Devletleri                                                                     |
| <b>ASEAN</b>     | : The Association of Southeast Asian Nations (Güneydoğu Asya Ülkeleri Birliği)                    |
| <b>Aş.</b>       | : Aşağıya Atıf                                                                                    |
| <b>BDDK</b>      | : Bankacılık Düzenleme ve Denetleme Kurumu                                                        |
| <b>Bkz.</b>      | : Bakınız                                                                                         |
| <b>BM</b>        | : Birleşmiş Milletler                                                                             |
| <b>bs.</b>       | : Basım                                                                                           |
| <b>BTK</b>       | : Bilgi Teknolojileri ve İletişim Kurumu                                                          |
| <b>C.</b>        | : Cilt                                                                                            |
| <b>CBDDO</b>     | : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi                                                          |
| <b>CJEU</b>      | : Court of Justice of the European Union                                                          |
| <b>CLOUD Act</b> | : The Clarifying Lawful Overseas Use of Data Act (Yurtdışındaki Verilerin Yasal Kullanımı Kanunu) |
| <b>CMK</b>       | : Ceza Muhakemesi Kanunu                                                                          |
| <b>çev.</b>      | : Çeviren                                                                                         |
| <b>DTÖ</b>       | : Dünya Ticaret Örgütü                                                                            |
| <b>EDPB</b>      | : European Data Protection Board                                                                  |
| <b>eSIM</b>      | : Electronic Subscriber Identity Module (Elektronik Abone Kimlik Modülü)                          |
| <b>FBI</b>       | : Federal Bureau of Investigation (Federal Soruşturma Bürosu)                                     |
| <b>G20</b>       | : The Group of Twenty                                                                             |
| <b>GATS</b>      | : General Agreement on Trade in Services (Hizmet Ticareti Genel Anlaşması)                        |

|                    |                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>GATT</b>        | : General Agreement on Tariffs and Trade (Gümrük Tarifeleri ve Ticaret Genel Anlaşması)                              |
| <b>GCHQ</b>        | : The Government Communications Headquarters                                                                         |
| <b>GDPR</b>        | : General Data Protection Regulation (Avrupa Birliği Genel Veri Koruma Tüzüğü)                                       |
| <b>GPS</b>         | : Global Positioning System (Küresel Konumlama Sistemi)                                                              |
| <b>GSM</b>         | : Global System for Mobile Communication (Mobil İletişim İçin Küresel Sistem)                                        |
| <b>HMK</b>         | : Hukuk Muhakemeleri Kanunu                                                                                          |
| <b>ICSID</b>       | : International Centre for Settlement of Investment Disputes (Uluslararası Yatırım Anlaşmazlıklarının Çözüm Merkezi) |
| <b>IP</b>          | : Internet Protocol (İnternet Protokolü)                                                                             |
| <b>İYUK</b>        | : İdari Yargılama Usulü Kanunu                                                                                       |
| <b>KVKK</b>        | : Kişisel Verilerin Korunması Kanunu                                                                                 |
| <b>m.</b>          | : Madde                                                                                                              |
| <b>NCA</b>         | : National Cybersecurity Authority (Ulusal Siber Güvenlik Otoritesi)                                                 |
| <b>NSA</b>         | : National Security Agency (Ulusal Güvenlik Dairesi)                                                                 |
| <b>OECD</b>        | : Organisation for Economic Co-operation and Development (Ekonomik Kalkınma İş birliği Örgütü)                       |
| <b>PATRIOT Act</b> | : Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act  |
| <b>PRISM</b>       | : Planning Tool for Resource Integration, Synchronization, and Management                                            |
| <b>s.</b>          | : Sayfa                                                                                                              |
| <b>s.k.</b>        | : Sayılı Karar                                                                                                       |
| <b>SCA</b>         | : Stored Communications Act (Depolanan İletişimler Kanunu)                                                           |
| <b>SEDDK</b>       | : Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu                                                       |
| <b>SIM</b>         | : Subscriber Identity Module (Abone Kimlik Modülü)                                                                   |
| <b>SPK</b>         | : Sermaye Piyasası Kurulu                                                                                            |

|             |                                     |
|-------------|-------------------------------------|
| <b>TBMM</b> | : Türkiye Büyük Millet Meclisi      |
| <b>TCK</b>  | : Türk Ceza Kanunu                  |
| <b>TCMB</b> | : Türkiye Cumhuriyet Merkez Bankası |
| <b>TTK</b>  | : Türk Ticaret Kanunu               |
| <b>vd.</b>  | : Ve Diğerleri                      |
| <b>Yuk.</b> | : Yukarıya Atıf                     |
| <b>yy.</b>  | : Yüzyıl                            |



## GİRİŞ

20. yüzyılın sonunda ivme kazanan teknolojik gelişmeler ile internetin yaygınlaşması, insanların sosyal ve ekonomik yaşantısını ciddi bir şekilde değiştirdi ve bu değişim hala hızlı bir şekilde devam etmektedir. Yaşanan değişimin temelinde, bilgi aktarımı imkânlarının ciddi gelişimi ile yeni bir etkileşim alanı olan dijital ortamın oluşması yatmaktadır. Bu gelişim neticesinde kişiler arasında kurulan hukuki ilişkiler de gitgide dijital ortama taşınmaktadır.

Kişiler arasında bilgi aktarım imkânının gelişmesinin hukuki açıdan en önemli sonuçlarından biri, yabancılık unsuru içeren hukuki ilişkilerin içerik ve sayısının hızlı bir şekilde artmasıdır. Yabancılık unsuru bulunan ilişkilerin artmasına rağmen, ilgili hukuki sorunların milletlerarası özel hukuk ve usul hukuku sistematigi dışında çözümlenmeye çalışıldığı gözlemlenmektedir. Özellikle devletlerin yurtdışındaki kişilere de uygulanabilir olacak şekilde yer bakımından kapsam kuralları ile yürürlüğe soktuğu kanunlar ve bunlara aykırılığa ilişkin yaptırımların özel hukuk mahkemelerinin denetimine tabi olmaması olguları, yabancılık unsuru bulunan hukuki işlemlerin sayısının dijital ortam nedeniyle artmasına rağmen milletlerarası özel hukuk ve usul hukuku disiplinin kapsamına girmemeleri ile sonuçlanmaktadır. Bu nedenle örneğin **Facebook** ya da **WhatsApp** gibi yabancı şirketler tarafından milyonlarca Türk vatandaşının kişisel verileri işlenmekteyken, bu konuda milletlerarası özel hukuk ve usul hukuku disiplini çerçevesinde çözümlenen uyuşmazlık sayısında henüz kayda değer bir artış bulunmamaktadır.

Milletlerarası özel hukuk sistematigi çerçevesinde yabancı bir hukukun ev sahibi ülke içerisinde uygulanmasının yegâne yolu, ev sahibi devletin ilgili yabancı hukukun uygulanmasına yasal düzenlemeleriyle imkân tanınmasıdır. Bu tür yasalara bağlama kuralları adı verilmektedir. Bağlama kuralları bağlama konusu ve bağlama noktası olarak iki bölümden oluşurlar. Bağlama konusu, ilgili kuralın düzenlediği hukuki ilişkiyi ifade ederken bağlama noktası ise bu hukuki ilişkiye uygulanacak hukuku tespit eder.

Türk hukuk sisteminde bulunan bağlama kurallarının büyük kısmı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun ile Türkiye'nin taraf olduğu ilgili milletlerarası sözleşmeler içerisinde bulunmaktadır. Bunlara örnek olarak söz konusu kanunun 35/3 numaralı maddesinde yer alan kişisel verilerin işlenmesi ile kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yoluyla kişilik haklarının ihlal edilmesi durumuna ilişkin bağlama kuralı gösterilebilir. Burada bağlama konusu kişisel verilerin işlenmesi ile kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yoluyla kişilik haklarının ihlalidir. Bağlama noktası ise aynı maddenin ilk fıkrasında detaylıca düzenlenen şartlara göre seçilebilecek mutlak mesken, işyeri ya da zararın meydana geldiği ülke olarak belirlenmiştir. Yani bağlama konusu kapsamında bir olaya Türk mahkemelerinin uygulayacağı hukuk, bağlama noktalarından birisinin gösterdiği hukuktur.

Öte yandan kişisel verilerin korunmasına ilişkin mevcut bağlama kuralının, kişisel verilerin korunmasına ilişkin birçok hususu kapsam dışı bıraktığı ve sadece mahkemeye intikal etmiş bir uyumsuzluk için düzenleme getirdiği görülmektedir. Yabancı bir kişinin kişisel verilerin korunmasına ilişkin idari şikâyet mekanizmalarını kullanması durumunda hangi hukukun uygulanması gerektiği, yurtdışında yerleşik olup Türk vatandaşlarının kişisel verilerini işleyen kişilerin hangi kanuna uygun davranması gerektiği (güvenlik tedbirleri, veri işleme şartları, aydınlatma yükümlülüğü gibi çeşitli yükümlülükler hakkında) gibi birçok hususta bağlama kuralları çerçevesinde herhangi bir düzenleme yapılmamıştır.

Günümüzde farklı ülkelerin hukukları arasında yeni bir tür ihtilaf yani çatışma meydana gelmeye başladığı gözlemlenmektedir. Milletlerarası özel hukuktaki gönüllülük sisteminin aksine devletler iç hukuklarında yaptıkları düzenlemeler vasıtasıyla kendi kanunlarının, ev sahibi devlet kanunlarını dikkate almaksızın, yabancı devlet ülkesinde bulunan kişiler için de geçerli olmasını öngörmektedirler. Örneğin ABD'de yürürlüğe giren ve ABD adli makamlarının ceza yargılaması kapsamında bilgi taleplerinin ABD dışında da geçerli olduğunu hüküm altına alan CLOUD Act ile AB'de bulunan kişilerin kişisel verilerini AB dışında olarak işleyen kişilerin de uyum sağlaması gereken GDPR, bahse konu olguya örnek olarak

gösterilebilecektir. Bu tür kanunlar ilgili yabancı devletteki kişileri belirli iş ve işlemleri yapmaya zorlamaktayken, ev sahibi devletin kanunları da tam aksi yönde hükümler içerebilmektedir. Söz konusu durumlar çalışmamız boyunca hukukların çatışması olarak adlandırılacak olup çalışmamızın esas konusunu da bu olgu oluşturmaktadır.

Dijital ortamda egemenlik kuramama sorununu çözme ve aynı zamanda yabancı kanunların ülke içinde uygulanmasını engelleme ile verilere uygulanacak hukuku belirleme hedeflerine yönelik olarak; verilerin belirli bir ülke ya da bölgede bulundurulmasını zorunlu tutan veri lokalizasyonu yükümlülükleri de çalışmamız kapsamında incelenmiştir. Veri lokalizasyonu yükümlülükleri, her ne kadar etkililikleri, avantaj ve dezavantajları tartışılabilir olsa da hukukların çatışması sorununa yönelik üretilmiş en net ve yaygın çözüm olarak karşımıza çıkmaktadır. O nedenle çalışmamızın bir bölümü sadece veri lokalizasyonu yükümlülüklerine ayrılmıştır.

Doktora çalışmamız, hukuku çeşitli dallar altında değil, olabildiğince bir bütün olarak görme prensibine uygun olarak hazırlanmıştır. O nedenle dijital ortamdaki hukukların çatışması başlığı altında bu sorunun gözlemlenebildiği çok fazla farklı hukuk alanı üzerinde inceleme yapılmıştır. Çalışmamızın amacı ve metodu, bahsedilen her konunun tüm detayına kadar incelenmesi değil; bütünün parçalarını birleştirerek büyük resmin ortaya konulması ve makro ölçekte çözümler üretilmesidir. Bu yaklaşımın benimsenmesindeki ana sebep, çeşitli dallara ayrılmış hukuk biliminin; bir bütün olarak değerlendirilmeden, çalışmamıza konu hukukların çatışması problemini çözmekte yeterli olamayacağı düşüncesidir.

Doktora tezimizin amacı milletlerarası özel hukuk sistematigi dışında uygulama alanı bulan sınır ötesi uygulama kapsamına sahip kanunların teorik altyapısının ortaya konması, bunların yarattıkları sorunların tespiti ile sorunlara ilişkin çözüm önerileri

oluřturulmasıdır. Çalışmanın kapsamı ise dijital ortamı düzenleyen yasal düzenlemeler ile sınırlanmıştır<sup>1</sup>.

Çalışmanın ilk bölümünde uluslararası hukuk çerçevesinde devletlerin egemenliklerini sınır ötesi olarak kullanmalarına ilişkin durum incelenecek ve hukukların çatışması kavramı tanımlanacaktır. İkinci ve üçüncü bölümde ise yukarıda bahsedilen GDPR (KVKK ile birlikte) ve CLOUD Act, sınır ötesi uygulama kapsamına sahip kanun örnekleri olarak incelenecektir. Dördüncü bölümde ise veri üzerindeki egemenliği sağlama ve pekiştirme hedefi ile yürürlüğe konulan veri lokalizasyonu yükümlölükleri üzerinde değerdendirmeler yapılacaktır. Her bir bölüm içerisinde konuya ilişkin görüş ve çözüm önerileri de okuyucu bilgisine sunulacaktır.

---

<sup>1</sup> Sınır ötesi uygulama kapsamı içeren, ancak dijital ortamı doğrudan düzenlemeyen yasal düzenlemeler bu çalışma kapsamı dışındadır. Bu tür düzenlemelere örnek olarak ABD'nin uluslararası yaptırımlara ilişkin mevzuatı ile yabancı ölkelerde Amerikan şirket ve vatandaşlarının hukuka aykırı ödeme yapmalarını düzenleyen *The Foreign Corrupt Practices Act* gösterilebilir.



## BİRİNCİ BÖLÜM

### HUKUKLARIN ÇATIŞMASI

#### I. GİRİŞ

Yabancı bir hukukun başka bir ülke içerisinde uygulanması konusu hem Türkiye’de hem de dünyada temel olarak milletlerarası özel hukuk alanı altında değerlendirilmektedir. Türk hukuk sistemi içerisinde yabancı hukukların Türkiye’de uygulanmasına ilişkin ana kanun MÖHUK’tur. Milletlerarası özel hukuk ya da başka bir adıyla kanunlar ihtilafı alanı, çeşitli özel hukuk kurumları hakkında bağlama noktalarını göz önüne alarak uygulanacak hukuku tespit etmektedir. Herhangi bir konuda uygulanacak hukuk tespit edildikten sonra, artık bu konuya ilişkin yabancı hukuk, kamu ya da özel hukuk ayrımı yapılmaksızın, bir bütün olarak uygulanmaktadır<sup>2</sup>. Yabancı hukukun uygulanmasının, Türk hukuku tarafından sınırlandırılması ise iki farklı kural altında gerçekleşmektedir. Bunlardan ilki uygulanacak yabancı hukukun, Türk kamu düzenine aykırılık teşkil etmemesi kuralıdır (MÖHUK m. 5). İkincisi ise yabancı hukukun uygulanması sırasında, Türk hukukunun doğrudan uygulanan kuralları her hâlükârda uygulama alanı bulmasıdır (MÖHUK m. 6). Türk hukukunun doğrudan uygulanan kuralları ile uygulanacak yabancı hukukun çelişmesi halinde, Türk hukukunun doğrudan uygulanan kurallarına öncelik verilmesi gerekmektedir<sup>3</sup>. Açıklanan bu metodoloji, yabancı hukuk sistemlerinde de ana hatları ile aynı şekildedir.

---

<sup>2</sup> “5718 Sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun”, (2007), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5718&MevzuatTur=1&MevzuatTertip=5>, 16.03.2021.

<sup>3</sup> Ergin Nomer, **Devletler Hususi Hukuku**, 22. bs, İstanbul, Beta Basım A.Ş., 2017, s. 188; Aysel Çelikel, B. Bahadır Erdem, **Milletlerarası Özel Hukuk**, 17. bs, İstanbul, Beta Basım A.Ş., 2021, s. 161; Vahit Doğan, **Milletlerarası Özel Hukuk**, 8. bs, Ankara, Savaş Yayınevi, 2022, s. 280; Cemal Şanlı, Emre Esen, İnci Ataman-Fıganmeşe, **Milletlerarası Özel Hukuk**, 10. bs, İstanbul, Beta Basım A.Ş., 2023, s. 11; Gülören Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, 13. bs, İstanbul, Vedat Kitapçılık, 2020, s. 50; Ziya Akıncı, **Milletlerarası Özel Hukuk**, 1. bs, İstanbul, Vedat Kitapçılık, 2020, s. 23.

Milletlerarası özel hukuk kapsamında yabancı hukukun uygulanması, esasen bir iç hukuk kuralı niteliği taşıyan MÖHUK'a (yabancı ülkelerde de kendi iç kanunlarına) dayanmaktadır. Benzer kanunlar dünyanın hemen her ülkesinde bulunmaktadır. Dolayısıyla milletlerarası özel hukuk kapsamında yabancı bir hukukun uygulanması, esasen egemen devletlerin kendi ülkelerinde yabancı kanunların uygulanmasına izin vermeleri anlamına gelmektedir. Halbuki yabancı bir kanunun başka bir ülkede uygulanması, ev sahibi devletin rızası dışında da gerçekleşebilmektedir. Sınır ötesi uygulama kapsamına sahip (**extraterritorial scope**) olarak adlandırılan bu tür kanunlar, iç hukuktan aldıkları yetki çerçevesinde yabancı ülkelerde de uygulama alanı bulabilmektedirler. Özellikle bilgi ve iletişim teknolojilerinin yaygınlaşması, dijital ortamı düzenleyen yeni kanunların sınır ötesi uygulama kapsamına sahip olması sonucunu doğurmaktadır.

Sınır ötesi uygulama kapsamına sahip yabancı kanunlar ile ev sahibi ülkenin kendi kanunlarının birbiri ile çelişen yükümlülükler getirmesi son derece olasıdır. Hatta kanaatimizce her iki grup kanunun da bağımsız ve egemen devletler tarafından çıkarıldığı düşünüldüğünde, bu kanunların farklı çıkarları gözetmesini ve dolayısıyla birbirleriyle çelişmesini beklemek doğal bir sonuç olarak değerlendirilmelidir. İşte bu tip durumların nasıl değerlendirilmesi ve hem devletlerin egemenlik hakları hem de ilgili hukuklara tabi kılınan kişilerin hangisine uygun hareket etmesi gerektiği sorunları, çalışmamızın temel konusunu oluşturmaktadır.

Çalışmamız boyunca, sınır ötesi uygulama alanı bulan hukuk kuralları ile ev sahibi ülkenin hukuk kurallarının birbiri ile çelişmesi durumu, hukukların çatışması kavramı olarak adlandırılacaktır. Her ne kadar çalışmamızın ana odağı dijital ortamı düzenleyen kanunlar nezdinde hukukların çatışması durumlarını incelemek ve bu durumlara özgü çözümler üretmek olsa da bu bölümde öncelikle hukukların çatışması kavramının analizi yapılacak ve bu kavramın anlaşılabilmesi için değerlendirilmesi gereken hukuki kavramlar (devletlerin egemenliği, devletlerin uluslararası yetkisi, milletlerarası özel hukukun kapsamı) incelenecektir.

## II. DEVLETLERİN EGEMENLİĞİ

### A. Egemenlik Kavramının Tanımı

Ülke ve insan topluluğuyla birlikte devletin unsurlarından biri olan egemenlik (**sovereignty**) kavramı<sup>4</sup>, tarih boyunca devletlerin ve toplumların kaderini belirleyen en önemli hususlardan birisi olmuştur. Egemenliğin kaynağı ve egemenliğin bireye karşı sınırlandırılması konuları, önemli birçok tarihi olayın temelinde yatan sebeplerdir.

Egemenlik kavramı, bağımsız bir devletin tamamen kendi iradesinden kaynaklanan, üstün, sınırsız, emretme ve yaptırım uygulama gücü olarak tanımlanmaktadır<sup>5</sup>. Bir başka tanıma göre ise egemenlik, bir toprak parçası üzerinde devlet fonksiyonlarını icra etme ve bu toprak parçası içerisinde başka devletlerin egemenlik güçlerini kullanamaması anlamına gelmektedir<sup>6</sup>.

---

<sup>4</sup>Malcolm N. Shaw, **International Law**, 8. bs, United Kingdom Padstow, Cornwall, Cambridge University Press, 2017, s. 157; Mesut Hakkı Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, 1. bs, İstanbul, Yeditepe Üniversitesi Yayınları, 2019, s. 233; İlyas Doğan, **Devletler Hukuku**, 4. bs, Ankara, Astana Yayınları, 2020, s. 274; Hüseyin Pazarcı, **Uluslararası Hukuk**, 19. bs, Ankara, Turhan Kitabevi, 2020, s. 145; Gerhard Von Glahn, James Larry Taulbee, **Law Among Nations An Introduction to Public International Law**, 11. bs, New York, NY, USA, Routledge Taylor & Francis Group, 2017, s. 199; Carlo Focarelli, **International Law**, Cheltenham, UK, Edward Elgar Publishing, 2019, s. 39; Şeref Ünal, **Uluslararası Hukuk**, 1. bs, Ankara, Yetkin Basım, 2005, s. 99; Kemal Gözler, **Anayasa Hukukunun Genel Esasları**, 13. bs, Bursa, Ekin Basım Yayın Dağıtım, 2021, s. 162; Rona Aybay, **Genel Kamu Hukuku**, 3. bs, İstanbul, DER Kitabevi, 2020, s. 146; Kemal Gözler, **Devletin Genel Teorisi**, 9. bs, Bursa, Ekin Basım Yayın Dağıtım, 2018, s. 77.

<sup>5</sup> Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 258; Ünal, **Uluslararası Hukuk**, s. 118; Pazarcı, **Uluslararası Hukuk**, s. 153; Erdoğan Teziç, **Anayasa Hukuku (Genel Esaslar)**, 24. bs, İstanbul, Beta Basım A.Ş., 2020, s. 101; Gözler, **Anayasa Hukukunun Genel Esasları**, s. 162; Aybay, **Genel Kamu Hukuku**, s. 149; Gözler, **Devletin Genel Teorisi**, s. 78; Patrick W. Franzese, "Sovereignty in Cyberspace: Can it exist?", **Air Force Law Review**, C. 64, (Çevrimiçi) <https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist>, 26.12.2020; Adnan Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", **Uyuşmazlık Mahkemesi Dergisi**, S. 6, 2016, s. 316; Cedric Ryngaert, **Jurisdiction in International Law**, 2. bs, New York, Oxford University Press, 2015, s. 5; Michael N. Schmitt, Liis Vihul (ed.), **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, 1. bs, United Kingdom, Cambridge University Press, 2017, s. 11.

<sup>6</sup> Island of Palmas Case (or Miangas), United States v Netherlands, C. Reports of International Arbitral Awards, (Permanent Court of Arbitration 1928).

Egemenlik kavramının iç egemenlik ve dış egemenlik olmak üzere iki farklı görünümü bulunmaktadır<sup>7</sup>. İç egemenlik, devletin kendi ülkesi içerisinde egemenlik haklarını münhasıran ve uluslararası hukuk çerçevesinde sınırsız olarak kullanabilmesi anlamına gelmektedir<sup>8</sup>. Egemenlik kavramı tanım itibarıyla sınırsız olsa da egemenliğin devletlerce kullanımı iç hukuklar vasıtasıyla sınırlandırılmış durumdadır. Söz konusu sınırlandırmalar, bireylerin korunması amacıyla anayasa ve kanunlar vasıtasıyla yapılmıştır. Dış egemenlik kavramı ise bir devletin diğer devletlerle olan ilişkilerinde kendi iradesi ile hareket edebilme imkanına sahip olması ile diğer devletlerle hukuki açıdan eşit olması anlamına gelmektedir<sup>9</sup>. Dış egemenlik kavramı aynı zamanda bağımsızlık olarak da adlandırılmaktadır<sup>10</sup>.

Orta Çağ'ın başlangıcından 18. yy'a kadar geçen dönem boyunca egemenliğin kaynağının ilahi olduğu kabul edilmiştir<sup>11</sup>. Bu anlayışa göre egemenliğin sahibi tanrıdır ve siyasi iktidarlar tanrıdan aldıkları yetkiye dayanarak egemenlik yetkilerini kullanmaktadırlar. ABD'nin kuruluşu (1776) ile Fransız İhtilalinden (1789) sonra kabul edilen anlayışa göre ise egemenliğin kaynağı bireyler yani toplumdur<sup>12</sup>. Yani

---

<sup>7</sup> Ünal, **Uluslararası Hukuk**, s. 119; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 13; Gözler, **Anayasa Hukukunun Genel Esasları**, s. 163; Gözler, **Devletin Genel Teorisi**, s. 79; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 317; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 261; Pazarcı, **Uluslararası Hukuk**, s. 154.

<sup>8</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 13; Ünal, **Uluslararası Hukuk**, s. 119; Gözler, **Anayasa Hukukunun Genel Esasları**, s. 164; Gözler, **Devletin Genel Teorisi**, s. 81; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 318; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 261; Pazarcı, **Uluslararası Hukuk**, s. 154.

<sup>9</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 16; Ünal, **Uluslararası Hukuk**, s. 119; Doğan, **Devletler Hukuku**, s. 335; Gözler, **Anayasa Hukukunun Genel Esasları**, s. 163; Gözler, **Devletin Genel Teorisi**, s. 79; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 318; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 261; Pazarcı, **Uluslararası Hukuk**, s. 154.

<sup>10</sup> Gözler, **Anayasa Hukukunun Genel Esasları**, s. 163; Gözler, **Devletin Genel Teorisi**, s. 79; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 16; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 318; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 322; Pazarcı, **Uluslararası Hukuk**, s. 154.

<sup>11</sup> Teziç, **Anayasa Hukuku (Genel Esaslar)**, s. 104; Gözler, **Devletin Genel Teorisi**, s. 87; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 319; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 260.

<sup>12</sup> Teziç, **Anayasa Hukuku (Genel Esaslar)**, s. 107; Gözler, **Devletin Genel Teorisi**, s. 89; Küçük, "Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm", s. 322; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 260.

egemenlik kavramının ilahi bir niteliği yoktur ve egemenlik tamamen beşerî bir kavramdır.

Egemenlik kavramının çalışmamız açısından önemi, bu kavramın devletlerin uluslararası yetkisinin kaynağını ve aynı zamanda sınırlarını oluşturmasıdır. Bu çerçevede sınır ötesi uygulama kapsamına sahip hukuk kurallarının yürürlüğe konması<sup>13</sup> ile uygulanması açılarından egemenlik kavramının da önemli etkileri bulunmaktadır.

## **B. Egemenlik Kavramının Mekânsal Sınırları**

Egemenlik, kural olarak bir devletin ülkesi içerisinde mevcuttur ve egemenlikten doğan yetkiler, sadece ülke sınırları içerisinde kullanılabilmektedir<sup>14</sup>. Bu durum ülke kavramının hangi bölgeleri kapsadığı konusuna değinilmesini gerektirmektedir.

Uluslararası hukuk çerçevesinde bir ülkenin bütünü kara, deniz ve hava ülkelerinden oluşmaktadır<sup>15</sup>. Kara ülkesi, devletlerin birbirleri ile olan sınırlarını tespit etmeleri sonucunda oluşan belirli toprak parçası anlamına gelmektedir. Kara ülkesinin boyutu, devletlerin egemenlik hakları açısından herhangi bir önem arz etmemektedir.

Kara ülkesinin sınırları aynı zamanda devletlerin deniz ve hava ülkelerinin de sınırlarını belirlemektedir. Devletlerin denizlerdeki egemenlik alanları milletlerarası sözleşmeler ile belirlenmiş durumdadır<sup>16</sup>. Bu kapsamda deniz ülkesinin parçaları

<sup>13</sup> Sınır ötesi uygulama kapsamına sahip hukuk kurallarının yürürlüğe konması, esasen iç egemenliğin, diğer devletlerin iç egemenliklerine etkide bulunabilecek şekilde kullanılması anlamına gelmektedir.

<sup>14</sup> Shaw, **International Law**, s. 363; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 237; Ian Brownlie, **Principles of Public International Law**, 7. bs, New York, Oxford University Press, 2008, s. 105; Ünal, **Uluslararası Hukuk**, s. 109; Anders Henriksen, **International Law**, 1. bs, New York, Oxford University Press, 2017, s. 85; Martin Dixon, Robert McCorquodale, Sarah Williams, **Cases & Materials on International Law**, 6. bs, New York, Oxford University Press, 2016, s. 244; Doğan, **Devletler Hukuku**, s. 274; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 13; Pazarcı, **Uluslararası Hukuk**, s. 155; Focarelli, **International Law**, s. 294.

<sup>15</sup> Brownlie, **Principles of Public International Law**, s. 115; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 238; Ünal, **Uluslararası Hukuk**, s. 110; Doğan, **Devletler Hukuku**, s. 297; Pazarcı, **Uluslararası Hukuk**, s. 149.

<sup>16</sup> “Conventions on the Law of the Sea”, (1958), (Çevrimiçi) <https://legal.un.org/avl/ha/gclos/gclos.html>, 11.01.2021; “United Nations Convention on the Law of the

olarak içsular, karasuları, takım ada suları ve boğazlar belirlenmiştir. Ayrıca devletlerin belirli egemenlik haklarına sahip olabilecekleri bölgeler de bitişik bölge, balıkçılık bölgesi, kıta sahanlığı ve münhasır ekonomik bölge olarak sıralanmıştır. Bu bölgelerin dışında kalan açık deniz ve uluslararası deniz yatağı alanları ise hiçbir devletin egemenliği altında bulunmamaktadır.

Hava ülkesinin ya da daha yaygın bilinen adıyla hava sahasının sınırları ise kara ülkesi ile buna bitişik içsuların ve karasularının üstünde bulunan hava bölgesi olarak kabul edilmektedir<sup>17</sup>. Bu alanlar dışında kalan bölgeler ise uluslararası hava sahası olarak adlandırılmaktadır. Devletlerin ulusal hava sahaları içerisinde egemenliğe sahip olduğu milletlerarası sözleşmeler hüküm altına alınmıştır<sup>18</sup>. Uluslararası hava sahası ise hiçbir ülkenin egemenliği altında değildir ve global olarak ortak bir alan şeklinde muamele görmektedir<sup>19</sup>.

İnsanlığın 1957 yılında uzaya ilk çıkışından itibaren uluslararası hukuk, uzay ile de ilgilenmeye başlamıştır. Bu kapsamda tüm gök cisimleri dahil olmak üzere uzayın insanlığın ortak malı olduğu kabul edilmiş ve bu kapsamda uzayın hiçbir devletin egemenliğinde olmadığı kabul edilmiştir<sup>20</sup>.

---

Sea”, (1982), (Çevrimiçi)  
[https://www.un.org/Depts/los/convention\\_agreements/convention\\_overview\\_convention.htm](https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm),  
11.01.2021.

<sup>17</sup> Shaw, **International Law**, s. 404; Brownlie, **Principles of Public International Law**, s. 115; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 238; Ünal, **Uluslararası Hukuk**, s. 110; Doğan, **Devletler Hukuku**, s. 334; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 18; Focarelli, **International Law**, s. 328; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 407; Pazarcı, **Uluslararası Hukuk**, s. 317.

<sup>18</sup> “Chicago Convention on International Civil Aviation”, (1977), (Çevrimiçi)  
<https://www.icao.int/publications/pages/doc7300.aspx>, 20.01.2021.

<sup>19</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 12; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 408; Pazarcı, **Uluslararası Hukuk**, s. 319.

<sup>20</sup> “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies”, (1967), (Çevrimiçi)  
<https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>, 28.01.2021.

## C. Dijital Ortam Üzerinde Egemenlik

### 1. Dijital Ortam Kavramının Tanımı

Dijital ortamda devletlerin egemenliği konusuna geçmeden önce dijital ortamın (**cyberspace** ya da siber alan) tanımının yapılması gerekmektedir. ABD Ordusu tarafından yapılan tanıma göre dijital ortam, internet, telekomünikasyon ağları, bilgisayar sistemleri, entegre işlemci ve kontrolcüler dahil olmak üzere bağımsız bilgi teknolojileri altyapılarından ve bunlarda bulunan verilerden oluşan bilgi ortamıdır<sup>21</sup>. Başka bir tanıma göre ise dijital ortam, internet, telekomünikasyon ağları, bilgisayar sistemleri, entegre işlemci ve kontrolcüler de dahil olmak üzere birbirinden bağımsız bilgi sistemleri ve altyapılarının oluşturduğu bilgi ortamı içerisinde yer alan global bir alandır<sup>22</sup>.

Türkiye'nin 2016 – 2019 Ulusal Siber Güvenlik Stratejisi içerisinde yer alan siber uzay (bu kavram dijital ortam tanımı yerine kullanılmıştır) tanımı ise “tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam” şeklindedir<sup>23</sup>. 7194 sayılı kanun çerçevesinde ise dijital ortam kavramı, fiziki olarak karşı karşıya gelmeksizin çevrim içi faaliyetin gerçekleştirildiği her türlü ortam şeklinde tanımlanmıştır<sup>24</sup>.

---

<sup>21</sup> **DOD Dictionary of Military and Associated Terms**, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>, USA Department of Defense, 2021, s. 55.

<sup>22</sup> ABD Ulusal Standartlar ve Teknoloji Kurumu (NIST) tarafından yapılan tanım için bkz. CSRC Content Editor, “Cyberspace - Glossary | CSRC”, (14.04.2021), (Çevrimiçi) <https://csrc.nist.gov/glossary/term/cyberspace>, 14.04.2021.

<sup>23</sup> “2016 - 2019 Ulusal Siber Güvenlik Stratejisi”, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, s. 7, (13.02.2021), (Çevrimiçi) <https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>, 13.02.2021.

<sup>24</sup> “7194 sayılı Dijital Hizmet Vergisi ile Bazı Kanunlarda ve 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun”, (2019), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7194&MevzuatTur=1&MevzuatTertip=5>, 11.11.2020.

## 2. Dijital Ortamın Bir Egemenlik Alanı Olarak Tanımlanıp Tanımlanamayacağı Sorunu

Dijital ortam ile ilgili olarak değerlendirilmesi gereken ilk sorun, dijital ortamın kara, deniz, hava ya da uzay gibi bağımsız ve yeni bir egemenlik alanı olarak değerlendirilip değerlendirilemeyeceğidir. Dijital ortamın yeni bir egemenlik alanı olarak tanımlanması gerektiği yönünde çeşitli görüşler mevcuttur<sup>25</sup>. Ancak uluslararası hukukun mevcut durumu ve doktrindeki hâkim görüşler uyarınca dijital ortam ayrı bir egemenlik alanı olarak kabul edilmemektedir<sup>26</sup>.

Doktrindeki hâkim görüşe göre dijital ortam fiziki, mantıksal ve sosyal katmanlardan oluşmaktadır<sup>27</sup>. Fiziki katman, dijital ortamın var olmasını sağlayan bilgisayarlar, veri merkezleri ve diğer donanımlardan oluşmakta olup bunlar esasen belirli ülkelerde fiziksel olarak bulunmaktadır. Mantıksal katman ise fiziki katmanlar arasında veri akışını mümkün kılan veriler, yazılımlar ve ağ bağlantılarından oluşmaktadır. Sosyal katman da dijital ortamda faaliyetlerde bulunan kişileri ifade etmektedir. Tüm bu katmanlar esasen devletlerin egemenlik alanlarında, yani ülkelerinde (kara, deniz ya da hava) bulunmaktadır. Dolayısıyla dijital ortam zaten mevcut egemenlik alanları içerisinde bulunduğundan beşinci olarak yeni bir egemenlik alanı yaratmaya gerek görülmemiştir. Bu çerçevede, dijital ortamın ayrı bir egemenlik alanı olması yönündeki görüşler de dijital ortamın fiziki egemenlik alanları ile ilişkisini ortadan kaldırdığı için hâkim görüş tarafından reddedilmiştir<sup>28</sup>.

<sup>25</sup> “NATO Warsaw Summit Communiqué”, 2016, par. 70, (Çevrimiçi) [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](http://www.nato.int/cps/en/natohq/official_texts_133169.htm), 11.04.2021; “Department of Defense Strategy for Operating in Cyberspace”, ABD Savunma Bakanlığı, 2011, s. 5, (Çevrimiçi) <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>, 20.01.2021; **DOD Dictionary of Military and Associated Terms**, s. 55; “The Defence Cyber Strategy”, Hollanda Savunma Bakanlığı, 2012, s. 4, (Çevrimiçi) [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/Netherlands\\_2012\\_NDL-Cyber\\_StrategyEng.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf), 10.03.2021; Dijital ortamın askeri açıdan ayrı bir egemenlik alanı olduğu Birleşik Krallık, Çin, İsrail ve İran tarafından kabul edilmektedir (bkz. Kristen E. Eichensehr, “The Cyber-Law of Nations”, **The Georgetown Law Journal**, C. 103, 2015, s. 329).

<sup>26</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 12; Franzese, “Sovereignty in Cyberspace: Can it exist?”, s. 34; François Delerue, **Cyber Operations And International Law**, 1. bs, Cambridge UK, Cambridge University Press, 2020, s. 11.

<sup>27</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 12.

<sup>28</sup> a.y.; Delerue, **Cyber Operations And International Law**, s. 12.



Dijital ortamın bir egemenlik alanı olarak belirlenmesinin çeşitli problemler doğurması da söz konusu olacaktır. Bunların başında, diğer egemenlik alanlarının oluşumunda olduğu gibi dijital ortamın da egemenlik alanı olarak belirlenmesine yönelik milletlerarası sözleşmelerin yapılıp yapılamayacağı hususu gelmektedir<sup>29</sup>. Denizler, Antarktika, uzay ya da hava sahası gibi alanlar üzerindeki egemenlik sorunları ile bu alanların yönetimi konuları, esasen bu konularda yapılan milletlerarası sözleşmeler ile çözümlenmiştir. İşte bunlara benzer şekilde dijital ortam üzerindeki egemenlik sorunlarını çözmek ve bu alanın bir egemenlik alanı olarak tanınması ile yönetimini sağlamak için de benzer şekilde milletlerarası sözleşmelere ihtiyaç bulunmaktadır. Devletlerin bu konuda bir irade ve uzlaşma gösterip göstermeyeceği şu an için belirsiz bir konudur. Ancak kanaatimizce, açıklanan şekilde bir milletlerarası sözleşme yapılması kısa ya da orta vadede mümkün değildir. Zira dijital ortam, çalışmamızın tarihi itibarıyla neredeyse tamamen ABD hegemonyasıdadır. ABD'nin en büyük rakibi ise, tıpkı diğer alanlarda da olduğu gibi, Çin Halk Cumhuriyeti'dir. Diğer devletler ise büyük ölçüde bu iki ülke tarafından geliştirilen teknolojileri kullanmaktadır. Dolayısıyla tüm devletler arasında dijital ortamın bir egemenlik alanı olarak belirlenmesi için bir uzlaşma ihtiyacının doğabileceğini söylemek için kanaatimizce henüz çok erkendir.

Dijital ortamın bir egemenlik alanı olarak belirlenebilmesinin önünde bulunan diğer engellerden biri ise, dijital ortamda egemenlik sınırlarının nasıl belirleneceği ve bu sınırların nasıl kontrol edileceği konusudur<sup>30</sup>. Başka bir sorun ise dijital ortamda faaliyette bulunan kişilerin kimliklerinin tespit edilmesi hususudur<sup>31</sup>. Her ne kadar bu iki konu teknik önlemlerle (örneğin yurtdışından gelen veri trafiğinin filtrelenmesi, dijital ortamda faaliyette bulunan kişilerin kimliklerinin takip edilmesi, veri lokalizasyonu yükümlülükleri getirilmesi, içeriklere erişimin engellenmesi ya da

---

<sup>29</sup> Franzese, "Sovereignty in Cyberspace: Can it exist?", s. 27.

<sup>30</sup> Franzese, **a.g.e.**, s. 39.

<sup>31</sup> Franzese, **a.y.**

erişimin yavaşlatılması gibi) çözülebilecek nitelikteyse de bu önlemlerin özellikle dünya kamuoyu tarafından kabul edilmesi şu an için pek mümkün görünmemektedir<sup>32</sup>.

### 3. Devletlerin Dijital Ortam Üzerinde Egemenlik Sahibi Olup Olamayacağı Sorunu

Devletlerin dijital ortam üzerinde egemenlik sahibi olup olamayacağı konusunda çeşitli görüşler bulunmaktadır. Dijital ortamın ilk ortaya çıktığı dönemde, dijital ortamın herhangi bir devlet egemenliğinde olmaması gerektiği, bunun yerine dijital ortamın bireylerin serbestçe iletişim kurabileceği kendi kendini yöneten bir ortam olarak kalması gerektiği yönünde görüşler ortaya atılmıştır<sup>33</sup>. Ancak bu görüş, çeşitli sebepler nedeniyle hayata geçememiştir. Bu sebepler dijital ortamın çalışabilmesi için mutlaka fiziksel altyapısının kontrol altında tutulması ve yönetilmesi ihtiyacı, dijital ortamdaki finansal yükümlülükler içeren hukuki işlemlerin çeşitli hukuk kurallarına tabi olmasının gerekmesi, dijital ortamdaki içeriklerin fiziki dünyada da etki doğurması ve milli güvenlik gerekçeleri ile devletlerin dijital ortamda aktif olma gereği duymaları şeklinde sıralanmaktadır<sup>34</sup>. Benzer şekilde dijital ortamın, büyük teknoloji şirketleri tarafından çeşitli kurallara tabi tutulmasının uygun olacağı şeklinde de bir görüş öne sürülmüştür<sup>35</sup>. Ortaya atılan bireyler ya da şirketler (veya bağımsız kuruluşlar) vasıtasıyla dijital ortamın kendi kendini yönetmesi görüşü<sup>36</sup>, yukarıda açıklanan dijital ortamın kendi kendini yöneten bir ortam olarak kalması fikrinin doğal bir sonucudur.

---

<sup>32</sup> Franzese, “Sovereignty in Cyberspace: Can it exist?”, s. 38. Ülkemizde de bir siteye tamamen erişimin engellenmesi, Anayasa’ya aykırı bulunmaktadır. Ayrıca dijital ortama yönetil bu tür engelleme ve sınırlamalar Türk kamuoyunca olumsuz olarak karşılanmaktadır.

<sup>33</sup> Franzese, **a.g.e.**, s. 11; Eichensehr, “The Cyber-Law of Nations”, s. 326.

<sup>34</sup> Franzese, “Sovereignty in Cyberspace: Can it exist?”, s. 12.

<sup>35</sup> Paul De Hert, Johannes Thumfart, “The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 08.07.2018, s. 26, (Çevrimiçi) <https://papers.ssrn.com/abstract=3228388>, 15.06.2019.

<sup>36</sup> Milton Mueller, “Sovereignty and Cyberspace: Institutions and Internet Governance”, s. 13, (29.11.2020); Thomas Schultz, “Private Legal Systems: What Cyberspace Might Teach Legal Theorists”, **Private Legal Systems**, 10 YALE J.L. & TECH. 151, 2007, s. 193, (Çevrimiçi) <https://yolt.org/sites/default/files/schultz-10-yolt-151.pdf>, 28.03.2019; Joel Trachtman, “Cyberspace, Sovereignty, Jurisdiction, and Modernism”, **Indiana Journal of Global Legal Studies**, C. 5, S. 2, 1998, s. 580; Andrew Keane Woods, “Litigating Data Sovereignty”, **Yale Law Journal**, C. 128, S. 2, 2018, s. 405.

Dijital ortamda devletlerin egemenlik sahibi olup olamayacağına dair ikinci görüş ise dijital ortamın global olarak ortak bir alan (**global common**) kabul edilmesi şeklindedir. Bu kapsamda dijital ortam tıpkı açık denizler, uluslararası hava sahası ya da uzay gibi muamele görmelidir<sup>37</sup>. Global olarak ortak alan kavramı, OECD tarafından okyanuslar, uzay ya da Antarktika kıtası gibi devletlerin uluslararası yetki kullanabilecekleri bölgelerin dışında bulunan doğal varlıklar şeklinde tanımlanmıştır<sup>38</sup>. Ancak bahse konu bölgelerin global olarak ortak alan sıfatı almaları, bu yönde milletlerarası sözleşmeler imzalanması ile mümkün olmuştur<sup>39</sup>. Milletlerarası sözleşmeler ayrıca bu bölgelerin nasıl kullanılacağını, söz konusu bölgelerde devletlerin egemenliği bulunup bulunmadığını ve bölgelerin sınırları konularını da detaylarıyla belirlemiş durumdadır. Bahsedilen bölgeler üzerinde herhangi bir devletin egemenlik hakları fiilen kullanması pratikte mümkün olmadığı için ilgili milletlerarası sözleşmelerin tüm devletlerce kabul gördüğünü öne sürmek de mümkündür<sup>40</sup>. Dijital ortamı global olarak ortak alan şeklinde tanımlayacak bir milletlerarası sözleşme olmadığı göz önüne alındığında, uluslararası hukukun mevcut durumu çerçevesinde dijital ortamın şu an için global olarak ortak bir alan olmadığı neticesine erişilmektedir.

Ortaya atılan diğer bir görüş ise dijital ortam üzerinde egemenliğin mülkilik ilkesi yerine egemenlik konusu verinin tipi, bu verinin ilişkili olduğu suç, söz konusu duruma ilişkin ilgili devletlerin hukuk kuralı koymaktaki menfaatleri ve olayla bağlantıları gibi kriterler kullanılarak tespit edilmesi şeklindedir<sup>41</sup>. Benzer bir görüş de global bir ortak alan, mülkilik esası ya da devletlerin katılımının olmadığı ve şirketler veya bireylerin kendi kendini yönettiği bir model gibi görüşlerin hepsinin yetersiz

---

<sup>37</sup> Franzese, "Sovereignty in Cyberspace: Can it exist?", s. 14; Eichensehr, "The Cyber-Law of Nations", s. 337; Darrel Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", **Michigan Telecommunications and Technology Law Review**, C. 4, S. 1, 1998, s. 101.

<sup>38</sup> "OECD Glossary of Statistical Terms", OECD, 2004, s. 299.

<sup>39</sup> "The Antarctic Treaty", (1959), (Çevrimiçi) [https://documents.ats.aq/atcm42/ww/ATCM42\\_ww011\\_e.pdf](https://documents.ats.aq/atcm42/ww/ATCM42_ww011_e.pdf), 26.08.2020; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

<sup>40</sup> Franzese, "Sovereignty in Cyberspace: Can it exist?", s. 17.

<sup>41</sup> De Hert, Thumfart, "The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies", s. 26.

olduğunu; bunlar yerine dijital ortama ilişkin tamamen yeni bir hukuki yaklaşım geliştirilmesi yönündedir<sup>42</sup>.

Uluslararası hukukta, devletlerin dijital ortam üzerindeki egemenliklerine özgü bir kural bulunmamaktadır. Doktrindeki hâkim görüş ise devletlerin dijital ortam üzerinde de egemenlikleri bulunduğunu kabul etmektedir<sup>43</sup>. Yukarıda da açıklandığı üzere dijital ortam temel olarak fiziki, mantıksal ve sosyal katmanlardan oluşmaktadır. Dijital ortamı oluşturan bu katmanlar, zaten devletlerin egemenlik alanlarında yani ülkelerinde fiziki olarak bulunmaktadır. Devletlerin ülkeleri üzerinde egemenlikleri olduğu göz önüne alındığında, ülkede bulunan katmanlar vasıtasıyla dijital ortam üzerinde de egemenlik haklarına sahip oldukları sonucuna ulaşılmaktadır<sup>44</sup>. Ayrıca herhangi bir devletin, kendi ülkesinde bulunan unsurlar üzerindeki egemenliğinden;

---

<sup>42</sup> Doone Jones, Kim-Kwang Raymond Choo, “Should There Be a New Body of Law for Cyber Space?”, **22nd European Conference on Information Systems**, Tel Aviv, 2014, s. 4, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2431614](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2431614), 24.12.2020; Yu Hong, Gerald Thomas Goodnight, “How to Think about Cyber Sovereignty: The Case of China”, **Chinese Journal of Communication**, 2020, s. 29, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3467933](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3467933), 01.01.2021.

<sup>43</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 11 (Tallinn Manual 2.0, yirmi kadar uzman tarafından NATO’nun talep ve desteği ile dijital ortama ilişkin uluslararası hukuk hakkında hazırlanmıştır. Dolayısıyla atfa konu kaynak, hakim görüş olarak çalışmamızda kabul edilmiştir.); Peter B.M.J. Pijpers, Bart van den Bosch, “The ‘Virtual Eichmann’: on Sovereignty in Cyberspace”, **Amsterdam Law School Research Paper**, No: 2020-65, 2020, s. 20, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3746843](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746843), 01.01.2021; Wolff Heintschel von Heinegg, “Legal Implications of Territorial Sovereignty in Cyberspace”, **NATO CCD COE Publications**, 2012, s. 19; Eichensehr, “The Cyber-Law of Nations”, s. 328; Benedikt Pirker, “Territorial Sovereignty and Integrity and the Challenges of Cyberspace”, **Right and Obligations of States in Cyberspace Part 2**, the Peacetime Regime for State Activities in Cyberspace - International Law, Foreign Affairs and Cyber-Diplomacy, Tallinn, 2013, s. 214, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3011337](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3011337), 17.12.2020; Eric Talbot Jensen, “Cyber Sovereignty: The Way Ahead”, **Texas International Law Journal**, C. 50, S. 2, 2015, s. 304; Sean Watts, Theodore T. Richard, “Baseline Territorial Sovereignty and Cyberspace”, **Lewis & Clark Law Review**, C. 22, S. 3, 2018, s. 872; Russell Buchan, **Cyber Espionage And International Law**, 1. bs, Oxford UK, Hart Publishing, 2019, s. 50; Binxing Fang, **Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace**, Beijing, China, Springer International Publishing and Science Press Beijing, 2018, s. 103. Ayrıca belirtmek gerekir ki Avustralya, Yeni Zelanda, Estonya, Çin, Fransa ve Hollanda dijital ortam üzerinde egemenlik hakkı bulunduğuna dair görüş beyan etmişlerdir (bkz. Pijpers, Bosch, “The ‘Virtual Eichmann’: on Sovereignty in Cyberspace”, s. 11); Rusya ve Çin ise dijital ortam üzerindeki egemenliğin tıpkı hava sahası gibi her devletin kendi dijital ortamı üzerinde egemenlik kurması şeklinde yorumlamaktadır (bkz. Eichensehr, “The Cyber-Law of Nations”, s. 336).

<sup>44</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 12; Fabio Christiano, “Palestine: Whose Cyber Security without Cyber Sovereignty?”, **Routledge Companion to Global Cyber-Security Strategy**, 2020, s.9, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3700850](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700850), 01.02.2021.

bu unsurların dijital ortama bağı olmaları nedeniyle feragat ettiğı sonucuna ulaşmak mümkün olmayacağı için de dijital ortam üzerinde devletlerin egemenliklerinin mevcut olduğu kabul edilmektedir<sup>45</sup>.

Hâkim görüşe göre bir devletin dijital ortam üzerinde tamamen egemenlik iddia etmesi de yine dijital ortamı oluşturan katmanların çeşitli ülkelerde bulunması nedeniyle mümkün değildir<sup>46</sup>. Zira her devlet, kendi ülkesinde bulunan katmanlar üzerinde egemenlik sahibidir ve bu nedenle başka ülkeler üzerinde bulunan katmanlara ilişkin egemenlik iddiasında bulunması uluslararası hukuka aykırı olacaktır.

Dijital ortamda devletin egemenliğinin bulunmasının sonucu ise devletin kendi egemenliği kapsamına giren fiziki altyapılar, kişiler ya da faaliyetler üzerinde egemenlik haklarını kullanabilmesidir<sup>47</sup>. Dolayısıyla bir devlet, egemenliği altında bulunan dijital ortam katmanları üzerinde, uluslararası hukuka uygun davranmak kaydıyla, dilediğı düzenlemeyi yapabilecek ve bu düzenlemenin uygulanmasını sağlayabilecektir<sup>48</sup>. Örnek olarak bir ülkede bulunan altyapılar ve ağ bağlantıları hakkında çeşitli güvenlik önlemleri alınması ya da belirli içeriklerin (çocuk pornosu ya da kumar gibi) hukuka aykırı kabul edilmesi veyahut da çeşitli içeriklere erişimin engellemesi gibi fiiller gösterilebilecektir.

Devletlerin kendi ülkeleri dışında bulunan, ancak ilgili devlete ya da ilgili devletin vatandaşlarına ait veriler üzerinde egemenlik hakkı bulunup bulunmadığı konusunda bir görüş birliği bulunmamaktadır. Konuya ilişkin azınlık görüş, söz konusu veriler üzerinde ilgili devletin egemenliği bulunduğu yönündedir<sup>49</sup>. Çoğunluk görüşü ise bahse konu veriler üzerinde ilgili devletin egemenlik hakkı bulunmadığı; ancak bu

---

<sup>45</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 13.

<sup>46</sup> **a.y.**

<sup>47</sup> **a.y.**

<sup>48</sup> Schmitt, Vihul, **a.g.e.**, s. 14.

<sup>49</sup> Schmitt, Vihul, **a.g.e.**, s. 16 (Bu kitabın hazırlanmasında görev alan 20'den fazla uzman arasında çıkan görüş ayrılığı neticesinde, azınlıkta kalan uzmanların görüşü bu şekilde ifade edilmiştir).

verilere ilişkin olarak ilgili devletin sınır ötesi uygulama kapsamına sahip hukuk kuralları getirebileceği şeklindedir<sup>50</sup>.

Kanaatimizce dijital ortam üzerindeki egemenliğin varlığı konusuna ilişkin olarak mevcut üç görüşten ilk ikisine, yani devletlerin dijital ortamda egemenlik hakları olmadığı ile siber alanın global olarak ortak bir alan olarak kabul edilmesi gerektiği görüşlerine katılmak mümkün değildir. Bu görüşler günümüz ihtiyaçlarını karşılamaktan uzaktır. Devletlerin dijital ortamdaki egemenliğine ilişkin mevcut hâkim görüşün birçok noktayı isabetli olarak değerlendirdiğini söylemek ise kanaatimizce mümkündür. Ayrıca bu konuda yeni yaklaşımlar geliştirilmesini öne süren fikirlere de ortada somut bir öneri olmadığı için itibar etmek uygun olmayacaktır. Ancak bu görüşün egemenlik hakkını, egemenliğin kullanıldığı bölgeye yani ülkeye bağlaması, dijital ortamın her yerden ve herkesçe erişilebilir olma özelliğini ortadan kaldırma riskini taşımaktadır<sup>51</sup>. Çünkü bu görüşe göre bir devletin dijital ortama erişimi sınırlaması ya da tamamen kapatması da egemenlik yetkileri içerisinde yer almaktadır.

Devletlerin dijital ortama ilişkin fiili uygulamalara bakıldığında ise hemen her devletin kendi ülkesinde etkisi bulunan konularda egemenlik yetkisini kullanmaya çalıştığı görülmektedir. Örnek vermek gerekirse AB çıkardığı kişisel verilerin korunması mevzuatları ile bölgesel olarak AB dışında bulunan kişileri de kendi kurallarına uymaya zorlamaya çalışmaktadır<sup>52</sup>. ABD ise verilere erişme konusundaki kendi mahkemelerinin verdiği kararları, veriler ABD dışında dahi olsa bağlayıcı olarak kabul etmektedir<sup>53</sup>. Çin ve İran gibi ülkeler ise birçok internet üzerinden faaliyette bulunan şirketlerin ülkelerinde faaliyette bulunmalarını yasaklamış durumdadır. Yine pek çok

---

<sup>50</sup> a.y.

<sup>51</sup> Cynthia E. Ayers, **Rethinking Sovereignty in the Context of Cyberspace**, Pennsylvania US, The United States Army War College, 2016, s. 67.

<sup>52</sup> “Regulation (EU) 2016/679 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 and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)”, (Çevrimiçi) [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf), 20.08.2017.

<sup>53</sup> “Stored Wire and Electronic Communications and Transactional Records Access Act”, C. Chapter 121 §§ 2701–2712, C. Chapter 121 §§ 2701–2712 18 U.S. Code §, (1986), (Çevrimiçi) <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>, 11.12.2020.

devlet, bazı faaliyetlere ilişkin verilerin kendi ülkelerinde depolanmasını şart koşturur<sup>54</sup>. Devletlerin bahsedilen şekillerde düzenlemeler yapması, devletlerin egemenlik haklarını dijital ortamda kullanmakta olduğunu açıkça göstermektedir. Dolayısıyla fiili durumda, devletlerin egemenliklerini dijital ortamda kullanmakta olduklarına dair herhangi bir şüphe bulunmamaktadır.

Devletlerin egemenlik haklarını fiilen kullanmaları hususu, uluslararası hukukta devletlerin uluslararası yetkisi başlığı altında incelenmektedir. Çalışmamızın bir sonraki başlığı altında bu konu detayları ile incelenecektir.

### III. DEVLETİN ULUSLARARASI YETKİSİ

#### A. Devletin Uluslararası Yetkisi Kavramı

Devletin uluslararası yetkisi (**jurisdiction**<sup>55</sup>), devletin uluslararası hukuktan doğan; belirli kişileri, eşyaları ya da fiilleri; düzenleme ya da başka şekillerde etkileme gücü olarak tanımlanmaktadır<sup>56</sup>. Devletin uluslararası yetkisi kavramı, özellikle devletin egemenliği kavramı ile yakından ilişkilidir. Zira devletin egemenlik haklarını fiilen kullanması, esasen devletin uluslararası yetkisini kullanması anlamına gelmektedir<sup>57</sup>. Devletin egemenlik haklarının sınırları, aynı zamanda o devletin uluslararası yetkisinin de sınırlarını teşkil etmektedir. Devletlerin birbirlerinin egemenliklerini

---

<sup>54</sup> Bkz. Aş. s. 250 vd.

<sup>55</sup> Bu kavram, dar anlamıyla en çok mahkemelerin yetkisi anlamında kullanılmaktadır. Uluslararası hukukta kullanıldığı geniş anlamıyla terimi karşılayabilmek amacıyla kavramın Türkçe karşılığı olarak “devletin uluslararası yetkisi” terimi çalışmamız boyunca kullanılacaktır.

<sup>56</sup> Shaw, **International Law**, s. 483; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 357; Brownlie, **Principles of Public International Law**, s. 298; Ünal, **Uluslararası Hukuk**, s. 237; Henriksen, **International Law**, s. 86; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 281; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 51; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 299; Focarelli, **International Law**, s. 284; Pazarcı, **Uluslararası Hukuk**, s. 159; Ergin Nomer, “Devletler Hususi Hukukunda Milletlerarası Yetki Mefhumi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 40, S. 1-4, 2011, s. 398; Ryngaert, **Jurisdiction in International Law**, s. 5.

<sup>57</sup> Shaw, **International Law**, s. 483; Brownlie, **Principles of Public International Law**, s. 106; Henriksen, **International Law**, s. 85; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 281; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 52; Çaşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 355; Ünal, **Uluslararası Hukuk**, s. 237; Pazarcı, **Uluslararası Hukuk**, s. 158.

ihlal etmeleri aynı zamanda uluslararası hukukun da ihlal edilmesi anlamına geleceğinden; herhangi bir devletin uluslararası yetkisini kullanırken diğer bir devletin egemenliğini ihlal etmesi de uluslararası hukukun ihlal edilmesi anlamına gelecektir. İşte bu nedenle devletlerin uluslararası yetkililerini, diğer devletlerin egemenliğini ihlal etmeyecek şekilde kullanmaları uluslararası hukukun gereklerinden birisidir<sup>58</sup>.

Devletin uluslararası yetkisi konusu, uluslararası hukuk yanında, diğer bazı hukuk dallarının da inceleme alanına konu olmaktadır. Uluslararası yetkinin kullanımı, iç hukuk açısından anayasa ve idare hukuku kapsamında incelenmektedir. Bu hukuk dalları devletin yetkilerinin sınırlanması ile bu yetkilerin nasıl kullanılacağına belirlenmesi noktalarına odaklanmış durumdadır. Kanunlar ihtilafı ve ceza hukuku<sup>59</sup> ise yabancılık unsuru içeren uyuşmazlıklara hangi devlet hukukunun uygulanacağını tespit etmeye çalışmakta; bir başka deyişle devletlerin uluslararası yetkisinin bir görünümü olan düzenleme yetkisi ile ilgilenmektedir. Milletlerarası usul hukuku ile ceza usul hukuku<sup>60</sup> da Türk mahkemelerinin yabancılık unsuru içeren olaylar açısından yetkisine; yani devletlerin uluslararası yetkisinin görünümünden bir diğeri olan yargılama yetkisinin nasıl kullanılacağı hususuna odaklanmaktadır.

Uluslararası yetki kavramı düzenleme, uygulama ve yargılama olmak üzere temel olarak üç alt başlıkta incelenmektedir. Ayrıca uluslararası yetkinin dayanak noktaları olarak mülklik, vatandaşlık ya da eylemlerin doğurduğu sonuçların etkileri gibi çeşitli kriterler kullanılmaktadır. Aşağıdaki başlıklar altında bu hususlar ile dijital ortama ilişkin devletin uluslararası yetkisi konuları irdelenecektir.

## **B. Devletin Uluslararası Yetkisinin Sınıflandırılması**

Devletin uluslararası yetkisi, kullanım alanlarına göre üç alt başlığa ayrılmaktadır<sup>61</sup>. Bunlar düzenleme yetkisi, uygulama yetkisi ve yargılama yetkisi olarak

---

<sup>58</sup> Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 359; Pazarcı, **Uluslararası Hukuk**, s. 161.

<sup>59</sup> Bu kapsamda TCK m. 8 ila 13 örnek olarak gösterilebilmektedir.

<sup>60</sup> Bu kapsamda CMK m. 12 ila 15 örnek olarak gösterilebilmektedir.

<sup>61</sup> Deniz hukukuna ilişkin olarak fonksiyonel yetki (**functional jurisdiction**) adlı bir kavram bulunmaktadır. Ancak bu kavram yaygın olarak doktrinde kabul edilmemektedir. Detaylı bilgi için bkz. Ryngaert, **Jurisdiction in International Law**, s. 4.



sıralanmaktadır. Düzenleme yetkisi, devletlerin hukuk kuralları koyma yetkisi anlamına gelmektedir. Uygulama yetkisi ise söz konusu hukuk kurallarına uyulmasını sağlama yetkisidir. Yargılama yetkisi ise bir devletin mahkemeleri vasıtasıyla yargılama yapma yetkisini ifade etmektedir.

Devletlerin uluslararası yetkisine ilişkin sınıflandırma; anayasalardaki yasama, yürütme ve yargı şeklinde sıralanan kuvvetler ayrılığı prensibini yansıtır gibi görünmekteyse de iç hukuktaki bu yaklaşım ile uluslararası yetki sınıflandırması birbirlerini tam olarak karşılamamaktadır. Düzenleme yetkisi açısından bakıldığında, hukuk kuralı koyma yetkisi sadece yasama organında olmadığı için (zira idarenin düzenleyici işlem yapma yetkisi de bulunmaktadır) düzenleme yetkisi ile yasama teriminin birebir aynı kavramı ifade ettiğini söylemek mümkün değildir. İdarelerin yaptığı düzenleyici işlemler de devletlerin düzenleme yetkisi kapsamına girmektedir. Benzer şekilde adli kolluk işlemleri uluslararası hukukta devletin uygulama yetkisi kapsamında değerlendirilmekteyken, iç hukukta yargı faaliyeti olarak kabul edilmektedir. Dolayısıyla uluslararası yetki sınıflandırması ile kuvvetler ayrılığı ilkesine göre devlet organlarının sınıflandırılması konularının birebir aynı ayrımı yapmadıkları sonucuna varmak mümkündür.

### 1. Düzenleme Yetkisi

Devletin uluslararası yetkisinin görünümlerinden birisi olan düzenleme yetkisi, bir devletin kişilere, eşyalara ya da fiillere yönelik hukuk kurallarını belirleme imkânı olarak tanımlanmaktadır<sup>62</sup>. Bu yetki sadece kanun koyucu yasama organları tarafından değil, aynı zamanda düzenleyici işlem yapan idareler (yani yürütme organı) tarafından da kullanılabilir. İlave olarak yargı kararlarının da kanun hükmü niteliği taşıdığı durumlar (örneğin Yargıtay içtihadı birleştirme kararları), söz konusu yetkinin yargı organı tarafından da kullanılabileceğini göstermektedir.

---

<sup>62</sup> Shaw, **International Law**, s. 486; Henriksen, **International Law**, s. 87; Focarelli, **International Law**, s. 285; Ryngaert, **Jurisdiction in International Law**, s. 9; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**; “Department of Defense Strategy for Operating in Cyberspace”.

## 2. Uygulama Yetkisi

Uygulama yetkisi, devletin uluslararası yetkisinin bir diğer görünümüdür. Uygulama yetkisi, bir devletin hukuk kurallarına uyulmasını sağlamak amacıyla güç kullanma otoritesi olarak tanımlanmaktadır<sup>63</sup>. Bu kapsamda fiziki olarak güç kullanılması (örneğin bir kişinin gözaltına alınması, hukuka aykırı bir binanın yıkılması ya da ülke içerisine kaçak yollarla giren birisinin yakalanması) ya da hukuk kurallarına uymayan kişilere idari para cezası uygulanması veya mahkeme kararlarının icra edilmesi gibi faaliyetler uygulama yetkisinin kullanımına örnekler teşkil etmektedir.

Uygulama yetkisi, bir devletin sadece kendi hukukundan doğan yükümlülükleri uygulayabileceği anlamına gelmemektedir. Gerekli koşulların varlığı halinde bir devlet, başka devletin hukukundan doğan yükümlülükleri de uygulayabilmektedir. Böyle durumlara örnek olarak yabancı suçlunun iadesi ya da yabancı bir mahkeme kararının tenfizi gösterilebilmektedir.

## 3. Yargılama Yetkisi

Devletin yargılama yetkisi, uluslararası yetkinin görünümlerinden bir diğeridir. Yargılama yetkisi, bir devletin mahkemelerinin yapacağı yargılama faaliyetleri vasıtasıyla hukuk kurallarını uygulama yetkisi olarak tanımlanmıştır<sup>64</sup>. Bir başka deyişle yargılama yetkisi, bir devletin mahkemelerinin yabancılık unsuru olsun ya da olmasın hangi hususlar hakkında yargılama yapabileceğine karar verme imkanındır.

19 yy.'da Avrupalı devletler, Osmanlı İmparatorluğu, Çin, ya da Japonya gibi ülkelerin hukuk sistemlerinin yeterli olmadığını öne sürerek kendi vatandaşları ile ilgili konularda konsolosluk mahkemeleri kurma yoluna gitmiştir<sup>65</sup>. Bahse konu ülkelerin güçlenmesine bağlı olarak egemenlik haklarını ciddi şekilde zedeleyen bu durum

---

<sup>63</sup> Shaw, **International Law**, s. 487; Henriksen, **International Law**, s. 96; Focarelli, **International Law**, s. 285; Ryngaert, **Jurisdiction in International Law**, s. 9; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 51.

<sup>64</sup> Shaw, **International Law**, s. 487; Focarelli, **International Law**, s. 285; Ryngaert, **Jurisdiction in International Law**, s. 10; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 52.

<sup>65</sup> Pazarcı, **Uluslararası Hukuk**, s. 163; Ryngaert, **Jurisdiction in International Law**, s. 61; Aybars Pamir, "Kapitülasyon Kavramı ve Osmanlı Devleti'ne Etkileri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 51, S. 2, 2002, s. 91.

ortadan kalkmıştır. Lozan Sözleşmesi çerçevesinde kapitülasyonların kaldırılması ile Türkiye Cumhuriyeti sınırları içerisinde Türk devletinden başka bir devletin yargılama yapma yetkisi de ortadan kalkmıştır<sup>66</sup>. Mahkemelerin yargılama yetkilerini ülke içerisinde hangi bölgelerde ve nasıl kullanacağı ise başta HMK, CMK ve İYUK olmak üzere TBMM tarafından çıkarılan kanunlarla belirlenmiş durumdadır.

Mahkemelerin yabancılik unsuru taşıyan uyuşmazlıklara dair yargılama yapma yetkileri, mahkemelerin milletlerarası yetkisi kavramı altında tanımlanmaktadır<sup>67</sup>. Hukuk mahkemelerinin milletlerarası yetkisi, milletlerarası özel hukuk alanı çerçevesinde incelenmektedir. Bu kapsamda MÖHUK m. 40 ila 47, Türk hukuk mahkemelerinin milletlerarası yetkisini belirlemektedir. CMK m. 12 ila 15 ise Türk ceza mahkemelerinin milletlerarası yetkisinin sınırlarını çizmektedir. Türk idare mahkemelerinin yetkisi ise İYUK m. 32 ila 37 kapsamında belirlenmektedir. Ancak idari davalarda sadece Türk idare organları taraf gösterilebileceği için idari yargıda milletlerarası yetkiden bahsetmek mümkün olmamaktadır.

Yargılama yetkisi ile düzenleme yetkisi arasındaki farka değinmek gerekmektedir. Yargılama yetkisi, mahkemelerin yetkisi ve yargılama faaliyeti yürütmesi ile ilgilenmektedir. Düzenleme yetkisi ise kanunların uygulama kapsamlarına (bölgesel ya da zamansal uygulama kuralları veya kuralların hangi kişilere uygulanabileceği gibi) odaklanmaktadır. Örnek vermek gerekirse, TCK m. 8 ila 13, hangi suçların ve hangi kişilerin TCK'ya tabi olduğunu göstermektedir. Buna karşılık CMK m. 12 ila 15, Türk ceza mahkemelerinin yargılama yapma yetkilerinin bölgesel sınırlarını çizmektedir. İlgili TCK hükümleri, devletin uluslararası yetkisinin görünümlerinden birisi olan düzenleme yetkisinin kullanımına örnek teşkil etmektedir. CMK hükümleri ise devletin yargılama yetkisinin kullanımına bir örnektir.

---

<sup>66</sup> Pazarcı, **Uluslararası Hukuk**, s. 163; “Lozan Antlaşması”, (1923) m. 28.

<sup>67</sup> Akıncı, **Milletlerarası Özel Hukuk**, s. 114-144; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 565-670.

### C. Devletin Uluslararası Yetkisini Kendi Ülkesi İçerisinde Kullanması

Devletin uluslararası yetkisi, yukarıda da açıklandığı üzere devletin egemenlik haklarının fiilen kullanımı anlamına gelmektedir. Modern dönemlerden önce devletin egemenlik haklarını kullanma konusunda dayandığı nokta, ilgili kişinin o devletin tebaasına ait olup olmamadır. Yani bir kişiye uygulanacak hukuk kuralları, o kişinin bulunduğu bölgeye göre değil; ait olduğu kavme göre belirlenmektedir. Örneğin Roma döneminde kişilerin bulunduğu yer fark etmeksizin Romalılara **ius civile**; yabancılara ise **ius gentium** uygulanmıştır<sup>68</sup>. Günümüzün vatandaşlık kavramı ile açıklanan belirli bir kavme ait olma durumunu özdeşleştirmek mümkündür.

1648 yılında imzalanan Vestfalya Sözleşmesinden itibaren devletlerin egemenliğinin kişiler üzerinde değil; ülke üzerinde bulunduğu yaklaşımı uluslararası hukukta kabul edilmeye başlanmıştır<sup>69</sup>. Sözleşme sonrasında belirli bir kavme ait olan kişiye o kavmin hukukunun uygulanması yaklaşımı terk edilmiştir. Bunun yerine ülke içerisinde bulunan herkese, söz konusu kişilerin ait olduğu kavim fark etmeksizin, ülke üzerinde egemen olan devletin hukukunun uygulanması yaklaşımı yani mülkilik ilkesi benimsenmiştir. Egemenliğin mülkiliği ilkesi neticesinde devletlerin ülkeleri içerisinde uluslararası yetkilerini kullanmalarının uluslararası hukuka uygun olduğu kabul edilmiştir<sup>70</sup>. Mülkilik ilkesi halen daha geçerliliğini korumaktadır.

<sup>68</sup> Ryngaert, **Jurisdiction in International Law**, s. 51; Özlem Söğütü, **Roma Özel Hukuku**, 1. bs, Ankara, Seçkin Yayıncılık, 2020, s. 100; Andreas Schwarz, **Roma Hukuku Dersleri**, C. I, çev. Türkan Rado, 7. bs, İstanbul, Doğan Kardeş Basımevi, 1965, s. 105; Paul Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, çev. Kudret Ayiter, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1971, s. 10; Ziya Umur, **Roma Hukuku Ders Notları**, 3. bs, İstanbul, Beta Basım A.Ş., 2010, s. 93; Bülent Tahiroğlu, Belgin Erdoğan, **Roma Hukuku Dersleri**, 14. bs, İstanbul, DER Kitabevi, 2020, s. 127; Paul Du Plessis, Andrew Borkowski, **Borkowski's Textbook on Roman Law**, 5. bs, New York, Oxford University Press, 2015, s. 111; A. Arthur Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, New York, Columbia University School of Law, 1936, s. 173; Paul J. Du Plessis, Clifford Ando, Kaius Tuori, **The Oxford Handbook of Roman Law And Society**, Great Britain, Oxford University Press, 2016, s. 584.

<sup>69</sup> Doğan, **Devletler Hukuku**, s. 49; Ryngaert, **Jurisdiction in International Law**, s. 54; Ayers, **Rethinking Sovereignty in the Context of Cyberspace**, s. 68.

<sup>70</sup> Shaw, **International Law**, s. 485; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 369; Ünal, **Uluslararası Hukuk**, s. 238; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 52; Brownlie, **Principles of Public International Law**, s. 300; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 282; Henriksen, **International Law**, s. 86; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 302; Focarelli, **International Law**, s. 284; Ryngaert, **Jurisdiction in**

Devletlerin uluslararası yetkilerini ülke içerisinde kullanmaları, objektif mülkilik (ya da etki doktrini) ve sübjektif mülkilik olarak iki alt sınıfa ayrılmaktadır. Sübjektif mülkilik, bir fiilin ülke içerisinde başlatılması; ancak sonucunun başka bir ülkede meydana gelmesi halinde fiilin başlatıldığı ülkedeki egemen devletin uluslararası yetki kullanabileceğini öne sürmektedir<sup>71</sup>. Buna karşılık objektif mülkilik ise başka ülkede gerçekleşen bir fiil hakkında, fiilin etkilerinin doğduğu ülkede egemen olan devletin uluslararası yetki bulunabileceğini ifade etmektedir<sup>72</sup>.

Öte yandan belirtmek gerekir ki egemenliğin mülkiliği ilkesi, iletişimin ve ticari ilişkilerin son derece geliştiği günümüz dünyasının hukuki sorunlarını çözmek için yeterli olmamaktadır. Bu nedenle devletlerin uluslararası yetkilerini kendi ülke sınırları dışında da kullandıkları senaryolar ortaya çıkmıştır. Bu konu bir sonraki başlıkta incelenecektir.

#### **D. Devletin Uluslararası Yetkisini Sınır Ötesi Uygulama Kapsamına Sahip Olarak Kullanması**

Gelişen ulaşım ve iletişim imkanları nedeniyle uluslararası nitelikteki hukuki işlemlerin sayısı önemli ölçüde artmıştır. Bu da devletlerin uluslararası yetkilerini, ülkeleri dışında da kullanmaları ihtiyacını doğurmuştur<sup>73</sup>. Devletlerin ülkeleri dışında da vatandaşlarını ve menfaatlerini korumak istemeleri, başka bir ülkede işlenen ancak etkisini diğer bir ülkede doğuran suçlar, yabancı bir ülkede yapılan faaliyetler

---

**International Law**, s. 49; Maria Gavouneli, **Functional Jurisdiction in the Law of the Sea**, Leiden, Hollanda, Martinus Nijhoff Publishers, 2007, s. 7.

<sup>71</sup> Shaw, **International Law**, s. 490; Henriksen, **International Law**, s. 88; Brownlie, **Principles of Public International Law**, s. 301; Ünal, **Uluslararası Hukuk**, s. 238; Focarelli, **International Law**, s. 287; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 303; Ryngaert, **Jurisdiction in International Law**, s. 79; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 56; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 7.

<sup>72</sup> Shaw, **International Law**, s. 490; Henriksen, **International Law**, s. 88; Ünal, **Uluslararası Hukuk**, s. 238; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 297; Focarelli, **International Law**, s. 287; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 303; Ryngaert, **Jurisdiction in International Law**, s. 78; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**; Gavouneli, **Functional Jurisdiction in the Law of the Sea**; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**.

<sup>73</sup> Ryngaert, **Jurisdiction in International Law**, s. 8.

vasıtasıyla diğerk bir ÷lkenin piyasalarını bozan işlemler gibi konular söz konusu ihtiyacın kaynaklarından bazılarıdır. İnternet ile gelen gelişmiş ve konumdan bağımsız iletişim imkanları da uluslararası yetkinin ÷lke dışında kullanımı ihtiyacını ciddi bir şekilde arttırmıştır.

Uluslararası yetkinin bir devlet tarafından kendi ÷lkesi dışında kullanımına sınır ötesi yetki (**extraterritorial jurisdiction**) adı verilmektedir<sup>74</sup>. Örneğın bir devletin kendi ÷lkesi sınırları dışında bulunan bir vatandaşına karşı yine kendi ÷lkesi dışında gerçekleştirilen bir fiili suç olarak tanımlaması, o devletin kendi uluslararası yetkisini sınır ötesi olarak kullanmasına örnek teşkil etmektedir.

Sınır ötesi yetki kullanımı, uluslararası hukuka her zaman için aykırı kabul edilmemektedir. Kullanılan uluslararası yetki sınıfına göre, sınır ötesi yetki kullanımının sınırları belirlenmiş durumdadır. Bu sınırlar aşağıdaki başlıklar altında değerlendirilecektir.

Sınır ötesi yetki kavramına geçmeden önce değinilmesi gereken bir diğerk husus ise iç hukukun uzaması kavramıdır. Bu kavram, tamamen mülki olarak uygulanan bir hukuk kuralının, yurtdışında bulunan kişileri ya da gerçekleşen fiilleri etkilemesini ifade etmektedir<sup>75</sup>. İç hukukun uzaması yöntemi, AB tarafından iç pazarına erişime izin vermek için kendi hukuk kurallarına uyma koşulu olarak konumlandırılmak suretiyle yaygın olarak kullanılmaktadır<sup>76</sup>. Örneğın AB hava sahasında faaliyet göstermek isteyen uçakların, dünyanın her yerinde yaptıkları uçuşlardaki güvenlik ve performans kayıtlarının AB hukuku ile uyumlu olması gerekmektedir<sup>77</sup>. Benzer uyumluluk gereksinimleri, ihracat ve finans gibi birçok alanda da mevcuttur<sup>78</sup>. Söz konusu yaklaşım nedeniyle uluslararası yetki, mülkilik ilkesi çerçevesinde kullanılmakta

---

<sup>74</sup> Ryngaert, **a.g.e.**, s. 7.

<sup>75</sup> Ryngaert, **a.g.e.**, s. 94; Joanne Scott, “Extraterritoriality and Territorial Extension in EU Law”, **American Journal of Comparative Law**, C. 62, S. 1, 2014, s. 90.

<sup>76</sup> Ryngaert, **Jurisdiction in International Law**, s. 94; Scott, “Extraterritoriality and Territorial Extension in EU Law”, s. 108.

<sup>77</sup> Ryngaert, **Jurisdiction in International Law**, s. 94; Scott, “Extraterritoriality and Territorial Extension in EU Law”, s. 96.

<sup>78</sup> Ryngaert, **Jurisdiction in International Law**, s. 95; Scott, “Extraterritoriality and Territorial Extension in EU Law”, s. 103.

olmasına rağmen hukuk kurallarının etkisi diğer ülkelere de yayılmaktadır<sup>79</sup>. Doğrudan yabancı ülkedeki bir faaliyeti düzenleme amacı olmadığı için burada uluslararası yetkinin sınır ötesi kullanımından bahsetmek mümkün olmamaktadır. İç hukukun uzaması konusu, çalışmamızın konusu dışında kalmaktadır.

### 1. Düzenleme Yetkisinin Sınır Ötesi Kullanımı

Düzenleme yetkisinin sınır ötesi kullanımı, diğer yetki sınıflarına göre oldukça yaygındır ve çözülmesi daha karmaşık sorunlar oluşturmaktadır. Yargılama ya da uygulama yetkilerinin sınır ötesi kapsamda kullanılması, bu yetkilerin fiili olarak kullanılmaları (bir kişinin yakalanması için kolluk gücü kullanılması ya da yargılanması için mahkeme kurulması gibi) gerektiği için oldukça sınırlıdır. Ancak düzenleme yetkisi sadece hukuk dünyasında sonuç doğurduğu için çok daha kolay bir şekilde sınır ötesi kapsamda kullanılabilir.

Düzenleme yetkisinin sınır ötesi kapsamda kullanımı konusu, uluslararası hukukta uzun bir süredir tartışılmaktadır. Konu ilk olarak Uluslararası Daimî Adalet Divanı'nın 1927 tarihli **Lotus** kararı<sup>80</sup> ile ele alınmıştır. Daha sonraki dönemlerde konuya ilişkin çeşitli görüşler ve teamüller ortaya atılmıştır. Aşağıdaki başlıklar altında uluslararası hukukun bu konudaki durumu incelenecektir.

#### a. Lotus Kararı Çerçevesinde Düzenleme Yetkisinin Sınır Ötesi Kullanımı

Türkiye Cumhuriyeti açısından da son derece önemli bir dava olan **Lotus** davası, 2 Ağustos 1926 tarihinde Midilli Adası açıklarında Türk gemisi Bozkurt ile Fransız gemisi **Lotus**'un çarpışması nedeniyle iki ülke arasında doğan uyuşmazlığı konu almaktadır. Çarpışma neticesinde 8 Türk denizci hayatını kaybetmiştir. Ertesi gün İstanbul'a varan **Lotus**'un kaptanı Türk mahkemelerince tutuklanmış ve yapılan yargılama neticesinde hapis ile para cezalarına çarptırılmıştır. Bu işlemler sırasında Fransa, Türkiye'nin bir Fransız vatandaşını yargılama konusunda uluslararası yetkisi olmadığını ve bu nedenle yapılan yargılamanın uluslararası hukuku ihlal ettiğini iddia

<sup>79</sup> Ryngaert, **Jurisdiction in International Law**, s. 96; Scott, "Extraterritoriality and Territorial Extension in EU Law", s. 90.

<sup>80</sup> Lotus Case, France v. Turkey, (Permanent Court of International Justice 1927).

etmiştir. Bu uyuşmazlığı çözmek adına Türkiye ve Fransa, konunun Uluslararası Daimî Adalet Divanı<sup>81</sup> önünde çözülmesi yönünde mutabakata varmışlardır. Uyuşmazlığı inceleyen Uluslararası Daimî Adalet Divanı, 1927 yılında verdiği kararda Türkiye'nin yargılama yapma konusunda uluslararası yetkisinin bulunduğu sonucuna varmıştır.

Divan, kararın gerekçesinde öncelikle uluslararası yetki kavramının iki alt sınıfı bulunduğunu ve bunların düzenleme yetkisi ile uygulama yetkisi olarak adlandırıldığını ifade etmiştir<sup>82</sup>. Divan kararına göre bir devlet, uygulama yetkisini başka bir devletin ülkesinde ancak ev sahibi ülkenin rızası olması halinde kullanabilecektir. Zira uluslararası hukuka göre her devletin kendi ülkesindeki egemenliği mutlaklıdır. Dolayısıyla ev sahibi devletin rızası olmadan o ülke içerisinde uygulama yetkisi kullanmak, ev sahibi devletin egemenliğinin ve dolayısıyla da uluslararası hukukun ihlali sonucunu doğuracaktır<sup>83</sup>.

Düzenleme yetkisi açısından ise Divan, her devletin bu yetkiyi kendi ülkesi dışında kullanmakta serbest olduğu kanaatine varmıştır<sup>84</sup>. Divana göre düzenleme yetkisinin ülke sınırları dışında kullanımını engelleyen bir uluslararası hukuk kuralı yoksa (egemenliğin ülke içerisinde mutlak olarak o ülkede bulunan devlete ait olması kuralı, uygulama yetkisi açısından ülke sınırları dışında yetki kullanımını engelleyen bir kural olarak değerlendirilmiştir), devletin egemenlik haklarını ve dolayısıyla da uluslararası yetkisini sınırlamak mümkün değildir<sup>85</sup>. Düzenleme yetkisini sınırlayan ve olaya

---

<sup>81</sup> Uluslararası Daimî Adalet Divanı, 1922 ile 1946 yılları arasında Milletler Cemiyeti nezdinde faaliyet göstermiş olan ilk genel yetkili uluslararası mahkemedir. Bu mahkeme yerini Birleşmiş Milletler nezdinde faaliyet yürütmekte olan Uluslararası Adalet Divanı'na bırakmıştır. Detaylı bilgi için bkz. "Permanent Court of International Justice | International Court of Justice", (26.03.2021), (Çevrimiçi) <https://www.icj-cij.org/en/pcij>, 26.03.2021.

<sup>82</sup> Ryngaert, **Jurisdiction in International Law**, s. 31.

<sup>83</sup> Ryngaert, **a.g.e.**, s. 32; Luc Reydams, **Universal Jurisdiction International and Municipal Legal Perspectives**, New York, Oxford University Press, 2006, s. 12; Michael Akehurst, "Jurisdiction in International Law", **British Year Book of International Law**, C. 46, 1972, s. 146.

<sup>84</sup> Ryngaert, **Jurisdiction in International Law**, s. 31; Reydams, **Universal Jurisdiction International and Municipal Legal Perspectives**, s. 12.

<sup>85</sup> Ryngaert, **Jurisdiction in International Law**, s. 32; Reydams, **Universal Jurisdiction International and Municipal Legal Perspectives**, s. 13.



uygulanabilecek bir hukuk kuralının mevcut olmaması, Divan'ın bu şekilde karar vermesine sebebiyet vermiştir.

Netice itibarıyla **Lotus** kararı, aksine bir uluslararası hukuk kuralı olmadığı sürece düzenleme yetkisinin sınır ötesi kapsamda kullanılabileceği sonucuna varmıştır. Ancak bu kural, kontrolsüz bir şekilde uluslararası yetki iddialarının artmasına sebep olabileceği gerekçesiyle doktrinde eleştirilmiştir<sup>86</sup>. **Lotus** kararı ile belirlenen bu kuraldan, Uluslararası Adalet Divanı'nın<sup>87</sup> 1970 tarihli **Barcelona Traction** kararı ile kısmen de olsa dönülmüştür<sup>88</sup>. **Lotus** kararında ortaya konulan kuraldan farklı devlet uygulamaları ve milletlerarası sözleşmelerin de bu konudaki uluslararası teamül hukukunu oluşturduğu kabul edilmektedir<sup>89</sup>. Tüm bu gelişmeler neticesinde doktrinde **Lotus** kararının hala etkisini koruyan bir içtihat teşkil etmediği öne sürülmüştür<sup>90</sup>. Buna karşılık devletlerin hala bu kararı uygulamalarında dayanak aldıkları görülmektedir<sup>91</sup>. İşte bu nedenle **Lotus** kararının etkisinin hala sürüp sürmediği konusunda yeterince araştırma yapılmadığı şeklinde bir görüş de ortaya çıkmıştır<sup>92</sup>.

#### **b. Uluslararası Teamül Hukuku Çerçevesinde Düzenleme Yetkisinin Sınır Ötesi Kullanımı**

Devletlerin zaman içerisindeki uygulamaları ile ortaya çıkan uluslararası teamül hukuku, düzenleme yetkisinin sınır ötesi kullanımı konusunda **Lotus** kararı ile tamamen ters bir yaklaşım benimsemiştir. Uluslararası teamül hukukuna göre düzenleme yetkisinin sınır ötesi kullanımı kural olarak yasaktır. Ancak sınır ötesi

---

<sup>86</sup> Ryngaert, **Jurisdiction in International Law**, s. 33; Walter Wheeler Cook, "The Application of the Criminal Law of a Country to Acts Committed by Foreigners Outside the Jurisdiction", **West Virginia Law Review**, C. 40, S. 4, 1934, s. 326; Reydams, **Universal Jurisdiction International and Municipal Legal Perspectives**, s. 13.

<sup>87</sup> Özgün adı International Court of Justice olan bu mahkeme hakkında detaylı bilgi için bkz. "The Court" (Çevrimiçi) <https://www.icj-cij.org/en/court>, 27.03.2021.

<sup>88</sup> Case Concerning Barcelona Traction, Light and Power Company Limited (Belgium vs. Spain), 1962, (International Court of Justice 05 Şubat 1970).

<sup>89</sup> Ryngaert, **Jurisdiction in International Law**, s. 34.

<sup>90</sup> Ryngaert, a.y.; Reydams, **Universal Jurisdiction International and Municipal Legal Perspectives**, s. 16.

<sup>91</sup> Ryngaert, **Jurisdiction in International Law**, s. 34.

<sup>92</sup> Pieter Jan Kuyper, "The European Community and the US Pipeline Embargo: Comments on Comments", **German Yearbook of International Law**, C. 27, 1984, s. 93, (Çevrimiçi) <https://heinonline.org/HOL/Page?handle=hein.journals/gyl127&id=72&div=&collection=>, 10.04.2021.

kullanıma izin veren bir hukuk kuralı varsa, bu durumda sınır ötesi düzenleme yetkisi kullanımı hukuka uygun kabul edilecektir<sup>93</sup>.

Devletlerin uluslararası yetkilerini kullanırken dayandıkları en önemli uluslararası hukuk ilkesi, egemenliğin mülkiliğidir. Yani bir devlet, kendi ülkesi içerisinde mutlak egemenliğe sahiptir ve bu egemenliğinden doğan uluslararası yetkisini kendi ülkesi içerisinde dilediği gibi kullanabilmektedir. Bölgesellik ilkesi, uluslararası teamül hukuku çerçevesinde sınır ötesi yetki kullanımının kural olarak yasak olmasının temel gerekçesini oluşturmaktadır. Zira bölgesellik ilkesi, aynı zamanda devletlerin eşitliği ve birbirlerinin iç işlerine karışma yasağı gibi temel uluslararası hukuk kurallarının da temelini oluşturmaktadır. Bu kurallar da bir devletin kendi sınırları dışında uluslararası yetki kullanımı önünde engel teşkil etmektedirler. İşte bu nedenle uluslararası teamül hukuku, düzenleme yetkisinin sınır ötesi kullanımını; aksi yönde bir uluslararası düzenlemesi yoksa, yasak olarak kabul etmektedir<sup>94</sup>.

Düzenleme yetkisinin sınır ötesi kapsamda kullanılmasının uluslararası hukuka uygun kabul edildiği hallerde müsamahakâr ilkeler (**permissive principles**) adı verilmektedir<sup>95</sup>. Müsamahakâr ilkeler, egemenliğin mülkiliği ilkesi neticesinde ortaya çıkmış kurallar değildir<sup>96</sup>. Bu ilkeler toplumsal beklentileri karşılamak amacıyla egemenliğin mülkiliği, devletlerin eşitliği ve başka devletlerin içişlerine karışma yasağı gibi kurallara istisna olarak meydana getirilmişlerdir<sup>97</sup>. Yine de bu ilkelere dayalı olarak düzenleme yetkisinin sınır ötesi kullanımı aynı zamanda devletlerin egemenlikten kaynaklanan uluslararası yetkilerini kullanmaları anlamına gelmektedir<sup>98</sup>. Müsamahakâr ilkelere dayanılarak uluslararası düzenleme yetkisinin kullanılması ile mülkilik ilkesine dayanılarak uluslararası düzenleme yetkisinin kullanılması hiyerarşik olarak eşit seviyede yetki kullanımı anlamına gelmektedir.

---

<sup>93</sup> Ryngaert, **Jurisdiction in International Law**, s. 35.

<sup>94</sup> Ryngaert, **a.g.e.**, s. 36.

<sup>95</sup> Ryngaert, **a.g.e.**, s. 129; Reydam, **Universal Jurisdiction International and Municipal Legal Perspectives**, s. 21.

<sup>96</sup> Ryngaert, **Jurisdiction in International Law**, s. 37.

<sup>97</sup> Ryngaert, **a.y.**

<sup>98</sup> Ryngaert, **a.y.**

Müsamahakâr ilkelerden en az birinin varlığı, düzenleme yetkisinin sınır ötesi kapsamda kullanılmasını uluslararası hukuka uygun hale getirmektedir. Aşağıdaki başlıklar altında her bir müsamahakâr ile ilke tek tek incelenecektir.

### (1) Aktif Kişilik İlkesi

Aktif kişilik ya da diğer adıyla vatandaşlık ilkesine göre her devlet, kendi vatandaşları üzerinde uluslararası yetkisini, vatandaşın bulunduğu ülke fark etmeksizin kullanabilme hakkına sahiptir<sup>99</sup>. Hatta bazı milletlerarası sözleşmelere ve ABD Yüksek Mahkemesi kararlarına göre devletlerin kendi vatandaşları üzerinde uluslararası yetki kullanmaya mecbur oldukları kabul edilmektedir<sup>100</sup>.

Aktif kişilik ilkesi özellikle ceza hukukunda, vergi hukukunda ve milletlerarası aile hukukunda etkisini göstermektedir. Söz konusu hukuk dalları çerçevesinde vatandaşların, bulundukları ülke fark etmeksizin vatandaşı oldukları devletin hukuk kurallarına tabi tutulmaları sık karşılaşılan bir durumdur<sup>101</sup>. ABD'nin ekonomik yaptırımlara ilişkin mevzuatına göre de ABD vatandaşı gerçek kişilerin ya da ABD hukukuna göre kurulmuş tüzel kişilerin fiilleri, bu kişiler dünyanın neresinde olursa olsun ABD hukukuna tabi kılınmıştır<sup>102</sup>. İran ya da Kuzey Kore gibi ülkelerle yapılacak ticarete ilişkin kısıtlamalar, bu konuda örnek olarak gösterilebilecektir.

---

<sup>99</sup> Shaw, **International Law**, s. 493; Henriksen, **International Law**, s. 89; Brownlie, **Principles of Public International Law**, s. 304; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 290; Ünal, **Uluslararası Hukuk**, s. 238; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 372; Focarelli, **International Law**, s. 290; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 306; Ryngaert, **Jurisdiction in International Law**, s. 104; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 60; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 13.

<sup>100</sup> Bu kapsamdaki milletlerarası sözleşme örnekleri şunlardır: United Nations Convention against Corruption, 31 Ekim 2003, m. 44/4; International Convention for the Suppression of Terrorist Bombings, 15 Aralık 1997, m. 6/1; International Convention for the Suppression of the Financing of Terrorism, 9 Aralık 1999, m. 7/1; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 10 Aralık 1984, m. 5. Konuya ilişkin örnek mahkeme kararı olarak bkz. United States v. Flores, 567, (U.S. Supreme Court 1937).

<sup>101</sup> Örneğin yurtdışında bulunan ABD vatandaşlarının hala ABD Hukukuna tabi olmaya devam edeceğine ilişkin karar için bkz. Blackmer v. United States, 200, 201, (U.S. Supreme Court 1932).

<sup>102</sup> "Export Control Reform Act of 2018", (2018), (Çevrimiçi) <https://www.congress.gov/bill/115th-congress/house-bill/5040>, 29.03.2021. Benzer durum ABD ile ilişkili kişilerin yurtdışında yolsuzluk yapmalarını engellemek için çıkarılan şu kanunda da mevcuttur: "The Foreign Corrupt Practices Act of 1977", (29.03.2021), (Çevrimiçi) <https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2012/11/14/fcpa-english.pdf>, 29.03.2021.

Modern dönemlerden önce devletlerin egemenliklerini kullanma konusunda dayandıkları nokta, o devletin halkına ait olup olmamaktır. Yani bir kişiye uygulanacak hukuk kuralları, kişinin bulunduğu bölgeye göre değil; ait olduğu kavme göre belirlenmektedir. Aktif kişilik ilkesi, işte bu prensibin günümüzdeki yansımaları oluşturmaktadır<sup>103</sup>.

## (2) Pasif Kişilik İlkesi

Pasif kişilik ilkesi, bir devletin kendi vatandaşına karşı herhangi bir fiilde bulunan kişiler üzerinde düzenleyici yetkisini sınır ötesi kapsamda kullanması anlamına gelmektedir<sup>104</sup>. Özellikle terör ve açık denizlerde korsanlık gibi konularda, devletler pasif kişilik ilkesine başvurarak kendi vatandaşlarına karşı saldırılarda bulunan kişilerin fiillerini suç sayabilmektedir<sup>105</sup>.

Pasif kişilik ilkesi doktrinde ciddi şekilde eleştirilmektedir<sup>106</sup>. Faillerin, hedef aldığı kişilerin vatandaşlığını bilmeleri mümkün değildir. Kaldı ki vatandaşlığı bilseler dahi o ülkenin hukuk kurallarını bilmelerini de kendilerinden beklemek doğru olmayacaktır. Dolayısıyla düzenleyici yetki kapsamına giren kişinin (yani failin) hangi hukuk kuralına tabi olduğunu bilmeden bu hukuk kuralının sonuçları ile karşılaşması durumu, bu ilkenin doktrinde eleştirilmesine sebep olmuştur<sup>107</sup>. Başka bir görüşe göre ise pasif kişilik ilkesi sayesinde bir devletin hukuku, diğer devletin ülkesindeki hukuki belirlilik ilkesini zedelemekte olduğu için düzenleyici yetkinin aşkın kullanımı olarak kabul edilmelidir<sup>108</sup>.

---

<sup>103</sup> Ryngaert, **Jurisdiction in International Law**, s. 107; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 13.

<sup>104</sup> Shaw, **International Law**, s. 497; Brownlie, **Principles of Public International Law**, s. 304; Henriksen, **International Law**, s. 90; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 293; Ünal, **Uluslararası Hukuk**, s. 238; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 376; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 308; Ryngaert, **Jurisdiction in International Law**, s. 110; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 60; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 29.

<sup>105</sup> Ryngaert, **Jurisdiction in International Law**, s. 111; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 30.

<sup>106</sup> Akehurst, "Jurisdiction in International Law", s. 163.

<sup>107</sup> Ryngaert, **Jurisdiction in International Law**, s. 111.

<sup>108</sup> Francis Mann, "The Doctrine of Jurisdiction in International Law", **Recueil des Cours de l'Académie de droit international**, C. I, S. 111, 1964, s. 92.

Devletlerin uygulamasında ise pasif kişilik ilkesinin, diğer devletlerce ciddi bir itiraz olmaksızın kullanılmaya devam ettiği görülmektedir<sup>109</sup>. Bu durumun ilk sebebi, pasif kişilik ilkesinin her türlü fiil için değil; sadece ciddi suç (öldürme, terör, diplomatlara saldırı ya da tecavüz gibi) teşkil edebilecek fiiller için uygulanıyor olmasıdır<sup>110</sup>. İkinci sebep ise failin düzenleyici yetki kullanan devlet ülkesinde bulunmadığı durumlarda, pasif kişilik ilkesine dayanabilmek için failin bulunduğu devletin iş birliğinin gerekmesidir<sup>111</sup>. Dolayısıyla ilgili devletler arasında bir uzlaşma olmadan pasif kişilik ilkesi çerçevesinde düzenleme yetkisinin sınır ötesi kapsamda kullanılması da mümkün olmamaktadır.

### (3) Koruma İlkesi

Bir devletin kendi ülkesi dışında, yine o devletin egemenliğine ya da siyasi bağımsızlığına karşı gerçekleştirilen fiiller üzerinde düzenleme yetkisini kullanabilmesi, koruma ilkesi gereğince mümkündür<sup>112</sup>. Devletlerin uygulamalarında yaygın olarak kullanıldığı için koruma ilkesinin uluslararası teamül hukukunun bir parçası olduğuna şüphe bulunmamaktadır<sup>113</sup>.

Koruma ilkesine dayanılarak sınır ötesi düzenleme yetkisi kullanılan durumlara örnek olarak sahte para basımı, vize almak için gerçeğe aykırı beyanda bulunma ya da uyuşturucu kaçakçılığı gibi fiillerin suç sayılması verilebilmektedir<sup>114</sup>. Ayrıca ülkelerin uyguladıkları ambargolarda da bu ilkenin kullanıldığı görülmektedir<sup>115</sup>. Örneğin 1996 tarihli bir kanun ile ABD, vatandaşlığı fark etmeksizin tüm kişilerin;

<sup>109</sup> Ryngaert, **Jurisdiction in International Law**, s. 111.

<sup>110</sup> Ryngaert, a.y.; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 30.

<sup>111</sup> Ryngaert, **Jurisdiction in International Law**, s. 113.

<sup>112</sup> Shaw, **International Law**, s. 499; Henriksen, **International Law**, s. 91; Brownlie, **Principles of Public International Law**, s. 304; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 291; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 377; Ünal, **Uluslararası Hukuk**, s. 240; Focarelli, **International Law**, s. 291; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 307; Ryngaert, **Jurisdiction in International Law**, s. 114; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 60; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 29.

<sup>113</sup> Ryngaert, **Jurisdiction in International Law**, s. 116; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 32.

<sup>114</sup> Bu konudaki bir ABD mahkemesi kararı için bkz. United States of America, Appellee, v. Jean Philomena Pizzarusso, 155/31392, (United States Court of Appeals, Second Circuit 1968).

<sup>115</sup> Ryngaert, **Jurisdiction in International Law**, s. 117.

ABD vatandaşlarına ait kamulaştırılmış eşyaların Küba'dan çıkarmasını ya da Küba'ya götürmesini yasaklamıştır<sup>116</sup>.

#### (4) Evrensellik İlkesi

Müsamahakâr ilkelerden bu başlığa kadar incelenen her birinin ortak özelliği, düzenleme yetkisinin kullanımı ile yetki kullanan devlet arasında bir bağlantı (örneğin vatandaşlık) olmasıdır. Evrensellik ilkesinde ise herhangi bir bağlantı aranmaksızın düzenleyici yetkinin kullanılabilmesi için savaş suçları, insanlığa karşı suçlar, soykırım ya da işkence gibi bazı fiillerin varlığı yeterli kabul edilmektedir<sup>117</sup>. Bahse konu fiiller gerçekleştirilmişse, artık herhangi bir devlet evrensellik ilkesine dayanarak söz konusu fiiller üzerinde düzenleyici yetkisini kullanabilmektedir.

#### 2. Uygulama Yetkisinin Sınır Ötesi Kullanımı

Uygulama yetkisi, yukarıda da açıklandığı üzere bir devletin hukuk kurallarına uyulmasını sağlamak amacıyla güç kullanma imkânı olarak tanımlanmaktadır. Uygulama yetkisi, devletlerin egemenlik haklarını kullanmalarının sonuçlarının en somut şekilde görüldüğü yetki tipidir. Çünkü burada devlet, bir kişiyi hapsedme, bir mala el koyma ya da para cezasını tahsil etme gibi günlük hayata doğrudan etkisi olan işlemler yapmaktadır.

Devletlerin uygulama yetkilerini sınır ötesi olarak kullanmalarına ilişkin şartlar, **Lotus** kararı kapsamında belirlenmiş durumdadır<sup>118</sup>. Söz konusu karara göre bir devletin, uygulama yetkisini kendi ülkesi dışında kullanması yasaklanmıştır. Dolayısıyla bir kişinin hapsedilmesi için bu kişinin ya gönüllü olarak ya da suçluların iadesi prosedürleri neticesinde ilgili devlet ülkesinde bulunması gerekmektedir. Yine bir para

<sup>116</sup> İlgili kanun için bkz. “Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996”, (1996), (Çevrimiçi) <https://www.congress.gov/bill/104th-congress/house-bill/927/text>, 29.03.2021.

<sup>117</sup> Shaw, **International Law**, s. 500; Dixon, McCorquodale, Williams, **Cases & Materials on International Law**, s. 298; Henriksen, **International Law**, s. 92; Brownlie, **Principles of Public International Law**, s. 305; Ünal, **Uluslararası Hukuk**, s. 241; Caşın, **Modern Uluslararası Hukukun Temel Esasları**, s. 378; Glahn, Taulbee, **Law Among Nations An Introduction to Public International Law**, s. 309; Focarelli, **International Law**, s. 291; Ryngaert, **Jurisdiction in International Law**, s. 120; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 60; Gavouneli, **Functional Jurisdiction in the Law of the Sea**, s. 19.

<sup>118</sup> Bkz. Yuk. s. 28 vd.

cezasının tahsilini yapmak isteyen devletin haczedip satabileceği mal varlıkları, sadece kendi ülkesi içerisinde bulunan mal varlıklarıdır.

**Lotus** kararı aynı zamanda uygulama yetkisinin sınır ötesi olarak kullanımı yasağının bir istisnasını da öngörmüştür. Buna göre uluslararası hukukun bir devletin uygulama yetkisini başka bir devletin ülkesinde kullanmaya bir teamül ya da milletlerarası sözleşme ile izin vermesi halinde, bu devlet uygulama yetkisini diğer devletin ülkesi içerisinde de kullanabilmektedir<sup>119</sup>. Söz konusu durumlara örnek olarak Osmanlı İmparatorluğu’nun yabancılara verdiği adli kapitülasyonlardan bazılarını vermek mümkündür. Örneğin Osmanlı ülkesi içerisinde kurulu bulunan konsolosluk mahkemelerinin ya da Osmanlı mahkemelerinin, kapitülasyonlara taraf olan devlet vatandaşları hakkında verdikleri hapis cezalarının uygulanması amacıyla konsoloslukların yakalama yetkisine sahip olması ve bu suçlularının cezalarını kendi devletlerinin hapishanelerinde çekmesi gibi kurallar<sup>120</sup>, bir devletin başka bir devlet ülkesinde uygulama yetkisini kullanmasına örnek olarak gösterilebilecektir. Bir devletin kendi ülkesi içerisinde başka bir devletin uygulama yetkisi kullanmasına izin vermesi egemenlik haklarının ciddi şekilde sarsılması anlamına gelmektedir.

Son olarak belirtmek gerekir ki yabancı mahkeme kararlarının tenfizi, uygulama yetkisinin sınır ötesi kullanımı anlamına gelmemektedir<sup>121</sup>. Zira burada uygulama yetkisi yine kararı tenfiz eden ev sahibi devlet tarafından kullanılmaktadır. Benzer şekilde adli yardımlaşma ve suçluların iadesi gibi konulardaki sözleşmeler de uygulama yetkisinin sınır ötesi kullanımı değildir. Bu gibi konular esasen devletlerin birbirleri ile uygulama yetkisi açısından iş birliği yapması anlamına gelmektedir.

---

<sup>119</sup> Henriksen, **International Law**, s. 97; Brownlie, **Principles of Public International Law**, s. 309; Focarelli, **International Law**, s. 292; Ryngaert, **Jurisdiction in International Law**, s. 61; Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 66.

<sup>120</sup> Pamir, “Kapitülasyon Kavramı ve Osmanlı Devleti’ne Etkileri”, s. 92; Joseph Henry Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, Cambridge, Harvard University Press, 1916, s. 123.

<sup>121</sup> Ryngaert, **Jurisdiction in International Law**, s. 139.

### 3. Yargılama Yetkisinin Sınır Ötesi Kullanımı

Yargılama yetkisi, bir devletin yargı organları vasıtasıyla dava görme ve bunları karara bağlama yetkisidir. Yargılama yetkisinin ülke sınırları içerisinde mevcut bulunduğu ve egemen devlet tarafından kullanılacağı şüphesizdir. Yine de belirtmek gerekir ki egemen devletin rızası bulunması halinde, bu devletin ülkesinde yabancı devletlerin yargı organları da yargılama yetkisi kullanabilmektedir. Örnek vermek gerekirse Osmanlı İmparatorluğu tarafından tanınan kapitülasyonlar nedeniyle yabancı devletlerin konsolosları Osmanlı ülkesinde yargılama faaliyeti yapabilmıştır.

Yargılama yetkisinin ülke dışında bulunan kişiler veya eşyalar ya da ülke dışında vuku bulan olaylar hakkında kullanılması, yargılama yetkisinin sınır ötesi kullanımı olarak kabul edilmektedir. Yargılama yetkisinin sınır ötesi olarak kullanılabilmesi için yargılamanın taraflarının ya da konusunun herhangi bir şekilde yargılama yetkisini kullanmak isteyen devletle bağlantılı olması gerekmektedir<sup>122</sup> (evrensellik ilkesi kapsamında kullanılan yargılama yetkisi hariç). Bu bağlantı ise olayın ülkede gerçekleşmiş olması ya da tarafların vatandaş olması gibi unsurlarla sağlanmaktadır.

Yargılama yetkisinin hukuk mahkemeleri tarafından sınır ötesi olarak kullanılması (yani yurtdışında bulunan eşya ya da kişiler veya yurtdışında gerçekleşmiş bir olayla ilişkin olarak yabancılık unsuru olan uyuşmazlıklar hakkında kullanılması), milletlerarası yetki olarak ifade edilmektedir<sup>123</sup>. Hukuk mahkemelerinin milletlerarası yetkisi Kıta Avrupası ülkelerinde vatandaşlık, yerleşim yeri, mutlak mesken, fiilin gerçekleştiği yer ya da ülkede mal varlığı bulunması gibi kriterlere göre belirlenmektedir<sup>124</sup>. Buna karşılık Anglosakson hukuk sisteminin parçası olan ABD’de ise kişinin ABD ile asgari düzeyde bağlantısının olması yeterli kabul edilmektedir<sup>125</sup>.

---

<sup>122</sup> Ryngaert, **a.g.e.**, s. 10.

<sup>123</sup> Bkz. Yuk. s. 23 vd.

<sup>124</sup> Ryngaert, **Jurisdiction in International Law**, s. 14; Akehurst, “Jurisdiction in International Law”, s. 172.

<sup>125</sup> Ryngaert, **Jurisdiction in International Law**, s. 12; Akehurst, “Jurisdiction in International Law”, s. 170.



Yargılama yetkisinin ceza mahkemelerince ülke içerisinde kullanılabileceği konusunda herhangi bir şüphe bulunmamaktadır<sup>126</sup>. Mülkilik ilkesi çerçevesinde, bir ülkede başlayıp diğer ülkede biten ya da tam tersi durumda olan suçlar için de yargılama yetkisi kullanılabilir. Kişilik ilkesi de ceza mahkemelerinin milletlerarası yetkisinin belirlenmesinde göz önüne alınan unsurlardan birisidir. Bir vatandaşın yurtdışında işlediği suçlar (aktif kişilik ilkesi) ya da bir yabancı tarafından vatandaşlara karşı işlenen suçlar (pasif kişilik ilkesi) hakkında bu vatandaşın bağlı bulunduğu devletin mahkemeleri yargılama yetkisi öne sürebilmektedir. Ceza mahkemelerinin yargılama yetkisi kullanabilmek için dayandığı iki farklı husus daha bulunmaktadır. Bunlardan ilki bir devletin kendi güvenliğine karşı olarak yurtdışında bir yabancı tarafından işlenen suçlar üzerinde yargılama yetkisi kurması anlamına gelen koruma ilkesidir. İkinci husus ise belirli suçlar hakkında kullanılan evrensellik ilkesidir.

Yargılama yetkisi kullanma konusunda çok çeşitli kriterler olması, birden çok devletin yargı yetkisi iddiasında bulunmasına sebep olabilmektedir. Ancak uygulamada kişinin bulunduğu ülkedeki devletin yargılama yapması veya kişiyi suçluların iadesi süreçleri kapsamında diğer ilgili devlete iade etmesi ile sonuçlanmaktadır<sup>127</sup>.

Üzerinde durulması gereken bir diğer nokta ise düzenleme yetkisinin sınır ötesi kullanımına ilişkin kriterler ile yargılama yetkisinin sınır ötesi kullanımına ilişkin kriterlerin neredeyse tamamen aynı olmasıdır. Bu durumun sebebi, yürürlüğe sokulan bir hukuk kuralının aynı zamanda bir mahkeme tarafından da yargılama faaliyetine konu edilebilmesi gereksinimidir<sup>128</sup>.

---

<sup>126</sup> Akehurst, "Jurisdiction in International Law", s. 152.

<sup>127</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 54. Konunun ayrıca milletlerarası sözleşmelerle de çözümlenmesi mümkündür. Örnek olarak bkz. "Convention No. 185 of the Council of Europe on Cybercrime (Budapest Convention)", 23.11.2001, (Çevrimiçi) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, 26.08.2020 m. 22/5.

<sup>128</sup> Schmitt, Vihul, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, s. 53.

## **E. Devletlerin Uluslararası Yetkisini Sınır Ötesi Uygulama Kapsamına Sahip Olarak Kullanmasının Yarattığı Sorunlar ve Çözüm Yöntemleri**

### **1. Sorunlar**

Düzenleme, uygulama ve yargılama yetkilerinin devletlerce sınır ötesi olarak kullanılabildiği durumlar yukarıda açıklanmıştır. Uygulama yetkisi ile yargılama yetkisi açısından sınır ötesi yetki kullanımı noktasında pratikte ciddi bir sorun olmadığı gözlenmemektedir. Zira bu tür yetkilerin kullanımı, düzenleme yetkisinin aksine, fiilen ülke dışında güç kullanılmasını gerektirmektedir. Ülke içinde bulunan mahkemelerin sınır ötesi yetki kullanarak verdiği kararların da ülke dışında uygulanabilmesi, kararın uygulanacağı ülkenin takdirine bağlı olduğu için bu konuda da önemli bir sorun bulunmamaktadır. Hatta yabancı mahkeme kararlarının tanınması ve tenfizi konuları milletlerarası sözleşmelerle de açıklığa kavuşturulmuş durumdadır.

Öte yandan düzenleme yetkisinin sınır ötesi kullanımı ise önemli sorunlara yol açabilme potansiyeline sahiptir<sup>129</sup>. Zira düzenleme yetkisinin kullanımı önünde, güç kullanımı gereksinimi gibi herhangi bir sınır bulunmamaktadır. Devletler iç hukuk kurallarını yürürlüğe koymak suretiyle kolaylıkla sınır ötesi düzenleme yetkisi kullanabilmektedir. Her ne kadar müsamahakâr ilkeler çerçevesinde yetki kullanacak devlet ile yetkiye konu olgunun bir bağlantısı olması aransa da (evrensellik ilkesi hariç) bu durum birden fazla devletin aynı olgu üzerinde yetki iddiasında bulunmasını engellememektedir. Nitekim müsamahakâr ilkelerin kullanıldığı hemen her durumda mülkilik ilkesine dayanarak yetki iddiasında bulunan ev sahibi bir devlet de olacaktır. Bunun ötesinde müsamahakâr ilkelere dayanarak yetki iddiasında bulunması mümkün olan başka devletler de söz konusu olabilecektir. Dolayısıyla aynı olgu üzerinde birden fazla devletin yetki kullanması halinde devletler arasında yetki kullanımına ilişkin uyuşmazlıklar meydana gelmektedir. Örneğin **Lotus** kararı, böyle bir uyuşmazlığın ürünüdür.

---

<sup>129</sup> Ryngaert, **Jurisdiction in International Law**, s. 143.

Birden çok devletin aynı olgu üzerinde düzenleyici yetki iddiasında bulunmasının yarattığı sorunlara ilişkin birçok çözüm yöntemi önerilmiştir. Aşağıdaki başlıklar altında öncelikle doktrinde konuya ilişkin olarak öne sürülmüş görüşler incelenecektir.

## 2. Çözüm Yöntemleri

### a. Çözüm Yöntemi Olarak Öne Sürülen Çeşitli Görüşler

Birden fazla devletin aynı olgu üzerinde düzenleme yetkisi iddiasında bulunmasının yarattığı uyuşmazlıkların çözümüne yönelik ilk öneri, mülkilik ilkesine dayanarak yetki iddiasında bulunan devlete öncelik verilmesidir<sup>130</sup>. Ancak uluslararası hukukun yetkiye ilişkin kuralları, mülkilik ile müsamahakâr ilkeler arasında herhangi bir hiyerarşik ilişki kurmamakta ve bunları egemenlikten kaynaklanan eşit dereceli yetki kullanımları olarak görmektedir<sup>131</sup>. Bu nedenle öne sürülen çözüm yönteminin kabul edilmesi mümkün olmamıştır.

Önerilen ikinci çözüm yöntemi ise birden fazla yetki iddiasında bulunulabilecek durumların milletlerarası sözleşmeler vasıtasıyla çözüme kavuşturulmasıdır<sup>132</sup>. Bu öneri özellikle **Lotus** kararında da kendisine yer bulmuştur<sup>133</sup>. Devlet uygulamalarında ise özellikle vergi hukuku olmak üzere çeşitli alanlarda milletlerarası sözleşmeler vasıtasıyla yetki kullanımı konusunun çözüme kavuşturulduğu bilinmektedir<sup>134</sup>. Ancak rekabet, finans ya da ceza hukuku gibi alanlarda bu tür sözleşmelerin hala büyük oranda eksik olduğu görülmektedir<sup>135</sup>. Ayrıca birden fazla devletin aynı anda yetki iddiasında bulunabileceği tüm durumları önceden öngörmek mümkün olmadığı için sadece milletlerarası sözleşmelerle bu tür uyuşmazlıkları gidermek mümkün değildir<sup>136</sup>.

---

<sup>130</sup> Mann, "The Doctrine of Jurisdiction in International Law", s. 90; Akehurst, "Jurisdiction in International Law", s. 208.

<sup>131</sup> Ryngaert, **Jurisdiction in International Law**, s. 143; Akehurst, "Jurisdiction in International Law", s. 168.

<sup>132</sup> Ryngaert, **Jurisdiction in International Law**, s. 145.

<sup>133</sup> Lotus Case, France v. Turkey paragraf 47.

<sup>134</sup> Ryngaert, **Jurisdiction in International Law**, s. 146. Örnek olarak bkz. "Convention No. 185 of the Council of Europe on Cybercrime (Budapest Convention)" m. 22/5.

<sup>135</sup> Ryngaert, **Jurisdiction in International Law**, s. 146.

<sup>136</sup> Ryngaert, **a.g.e.**, s. 145.

ABD iç hukukunda kullanılmakta olan bir diğer çözüm yöntemi ise sınır ötesi yetki kapsamı bulunmadığına dair bir karinenin (**presumption against extraterritoriality**) kabul edilmesidir. ABD Yüksek Mahkemesi içtihatları ile şekillenmiş olan bu karineye göre bir kanunun ülke dışında uygulanabilmesi için ABD Kongresi'nin bu konudaki iradesini açıkça ifade etmiş olması aranmaktadır<sup>137</sup>. Böylelikle düzenleme yetkisinin sınır ötesi kullanıldığı durumlar azaltılarak bahse konu uyuşmazlıkların çıkma ihtimali düşürülmektedir. Ancak bu doktrin sınır ötesi kapsamda yetki kullanımının tamamen ortadan kaldırıldığı anlamına gelmemektedir ve ayrıca devletler arasında çıkabilecek olası uyuşmazlıkların çözümüne yönelik bir kural da getirmemektedir.

#### **b. Uluslararası Düzenleme Yetkisinin Makul Kullanımı**

Milletlerarası nezaket (**comitas gentium**) bir devletin kendi ülkesi içerisinde diğer bir devletin yasama, yürütme ya da yargı faaliyetlerinden doğan işlemlerine, uluslararası bir görev ya da kendi vatandaşları ya da koruması altında olan kişiler için uygun sonuç doğurmak amacıyla etki tanınması olarak tanımlanmıştır<sup>138</sup>. Milletlerarası nezaket kavramı, diplomaside ve uluslararası hukukta kullanılmaktadır. Ancak milletlerarası nezaketin bağlayıcı bir uluslararası hukuk kuralı niteliği taşımamakta olduğu kabul edilmektedir<sup>139</sup>.

Milletlerarası nezaket ilk olarak Hollanda'da **Ulrich Huber** tarafından milletlerarası özel hukuk kapsamında yabancı ülke hukuklarının ev sahibi ülke içerisinde uygulanmasının gerekçesini açıklamak amacıyla ortaya atılmıştır<sup>140</sup>. Günümüze kadar geçen sürede ise bu görüş ABD iç hukukunda kendisine geniş bir yer bulmuş ve mahkemelerce yabancı hukukun uygulanması, yabancı mahkeme kararlarının tanınması ve tenfizi, yabancı devletlerin yargı bağımsızlığı, adli istinabe ile düzenleme

---

<sup>137</sup> Ryngaert, **a.g.e.**, s. 69; Hartford Fire Insurance Co. et al. v. California et al., 91-111, (U.S. Supreme Court 28 Haziran 1993); EEOC v. Arabian American Oil Co., 89-1838, 89-1845, (U.S. Supreme Court 1991).

<sup>138</sup> Ryngaert, **Jurisdiction in International Law**, s. 147; Donald Earl Childress III, "Comity as Conflict: Resituating International Comity as Conflict of Laws", **U.C. Davis Law Review**, C. 44, S. 1, 2010, s. 14.

<sup>139</sup> Ryngaert, **Jurisdiction in International Law**, s. 147; William S. Dodge, "International Comity In American Law", **Columbia Law Review**, C. 115, S. 8, 2015, s. 2124.

<sup>140</sup> Bkz. Aş. s. 179 vd.

yetkisinin sınır ötesi kullanımının sınırları gibi konulara ilişkin kararlarda dayanak olarak kullanılmıştır<sup>141</sup>. Buna karşılık Kıta Avrupası Hukuk Sistemine dahil olan ülke mahkemelerinde ise milletlerarası nezaket doktrinine neredeyse hiç başvurulmadığı görülmektedir<sup>142</sup>.

Milletlerarası nezaketin ilk ortaya çıkış amacı, milletlerarası özel hukuk çerçevesinde bir devletin başka bir devletin hukukunu kendi ülkesinde uygulamasının dayanağını oluşturmaktır. Ancak modern milletlerarası nezaket yaklaşımı, devletlerin uluslararası yetkilerini; diğer devletlerin egemenlik haklarını ihlal etmeden kullanmaları gerektiğini ifade etmektedir<sup>143</sup>. İşte bu yaklaşım, uluslararası düzenleme yetkisinin makul kullanımı kuralının dayanağını teşkil etmektedir<sup>144</sup>.

Müsamahakâr ilkelerin her birinin (evrensellik hariç) yetki iddiasında bulunulacak olgu ile bir bağlantı aradığı görülmektedir. Ancak bu bağlantıların tek başına, yetki iddiasında bulunan çok sayıda devlet arasından birinin seçilmesine imkân vermediği açıktır. İşte bu sebeple yetki iddiaları arasında da bir inceleme yapılarak olgu ile en sıkı ilişkisi bulunan devletin tespit edilmesi yaklaşımına uluslararası düzenleme yetkisinin makul kullanımı kuralı adı verilmektedir<sup>145</sup>. Netice itibarıyla bu kurala göre bir devletin uluslararası düzenleme yetkisini bir olgu üzerinde kullanabilmesi için hem müsamahakâr ilkelerden birine dayanması hem de ilgili olgu ile en sıkı ilişkiye sahip olduğunu göstermesi gerekecektir.

---

<sup>141</sup> Ryngaert, **Jurisdiction in International Law**, s. 148; Akehurst, "Jurisdiction in International Law", s. 218.

<sup>142</sup> Ryngaert, **Jurisdiction in International Law**, s. 148; Akehurst, "Jurisdiction in International Law", s. 219.

<sup>143</sup> Ryngaert, **Jurisdiction in International Law**, s. 148; Akehurst, "Jurisdiction in International Law", s. 182; Dodge, "International Comity In American Law", s. 2079.

<sup>144</sup> Ryngaert, **Jurisdiction in International Law**, s. 147; **Restatement of the Law Third, the Foreign Relations Law of the United States**, C. 1, 1. bs, Washington D. C., The American Law Institute, 1986, s. 249.

<sup>145</sup> Ryngaert, **Jurisdiction in International Law**, s. 145; Dan E. Stigall, "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law", **Hastings International and Comparative Law Review**, C. 35, S. 2, 2012, s. 337.

ABD hukuk doktrininde uluslararası yetkinin makul kullanımı kuralı daha detaylı bir şekilde açıklanmıştır<sup>146</sup>. Buna göre uluslararası düzenleme yetkisinin makul kullanıldığının kabul edilebilmesi için aşağıdaki kriterlerin birlikte değerlendirilerek hayat ilişkisiyle en sıkı ilişkili devletin tespit edilmesi ve buna göre bir sonuca varılması gerekmektedir<sup>147</sup>: (i) fiilin düzenleyici yetki kullanacak devletin ülkesi ile bağlantısı (kısmen ya da tamamen ülke içinde gerçekleşme ya da ülke içinde etki doğurma gibi); (ii) vatandaşlık, yerleşim yeri ya da ekonomik aktivite gibi düzenleme yetkisini kullanan devlet ile düzenlemeye konu ya da düzenleme ile korunan kişi arasındaki bağlantılar; (iii) düzenlemeye konu olgunun özellikleri ile düzenleyen devlet için önemi, diğer devletlerin aynı olguya ilişkin düzenlemeleri ve bu düzenlemelerin kabul edilebilirliği; (iv) düzenleme neticesinde ortaya çıkması makul olan beklentilerin korunma ya da zarar görme derecesi; (v) düzenlemenin uluslararası siyasi, hukuki ve ekonomik sistem açısından önemi; (vi) düzenlemenin uluslararası sistemin teamülleri ile uyumu; (vii) diğer devletlerin aynı olgu üzerinde düzenleme yetkisi kullanmasına yönelik menfaatleri; (viii) diğer devletlerin düzenlemeleri ile çelişen durumlar ortaya çıkması olasılığı.

Yukarıda belirtilen kriterlere<sup>148</sup> göre değerlendirme yapıldığında (bu değerlendirmeye milletlerarası nezaket analizi adı verilmektedir) dahi, birden fazla devletin düzenleme yetkisini aynı olgu üzerinde kullanmasının makul olarak kabul edilmesi ihtimal dahilindedir<sup>149</sup>. Böyle durumları çözmek amacıyla doktrinde önerilen yöntem, yetki iddiasında bulunan ve konuyu değerlendirmekte olan devletin tüm faktörleri değerlendirerek hangi devletin menfaatinin açıkça daha büyük olduğunu tespit etmesi

---

<sup>146</sup> ABD hukukunun milletlerarası nezaket doktrininin yaygın kullanılması, kanunların sınır ötesi uygulama kapsamının bulunmadığına dair bir karinenin kabul edilmesi ve uluslararası yetkinin makul kullanımı kuralının getirilmesi gibi doktrinler geliştirmesi bir tesadüf değildir. Tarih boyunca olduğu gibi günümüzde de farklı devletlerle en çok ilişki kurulan bölgelerde bu tür kuralların geliştirildiği gözlemlenmektedir. Nitekim hem ABD'nin eyalet yapısı hem de dünyanın her yeri ile yoğun bir şekilde diplomatik ve ekonomik ilişkiler kurmuş olması, ABD hukukunun bahse konu hususlar üzerinde çalışma yapabilmesine ortam hazırlamıştır.

<sup>147</sup> **Restatement Third**, C. 1, s. 244.

<sup>148</sup> Söz konusu kriterlere göre analiz yapılması yaklaşımı Fourth Restatement ile birlikte terk edilmiştir. Buna karşılık en sıkı ilişki kuralının mevcudiyeti devam etmektedir (Bkz. William S. Dodge, "Jurisdictional Reasonableness under Customary International Law: The Approach of the Restatement (Fourth) of United States Foreign Relations Law", t.y., s. 6. Öte yandan sonraki bölümlerde inceleneceği üzere ABD kanunları içerisinde söz konusu kriterlerinin kullanılmaya devam ettiği görülmektedir.

<sup>149</sup> Ryngaert, **Jurisdiction in International Law**, s. 166; **Restatement Third**, C. 1, s. 246.

şeklindedir. Eğer diğer devletin daha büyük menfaati mevcutsa, o devletin yetki kullanması için değerlendirme yapan devletin kendi yetkisinden feragat etmesi beklenmektedir<sup>150</sup>. Önemle belirtmek gerekir ki bu çözüm yöntemi, sadece iki devletin uluslararası düzenleme yetkisinden doğan hukuk kuralları birbiriyle çelişiyorsa (yani birinin yap dediğini diğeri yapma demekteyse) kullanılabilecektir<sup>151</sup>. Eğer iki devletin öngördüğü hukuk kuralları farklı ancak birbiriyle çelişmeyen yükümlülükler getiriyorsa, bu durumda anılan çözüm yönteminin kullanılması mümkün değildir. İlgili kişiler her iki hukuk kuralına da uygun hareket etmek zorunda olacaklardır. Bu yaklaşıma bağlı olarak menfaat tespiti yönteminin, yetki uyumsuzluklarını değil; farklı devletlerin hukuk kurallarının çelişkili hükümler getirdiği durumları çözümlediği sonucuna varılmaktadır.

ABD hukuk doktrininde kabul edilen uluslararası yetkinin makul kullanımı kuralını tüm ABD yasama, yürütme ve yargı organlarının göz önüne alması gerekmektedir<sup>152</sup>. Uluslararası yetkinin makul kullanımı kuralı, herhangi bir hukuk alanı ile de sınırlı değildir<sup>153</sup>. Yani özel hukuk ya da kamu hukuku fark etmeksizin her türlü hukuki düzenleme ve yargı kararında dikkate alınmalıdır.

Uluslararası düzenleme yetkisinin makul kullanımı kuralının ABD iç hukukundaki görünümü, ABD doktrininin öne sürdüğü görüşe göre aynı zamanda uluslararası hukukta da kabul görmektedir<sup>154</sup>. Ancak uluslararası hukukun fiili durumuna bakıldığında durumun böyle olmadığı anlaşılmaktadır<sup>155</sup>. Zira ne doktrinde ne devlet uygulamalarında ABD doktrininin öne sürdüğü görüşü destekleyen bir unsur bulunmaktadır. Buna ek olarak Kıta Avrupası hukukunda makul yetki kullanımı ve

---

<sup>150</sup> Ryngaert, **Jurisdiction in International Law**, s. 166; **Restatement Third**, C. 1, s. 247.

<sup>151</sup> Ryngaert, **Jurisdiction in International Law**, s. 166; **Restatement Third**, C. 1, s. 247; Andreas F. Lowenfeld, "Harold Maier, Comity and the Foreign Relations Restatement", **Vanderbilt Journal of Transnational Law**, C. 36, S. 5, 2006, s. 1424; Karl M. Meessen, "Conflict of Jurisdiction under the New Restatement", **Law and Contemporary Problems**, C. 50, S. 3, 1987, s. 67; Stigall, "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law", s. 344.

<sup>152</sup> Ryngaert, **Jurisdiction in International Law**, s. 165; **Restatement Third**, C. 1, s. 248.

<sup>153</sup> Ryngaert, **Jurisdiction in International Law**, s. 165.

<sup>154</sup> Ryngaert, **a.g.e.**, s. 167; **Restatement Third**, C. 1, s. 245.

<sup>155</sup> Ryngaert, **Jurisdiction in International Law**, s. 170; Stigall, "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law", s. 338; Meessen, "Conflict of Jurisdiction under the New Restatement", s. 59.

menfaat dengeleme yaklaşımları da esasen reddedilmektedir. Zira Kıta Avrupası hukukundaki yaklaşımlara göre yargı organı olan mahkemeler, yürütme organının görev alanında olan diplomasi ve uluslararası politika gibi alanlara müdahale etmemelidir<sup>156</sup>.

Milletlerarası nezakete dayanan uluslararası düzenleme yetkisinin makul kullanımı yaklaşımının da uluslararası hukukun bağlayıcı bir kuralı olmadığı görülmektedir<sup>157</sup>. Zira bu yönde devletlerin herhangi bir uygulaması olmadığı gibi böyle bir kural bulunduğu dair bir inanç (**opinio juris**) da mevcut değildir. Zaten kuralın en başta uluslararası hukuka değil milletlerarası nezaket kavramına dayanması da kuralın hukuki bağlayıcılığı olmadığı göstermektedir.

#### **F. Dijital Ortam Üzerinde Devletlerin Uluslararası Yetkisi**

Dijital ortam üzerinde uluslararası yetki kullanılabilmesi için dijital ortama özel yeni kurallar benimsenmesine gerek olmadığı, hâkim görüş olarak kabul edilmektedir<sup>158</sup>. Bu kapsamda devletler, dijital ortam harici konularda yaptıkları şekilde dijital ortam üzerinde de uluslararası yetki kullanabileceklerdir.

Mülkilik ilkesine dayalı uluslararası yetki kullanımı çerçevesinde devletlerin kendi ülkeleri içerisinde dijital faaliyetlerde bulunan kişiler ve dijital ortam altyapıları üzerinde egemenlik sahibi oldukları açıktır. Ayrıca dijital faaliyetlerin ülke içerisinde başlaması ya da tamamlanması veya etki doğurması halinde de o ülkede bulunan devletin mülkilik ilkesi çerçevesinde uluslararası yetki kullanabilmesi mümkündür.

---

<sup>156</sup> Bu görüşün temeli Fransız devrimi ile ortaya çıkan her devlet organının kendi görev alanı dışına acıkmaması prensibine dayanmaktadır (Bkz. Ryngaert, **Jurisdiction in International Law**, s. 173). Öte yandan yargı organlarının uluslararası yetkinin makul kullanımına ilişkin kriterlerin değerlendirilmesi sırasında yürütme organının yerine geçtiği yönünde eleştiriler ABD hukukunda da mevcuttur (Bkz. Dodge, “International Comity In American Law”, s. 2132; Kathleen Hixson, “Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States”, **Fordham International Law Journal**, C. 12, S. 1, 1988, s. 152).

<sup>157</sup> Ryngaert, **Jurisdiction in International Law**, s. 180.

<sup>158</sup> Ryngaert, **a.g.e.**, s. 79.



Dijital ortama ilişkin hususlar hakkında sınır ötesi yetki kullanımının da mümkün olduğu kabul edilmektedir. Burada özellikle düzenleme yetkisi açısından müsamahakâr ilkelerin uygulama alanı bulmaya devam ettiğini belirtmekte fayda görülmektedir.

### **G. Değerlendirmeler**

Uluslararası yetki konusunda yapılan incelemeler neticesinde varılan ilk sonuç, yetki kullanımı kaynaklı olarak devletler arasında uyuşmazlık çıkarma potansiyeli en yüksek yetki tipinin düzenleme yetkisi olduğudur. Uygulama ve yargılama yetkilerinin sınır ötesi kapsamda kullanılmaları ise fiili güç gerektirdiği için fiilen mümkün olamamaktadır. Ayrıca bu konularda daha net hukuki kuralların mevcut olması da devletler arasında uyuşmazlık çıkma riskini azaltmaktadır.

Düzenleme yetkisinin sınır ötesi kullanımı ise devletler açısından son derece kolaydır. Bu nedenle de konu hakkında devletler arasında uyuşmazlık çıkma olasılığı da kanaatimizce diğer yetki tiplerine göre daha yüksektir. Uluslararası hukuk çalışmaları kapsamında düzenleme yetkisinin sınır ötesi kullanımı ile bu durumun yarattığı sorunların çözümü konularında birçok görüş ortaya atılmıştır. Ancak bu görüşler arasında dahi uluslararası hukuk kuralı olarak kabul edilen bir çözüm bulunmamaktadır.

Uluslararası hukuk çalışmaları kapsamında aranan çözümler, doğal olarak devletler arasındaki sorunları çözmeyi hedeflemektedir. Ancak sınır ötesi düzenleme yetkisinin kullanımı aynı zamanda kişileri farklı hukuk kurallarına uyma yükümlülüğü altında bırakmaktadır. Kişiler, kimi durumlarda birbirinden farklı hukuki yükümlülüklerle katlanmakta kimi durumlarda ise çelişen hukuki yükümlülüklerden birine uyarak diğer devletin öngördüğü hukuki yaptırımlara katlanmak durumunda kalmaktadırlar. Özellikle ekonomik bağlantıların, internetin ve iletişimin bu kadar geliştiği günümüzde düzenleyici yetkinin sınır ötesi kullanımının bireyler üzerindeki etkileri kanaatimizce artmaya devam edecektir.

Kişilerin günlük ve ticari hayatlarında birden fazla devletin kuralları arasında kalmaları sorununa örnek teşkil edecek düzenlemeler, çalışmamızın sonraki bölümlerinde dijital ortam ile sınırlı olarak verilecektir. Farazi bir örnek olarak bir Türk bankasının Türk hukukuna göre bankacılık verilerini yurt içinde saklaması zorunluyken, sınır ötesi uygulama kapsamı olan bir yabancı hukuk kuralının verilerin yurtdışındaki bir kişiye teslimini zorunlu kılması halinde; bankanın hangi hukuk kuralına uyması gerektiği sorunu verilebilir. Şüphesiz ki devletler arasındaki ilişkileri konu alan uluslararası hukuk çalışmalarının kişiler nezdinde doğan bu tür bir soruna çare aramasını beklemek doğru değildir. O halde sorunun iç hukuk alanı içerisinde çözümlenip çözümlenemeyeceğini değerlendirmek, kanaatimizce en doğru yaklaşım olacaktır.

#### **IV. DEVLETLERİN ULUSLARARASI YETKİSİ İLE MİLLETLERARASI ÖZEL HUKUK VE USUL HUKUKUNUN İLİŞKİSİ**

##### **A. Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Temel Bilgiler**

##### **1. Milletlerarası Özel Hukuk ve Usul Hukuku Alanı Kapsamına Giren Konular**

Milletlerarası özel hukuk (eski adıyla devletler hususi hukuku) ya da diğer adıyla kanunlar ihtilafı yabancılık unsuru taşıyan uyumsuzluklarda, mahkemelerin hangi ülkenin hukuk sisteminin kurallarını uygulaması gerektiğini tespit etmeyi amaçlamaktadır<sup>159</sup>. Örnek vermek gerekirse farklı vatandaşlıklara sahip evli bir çiftin

---

<sup>159</sup> Erdoğan Göger, **Devletler Hususi Hukuku**, 4. bs, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1977, s. 1; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 5; Nomer, **Devletler Hususi Hukuku**, s. 4; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 3; Doğan, **Milletlerarası Özel Hukuk**, s. 5; Akıncı, **Milletlerarası Özel Hukuk**, s. 4; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 2; Ugljesa Grusic vd., **Cheshire, North & Fawcett Private International Law**, ed. Paul Torremans, 15. bs, Oxford, Oxford University Press, 2017, s. 3; Geert van Calster, **European Private International Law**, 2. bs, Oxford UK, Hart Publishing and Bloomsbury Publishing, 2016, s. 1; Lea Brilmayer, Jack Goldsmith, Erin O'Hara O'Connor, **Conflict of Laws Cases and Materials**, 7. bs, New York, Wolters Kluwer Law & Business, 2015, s. 29; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 1; Elliott E. Cheatham, "Stone on Conflict of Laws", **Columbia Law Review**, C. 46, 1946, s. 719.

boşanmasında mahkemenin hangi eşin vatandaşlık bağı olan ülkenin hukukunu boşanma işlemine uygulaması gerektiği sorusu, milletlerarası özel hukukun cevabını aradığı bir sorudur.

Milletlerarası özel hukuk esasen iç hukuk kurallarından oluşmaktadır<sup>160</sup>. Yani her devlet kendi egemenliğine ve dolayısıyla uluslararası yetkisine dayanarak yabancılık unsuru taşıyan uyuşmazlıklara uygulayacağı hukuku tespit etmektedir. Bu durum da milletlerarası özel hukukun ya da kanunlar ihtilafı kurallarının hukuk sistemleri arasındaki gerçek bir çatışmayı çözmeyi hedeflemediğini göstermektedir<sup>161</sup>. Yani farklı vatandaşlığa sahip eşlerin boşanmasında, her eşin tabi olduğu milli hukuklar; kendilerinin uygulanması için yarışmamaktadır veya ilgili devletler kendi hukuklarının ülkeleri sınırları dışında uygulanması için irade göstermemektedirler. Bunun yerine her devlet kendi iç hukuku vasıtasıyla olayla en sıkı ilişkili hukukun uygulanabilmesine, uyuşmazlık taraflarının ilgili olay veya ilişkiye ait makul ve haklı beklentilerini tatmin etmek amacıyla izin vermektedir<sup>162</sup>.

Milletlerarası özel hukukun diğer bir özelliği de sadece özel hukuka ilişkin uyuşmazlıklarda, özel hukuk mahkemelerinin önüne gelen uyuşmazlıklara hangi hukukun uygulanacağını tespit etmesidir. Kamu düzeni ya da doğrudan uygulanan kurallar gibi kurumlar vasıtasıyla kamu hukuku kurallarına etki tanınmaktaysa da esas odağının mahkemeler nezdinde görülmekte olan özel hukuk uyuşmazlıkları olduğu açıktır.

---

<sup>160</sup> Göger, **Devletler Hususi Hukuku**, s. 3; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 14; Nomer, **Devletler Hususi Hukuku**, s. 10; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 3; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 2; Doğan, **Milletlerarası Özel Hukuk**, s. 10; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 9; Calster, **European Private International Law**, s. 2; Guangjian Tu, **Private International Law in China**, Singapore, Springer International Publishing, 2016, s. 34.

<sup>161</sup> Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 16; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 14.

<sup>162</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 33; Nomer, **Devletler Hususi Hukuku**, s. 14; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 29; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 27; Doğan, **Milletlerarası Özel Hukuk**, s. 207; Akıncı, **Milletlerarası Özel Hukuk**, s. 11; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 37; Brilmayer, Goldsmith, O'Connor, **Conflict of Laws Cases and Materials**, s. 259; Calster, **European Private International Law**, s. 6; Tu, **Private International Law in China**, s. 39.

Milletlerarası usul hukuku ise yabancılık unsuru içeren uyuşmazlıklarda mahkemelerin yetkisi, tebligat, teminat, tahkim usulleri ile yabancı mahkeme kararlarının tanınması ve tenfizi gibi konularla ilgilenmektedir. Milletlerarası usul hukuku da kanunla düzenlendiği için esasen iç hukuk niteliği taşımaktadır.

Milletlerarası özel hukuk ve usul hukuku alanı aynı zamanda kendi alanına ilişkin milletlerarası sözleşmeleri de incelemektedir. Yine bu kapsamda yabancı yatırımlar hukuku ya da milletlerarası çevre hukuku gibi alanlar da milletlerarası özel hukuk ve usul hukuku kapsamında değerlendirilmektedir. Vatandaşlık ve yabancılar hukuku da yabancılık unsurunun tespiti açısından büyük önem arz ettiği için yine bu alan kapsamında çalışılmaktadır.

## **2. “Milletlerarası Özel Hukuk” ya da “Kanunlar İhtilafı” Terimlerinin Kullanımı**

Milletlerarası özel hukuk alanının isimlendirilmesi, doktrinde uzun yıllardan beri tartışılmakta olan bir konudur<sup>163</sup>. Bu hukuk alanı milletlerarası özel hukuk ya da kanunlar ihtilafı<sup>164</sup> gibi iki farklı terim kullanılarak adlandırılmaktadır. Ancak her iki terimin de yanıltıcı yönleri bulunmaktadır. Çünkü bu alan esasen ne hukuk sistemleri arasındaki ihtilafları gidermekte ne de milletlerarası bir nitelik taşımaktadır. Milletlerarası özel hukuk ya da kanunlar ihtilafı kuralları, bir iç hukuk kuralı niteliğinde olup yabancılık unsuru taşıyan uyuşmazlıklarda hangi ülke hukukunun uygulanması gerektiğini (ülke hukukları arasında herhangi bir çatışma mevcut değildir) tespit etmeye çalışmaktadır.

---

<sup>163</sup> Göger, **Devletler Hususi Hukuku**, s. 15; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 19; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 19; Doğan, **Milletlerarası Özel Hukuk**, s. 10; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 15; Brilmayer, Goldsmith, O'Connor, **Conflict of Laws Cases and Materials**, s. 30; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 14; Friedrich K. von Savigny, **Private International Law and the Retrospective Operation of Statutes\_ A Treatise on the Conflict of Laws, and the Limits of their Operation in Respect of Place and Time**, 2. bs, Edinburgh, T&T Clark Law Publishers, 1880, s. 51.

<sup>164</sup> “Kanunlar ihtilafı” yerine “yasaların çatışması” kavramının kullanıldığı bir çalışma için bkz. Rona Aybay, Esra Dardağan, **Yasaların Çatışması**, 2. bs, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2008, s. 4.

Milletlerarası özel hukuk alanının isimlendirilmesi konusu, çalışmamız açısından önem arz etmektedir. Zira bu çalışmanın temel konusu, devletlerin uluslararası düzenleyici yetkilerini kullanarak aynıolguyu düzenlemeleri halinde doğacak çelişkili durumların çözümlenmesidir. Bir başka deyişle çalışmamızın konusunu gerçek anlamda “kanunlar ihtilafı” oluşturmaktadır. Kanunlar ihtilafı teriminin herkesçe kabul edilen anlamı göz önüne alındığında, çalışmamızın konusunu izah etmek amacıyla bu terimin kullanılamayacağı açıktır. Bu nedenle sonraki başlıklar altında görüleceği üzere yeni bir terim üretme ihtiyacı doğmuştur.

### 3. Kanunlar İhtilafı Kurallarının Tarihi Gelişimi

Yabancı kanunların ev sahibi ülke içerisinde uygulanması, tarih boyunca çeşitli kavimlerin birbirleriyle ticari, siyasi veya ailevi ilişkilerinin artmasına bağlı olarak ortaya çıkmış bir sorundur<sup>165</sup>. Değişik insan toplulukları arasındaki ilişkiler güçlendikçe yabancı hukukun uygulanmasına yönelik yaklaşım ve çözümler de gelişmeye başlamıştır. Bu gelişim özellikle son yüzyıllarda ulaşım ve iletişim olanaklarının (ve bunlara bağlı olarak uluslararası ticaret ile yatırımların) artmasına bağlı olarak hızlanmıştır<sup>166</sup>.

Modern hukuk kurallarının temelleri, Roma devrinde gelişen hukuka dayanmaktadır. Öyle ki Romalı hukukçularının geliştirdiği kuralların önemli bir kısmı halen dahi kullanılmaktadır. Hemen her özel hukuk dalında olduğu gibi, kanunlar ihtilafı konusunda da kayda değer ilk kurallar Romalı hukukçular tarafından ortaya konmuştur<sup>167</sup>.

---

<sup>165</sup> Nomer, **Devletler Hususi Hukuku**, s. 51; Brilmayer, Goldsmith, O'Connor, **Conflict of Laws Cases and Materials**, s. 1; Tu, **Private International Law in China**, s. 2.

<sup>166</sup> Doğan, **Milletlerarası Özel Hukuk**, s. 1; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 5; William Tucker Jr. Dean, “The Conflict of Conflict of Laws”, **Stanford Law Review**, C. 3, S. 3, 1951, s. 409.

<sup>167</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 18; Söğütü, **Roma Özel Hukuku**, s. 100; Alex Mills, “The Private History of International Law”, **International and Comparative Law Quarterly**, C. 55, S. 1, 2006, s. 6; Luther L. McDougal, “‘Private’ International Law: Ius Gentium versus Choice of Law Rules or Approaches”, **The American Journal of Comparative Law**, C. 38, S. 3, 1990, s. 521.

Cumhuriyet döneminde Romalılar, kendi hukukları olan **ius civile**'yi kişiye bağlı olarak uygulama yolunu seçmişlerdir<sup>168</sup>. Buna göre her Roma vatandaşı, Roma devletinin hâkim olduğu her bölgede **ius civile**'ye tabi olmaktadır. **Ius civile**, Roma vatandaşlarına özgü olduğu kabul edilerek kutsallık addedilen ve yabancılara uygulanması mümkün görülmeeyen bir hukuk olarak yürürlükte kalmıştır<sup>169</sup>.

Güçlerinin zirvesinde oldukları dönemde Romalılar yabancı kavimlere ait hukukları tamamen görmezden gelerek dikkate almamışlardır<sup>170</sup>. Bir yabancı ile bir Romalı arasındaki ilişkiler ise Roma hukukunun bir kısmının ya da tamamının ilgili ilişkiye uygulanmasına imkân veren yetkilendirmeler yoluyla düzenlenmiştir<sup>171</sup> (örneğin Roma'da sözleşme yapma imkânı veren **commercium** yetkisi). Bu tür yetkilendirmeler ticaret ve mülkiyete ilişkin konuları kapsamakta olup kişi, aile ya da miras hukukları alanlarına yaygın bir şekilde sirayet etmemişlerdir<sup>172</sup>.

Zaman içerisinde Roma devleti, fetih yoluyla siyasi egemenlik alanını genişleterek bir imparatorluk halini almıştır. Bu durum **ius civile**'nin kişiye bağlı olarak uygulanmasını zorlaştırmaya başlamıştır<sup>173</sup>. Ek olarak ülke içerisindeki yabancı

---

<sup>168</sup> Söğütü, **Roma Özel Hukuku**, s. 96; Schwarz, **Roma Hukuku Dersleri**, C. I, s. 106; Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, s. 9; Umur, **Roma Hukuku Ders Notları**, s. 93; Tahiroğlu, Erdoğan, **Roma Hukuku Dersleri**, s. 127; Du Plessis, Borkowski, **Borkowski's Textbook on Roman Law**, s. 111; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 18; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171.

<sup>169</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 18; Söğütü, **Roma Özel Hukuku**, s. 94; Umur, **Roma Hukuku Ders Notları**, s. 93; Tahiroğlu, Erdoğan, **Roma Hukuku Dersleri**, s. 127; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171; David Johnston, **The Cambridge Companion to Roman Law**, 1. bs, New York, NY, USA, Cambridge University Press, 2015, s. 48.

<sup>170</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 18.

<sup>171</sup> Söğütü, **Roma Özel Hukuku**, s. 99; Schwarz, **Roma Hukuku Dersleri**, C. I, s. 106; Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, s. 10; Du Plessis, Borkowski, **Borkowski's Textbook on Roman Law**, s. 111; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171; Johnston, **The Cambridge Companion to Roman Law**, s. 217.

<sup>172</sup> Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171; Söğütü, **Roma Özel Hukuku**, s. 99; Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, s. 10; Du Plessis, Borkowski, **Borkowski's Textbook on Roman Law**, s. 111.

<sup>173</sup> Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171. İmparatorluk dönemi içerisinde Roma'nın gücü, Kavimler Göçü'nün yarattığı büyük nüfus hareketleri sonucunda ciddi şekilde zayıflamıştır. İmparatorluk içerisinde Roma vatandaşlığı

sayısının artması ve ticari ilişkilerin hızlı bir şekilde gelişmesi gibi sebepler de yabancıların hukuki korumadan yoksun bırakılmasını dayanılmaz hale getirmiştir.<sup>174</sup> İşte böyle bir ortamda doğan, yabancılarla kurulan hukuki ilişkilerin düzenlenmesi ihtiyacı, Roma hukukçuları tarafından **ius gentium**<sup>175</sup> adlı yeni bir hukuk sisteminin geliştirilmesine yol açmıştır. **Ius gentium**, yabancılarla Romalılar arasında kurulan hukuki ilişkileri düzenleyen hukuk kurallarından oluşmaktadır<sup>176</sup>. **Ius gentium**, **ius civile** ya da ilgili yabancıların kendi hukuku veya bir tür kanunlar ihtilafı kuralı değildir. **Ius gentium** yabancılarla olan ilişkileri düzenlemesi yönü ile günümüz kanunlar ihtilafı kurallarının yerini tutan bir çözümdür. Yabancı hukuk sistemlerini öğrenmeyi ya da uygulamayı reddeden ve aynı zamanda **ius civile**'yi yabancılara uygulamayı da kabul etmeyen Romalı hukukçular, üçüncü bir hukuk sistemi olan **ius gentium** vasıtasıyla yabancılarla kurulan hukuki ilişkileri düzenlemişlerdir. Oysa modern zamanların kanunlar ihtilafı kuralları, yabancılık unsuru bulunan uyuşmazlıklara uygulanacak hukuku tespit etmektedir. Kanunlar ihtilafı kuralları çerçevesinde uyuşmazlığın esasına uygulanmak üzere yeni bir hukuk sistemi yaratılmamaktadır. Dolayısıyla Roma hukuku ile modern hukuklar arasında yabancılık unsuru olan uyuşmazlıkların çözümüne yönelik metot açısından önemli farklılık bulunmaktadır.

---

meselesinin yarattığı sorunların ortadan kaldırılması amacıyla İmparator Antoninus Caracalla tarafından 212 yılında yayınlanan emirname ile İmparatorluk sınırları içerisindeki tüm özgür kadın ve erkekler Roma vatandaşı ilan edilerek **ius civile**'ye tabi kılınmıştır. Böylelikle tarihte ilk defa bir hukuk kurallarının ülke içerisindeki herkese uygulanmasını öngören mülkilik ilkesinin doğduğu kabul edilmektedir. Bu gelişmeye rağmen eyaletler içerisinde yaşayan toplumların yerel hukukları da bir anda yok olmayarak yerel örf ve âdet olarak uygulanmaya devam etmiştir (Bkz. Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 19; Plessis, Ando, Tuori, **The Oxford Handbook of Roman Law And Society**, s. 289).

<sup>174</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 19; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 171; Söğütü, **Roma Özel Hukuku**, s. 99; Schwarz, **Roma Hukuku Dersleri**, C. I, s. 106; Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, s. 9; Umur, **Roma Hukuku Ders Notları**, s. 93; Tahiroğlu, Erdoğan, **Roma Hukuku Dersleri**, s. 128; McDougal, "Private International Law", s. 521.

<sup>175</sup> **Ius gentium** kavramının, çeşitli hukuk dalları içinde farklı anlamları vardır. Örneğin uluslararası hukuk alanı içerisinde kavram devletlerin birbirleri ile ilişkisine ilişkin kuralları açıklamak amacıyla da kullanılmaktadır. Ancak bu kavramın Roma hukuku kapsamında kullanılan anlamıyla bir ilgisi yoktur. Bkz. Schwarz, **Roma Hukuku Dersleri**, C. I, s. 106; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 177.

<sup>176</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 173; Söğütü, **Roma Özel Hukuku**, s. 100; Schwarz, **Roma Hukuku Dersleri**, C. I, s. 106; Koschaker, **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, s. 11; Umur, **Roma Hukuku Ders Notları**, s. 93; Tahiroğlu, Erdoğan, **Roma Hukuku Dersleri**, s. 128; Du Plessis, Borkowski, **Borkowski's Textbook on Roman Law**, s. 111; Schiller, **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, s. 173.

Roma İmparatorluğu'nun yıkılmasından sonra Romalıların artık Alman kavimlerinin hukuklarını görmezden gelmesi imkânsız hale gelmiştir<sup>177</sup>. Dolayısıyla yine bir Roma hukuku niteliğinde olan **ius gentium** yerine, kişilere bağlı oldukları kavmin hukuku uygulanmaya başlamıştır<sup>178</sup>. Bu yaklaşımın sonucu olarak Romalılar **ius civile**'ye tabi olmaya devam etmiştir. Ancak Romalılar yabancıların hukuklarını da tanımak zorunda kalmışlardır. Kişinin bağlı olduğu kavmin hukukunun kişi nereye giderse gitsin onu izlemesi yaklaşımı da böylelikle doğmuştur<sup>179</sup>.

Orta Çağ'ın başlangıcında statü adı verilen şehir devletlerine özgü ve Roma hukukundan farklılaşmış kurallar ortaya çıkmıştır<sup>180</sup>. Bu kurallar aynı zamanda kanunlar ihtilafına ilişkin hükümler de içermektedir. 14. yy'da yaşayan hukukçu **Bartolus** modern kanunlar ihtilafı kurallarının ilk temellerini atmıştır<sup>181</sup>. Orta Çağ boyunca İtalyan şehir devletlerinde ve Fransa'da (zira her bölge de şehir devletlerinden ya da kendi hukuklarına sahip ayrı şehirlerden oluşmaktadır) kanunlar ihtilafı kuralları gelişmeye devam etmiştir<sup>182</sup>. 17. yy'da ise Hollanda'da yaşanan gelişmeler neticesinde **Ulrich Huber** tarafından, yabancı hukukun başka bir ülkede uygulanmasının gerekçesinin milletlerarası nezaket olduğu öne sürülmüştür<sup>183</sup>. Bu yaklaşım ABD'li

<sup>177</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 18.

<sup>178</sup> Söğütü, **Roma Özel Hukuku**, s. 122; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 19.

<sup>179</sup> Kişinin ait olduğu kavmin hukukuna tabi olduğu hukuk sistemlerine ilişkin en önemli örneklerden birisi Osmanlı İmparatorluğu'dur (bkz. Savigny, **Private International Law and the Retrospective Operation of Statutes\_ A Treatise on the Conflict of Laws, and the Limits of their Operation in Respect of Place and Time**, s. 58).

<sup>180</sup> Göger, **Devletler Hususi Hukuku**, s. 27; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 48; Nomer, **Devletler Hususi Hukuku**, s. 51; Doğan, **Milletlerarası Özel Hukuk**, s. 191; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 24.

<sup>181</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 48; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 26. Bartolus'a göre sözleşmelerin şekline ve geçerliliğine uygulanacak hukuk sözleşmenin kurulduğu yer; ifasına uygulanacak hukuk ise ifanın gerçekleştirildiği yer hukukudur. Haksız fiillere uygulanacak hukuk ise fiilin meydana geldiği yer hukukudur. Bu tür örnekleri çoğaltmak mümkündür.

<sup>182</sup> Göger, **Devletler Hususi Hukuku**, s. 30; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 48; Nomer, **Devletler Hususi Hukuku**, s. 52; Doğan, **Milletlerarası Özel Hukuk**, s. 192; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 29.

<sup>183</sup> Göger, **Devletler Hususi Hukuku**, s. 30; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 50; Nomer, **Devletler Hususi Hukuku**, s. 53; Doğan, **Milletlerarası Özel Hukuk**, s. 193; Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 41; Arthur Nussbaum, "Rise and Decline of the Law-of-Nations Doctrine in the Conflict of Laws", **Columbia Law Review**, C. 42, S. 2, 1942, s. 190; Ryngaert, **Jurisdiction in International Law**, s. 149; Akehurst, "Jurisdiction in International Law", s. 217.



hukukçular tarafından da benimsenmiştir ve günümüze kadar ABD kanunlar ihtilafı hukukunda kendisine yer bulmuştur<sup>184</sup>. 19. yy'dan itibaren ise modern anlamda kanunlar ihtilafı kuralları içeren kanunlaşma hareketleri başlamıştır. ABD'li yazar Joseph Story, 1834 yılında yayınladığı kitabı nedeniyle kanunlar ihtilafı alanının modern anlamda kurucusu olarak kabul edilmektedir<sup>185</sup>. 20. yy'dan itibaren ise uluslararası konferanslar vasıtasıyla kanunlar ihtilafı kurallarının yeknesaklaştırılmasına ilişkin çalışmalar yapılmaya başlanmıştır<sup>186</sup>. AB'nin kurulması ve bu alanda çıkardığı tüzük ve direktifler ile yeknesaklaşma yönünde önemli mesafeler alınmıştır.

Kanunlar ihtilafı kurallarının tarihi gelişimi konusunun çalışmamız açısından önem taşıdığı kısmı, Romalıların **ius gentium** uygulamasıdır. Romalılar, **ius gentium** vasıtasıyla diğer kavimlerin hukuklarını görmezden gelerek onlara kendi geliştirdikleri hukuk kurallarını uygulamışlardır. Bu yaklaşım, Roma devleti güçten düşene kadar da devam etmiştir. Günümüzde ise dijital ortamı düzenleyen ve sınır ötesi uygulama kapsamına sahip hukuk kuralları da diğer devletlerin iç hukuklarını adeta görmezden gelmektedirler. Dolayısıyla çeşitli hukuk dallarında farklı anlamlar taşıyan **ius gentium** kavramı, kanaatimizce Roma hukukundaki anlamıyla tekrar hukuk dünyasına dönmüş durumdadır. Kanunlar ihtilafı kurallarının tarihi gelişim sürecinin diğer bir önemi de bu alanın sürekli olarak uygulanacak hukuku tespite odaklanmış olduğunu göstermesidir.

#### 4. Bazı Kanunlar İhtilafı Kavramları

Milletlerarası özel hukuk ya da kanunlar ihtilafı kurallarının değindiği birçok sorun ve bunları çözümlemek için geliştirdiği birçok farklı hukuki kurum bulunmaktadır. Çalışmamızın konusu bakımından bu kavramlardan özellikle iki tanesi önem arz

---

<sup>184</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 42; Mesut Aygün, “ABD Kanunlar İhtilafı Hukukuna Kuramsal ve Metodolojik Bir Bakış: Çeşitli Teori ve Metotlar, II. Restatement ve Sözleşmeye Uygulanacak Hukuk”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. 20, S. 2, 2016, s. 135.

<sup>185</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 50; Altuğ Yılmaz, “Anglo - Amerikan Aleminin İlk Önemli Devletler Hususi Hukukçusu Joseph Story”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 24 S. 1-4, 1959 s. 64.

<sup>186</sup> Beale, **A Treatise on the Conflict of Laws or Private International Law**, C. 1, s. 54.

etmektedir. Bunlardan ilki kamu düzeni, ikincisi ise doğrudan uygulanan kurallardır. Çünkü bu kavramlar, bir ülkede kanunlar ihtilafı kapsamında uygulanacak yabancı hukukun (**lex causae**), yerel hukuk (**lex fori**) ile etkileşimi (başka bir deyişle çatışması) hususunu düzenlemektedir.

Kamu düzeni (**ordre public**) kuralları, bir ülkede kamu hizmetlerinin sağlanmasını, güvenliğinin teminini, bireyler arasındaki ilişkilerin huzur ve ahlak kurallarına uygun şekilde yürütülmesini sağlayan kuralların tamamı olarak tanımlanmıştır<sup>187</sup>. Kamu düzeni kavramı, toplumdan topluma farklılık gösterebilen, zaman içerisinde değişim gösterebilen bir kavramdır<sup>188</sup>. Ayrıca kamu düzenine ilişkin kurallar ile iç hukukun emredici hukuk her zaman aynı değildir<sup>189</sup>. Örneğin reşit olma yaşı iç hukukta emredici bir kuralken kanunlar ihtilafı kapsamında kamu düzeninden sayılan bir kural değildir.

Yabancı hukukun hâkim tarafından uygulanması konusunda kamu düzeni sınırlayıcı bir etkiye sahiptir<sup>190</sup>. Yani hâkim tarafından yabancı hukuk uygulandıktan sonra ortaya çıkan sonuç tekrar kamu düzeni açısından değerlendirilir. Eğer kamu düzenine aykırı bir netice ortaya çıkmışsa, ilgili yabancı hukuk hükmünün olaya uygulanması engellenir. Böylelikle de yabancı hukukun uygulanması sınırlandırılmış olur.

---

<sup>187</sup> Göger, **Devletler Hususi Hukuku**, s. 95; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 141; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 84; Doğan, **Milletlerarası Özel Hukuk**, s. 259; Akıncı, **Milletlerarası Özel Hukuk**, s. 20; Nomer, **Devletler Hususi Hukuku**, s. 165.

<sup>188</sup> Göger, **Devletler Hususi Hukuku**, s. 98; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 149; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 84; Doğan, **Milletlerarası Özel Hukuk**, s. 258; Nomer, **Devletler Hususi Hukuku**, s. 164; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 133; Sovyetler Birliği'nin kamu düzeni konusundaki yaklaşımı için bkz. Andre Garnefsky, **Public Policy in Soviet Private International Law**, 2. bs, Netherlands, Springer Science Business Media, 1970, s. 152.

<sup>189</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 141; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 45; Doğan, **Milletlerarası Özel Hukuk**, s. 264; Akıncı, **Milletlerarası Özel Hukuk**, s. 21; Nomer, **Devletler Hususi Hukuku**, s. 171.

<sup>190</sup> Göger, **Devletler Hususi Hukuku**, s. 97; Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 151; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 85; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 45; Doğan, **Milletlerarası Özel Hukuk**, s. 259; Akıncı, **Milletlerarası Özel Hukuk**, s. 20; Nomer, **Devletler Hususi Hukuku**, s. 180; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 132; Tu, **Private International Law in China**, s. 43.

Doğrudan uygulanan kurallar (**mandatory rules**) bir ülkenin sosyal, politik veya ekonomik yapısının korunması için uyulması zorunlu olan kurallardır<sup>191</sup>. Bu kurallar genellikle özel hukuk ilişkilerinde etkili ancak kamu menfaati gözetilen kurallar olarak vücut bulmaktadır<sup>192</sup>. Örneğin tarihi eserlerin satışına ilişkin kurallar ya da döviz alışverişlerinin tabi olduğu mevzuat bu kapsamda değerlendirilebilecek niteliktedir. Kanunlar ihtilafı kapsamında bir mahkeme yabancı bir hukukun uygulanmasına karar vermiş olsa dahi doğrudan uygulanan kuralları, kanunlar ihtilafı kurallarından bağımsız olarak uygulamak zorundadır. Sadece hâkimin hukukunun doğrudan uygulanan kuralları değil, uygulanacak hukukun ve kimi durumlarda üçüncü ülkelerin doğrudan uygulanan kuralları da hâkim tarafından uyuşmazlığa uygulanmalıdır<sup>193</sup>.

## **B. Düzenleme Yetkisinin Sınır Ötesi Kullanımı Açısından Milletlerarası Özel Hukukun Etkisi**

Tarih boyunca değişik gerekçelere dayanarak da olsa kanunlar ihtilafı kuralları, yabancı hukukların ilgili ülke içerisinde uygulanmasına imkân vermiştir. Ancak bu uygulama her zaman için ev sahibi ülkede egemen olan devletin kendi rızası ve kontrolü ile olmuştur. Egemen devletler hangi hukuki ilişkiye hangi hukukun uygulanacağına yine kendileri karar vermişler ve bu uygulamayı da kendi mahkemeleri aracılığı ile gerçekleştirmişlerdir. Mahkemelerin uygulamalarında ise kamu düzeni ya da doğrudan uygulanan kurallar gibi kurumlar, egemen devletlerin yabancı hukukun uygulanmasına rağmen kendi menfaatlerini koruyabilmelerini mümkün kılmıştır. Dolayısıyla kanunlar ihtilafı kapsamında yabancı bir hukukun bir ülke mahkemesince uygulanması, aynı zamanda o ülkedeki egemen devletin

<sup>191</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 155; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 8; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 49; Doğan, **Milletlerarası Özel Hukuk**, s. 279; Akıncı, **Milletlerarası Özel Hukuk**, s. 23; Nomer, **Devletler Hususi Hukuku**, s. 185; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 143; Tu, **Private International Law in China**, s. 43.

<sup>192</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 155; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 11; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 50; Doğan, **Milletlerarası Özel Hukuk**, s. 278; Akıncı, **Milletlerarası Özel Hukuk**, s. 23; Nomer, **Devletler Hususi Hukuku**, s. 185; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 143.

<sup>193</sup> Çelikel, Erdem, **Milletlerarası Özel Hukuk**, s. 158; Şanlı, Esen, Ataman-Figanmeşe, **Milletlerarası Özel Hukuk**, s. 379; Tekinalp, **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, s. 299; Doğan, **Milletlerarası Özel Hukuk**, s. 28; Grusic vd., **Cheshire, North & Fawcett Private International Law**, s. 144.

uluslararası düzenleme, yargılama ve uygulama yetkilerini de kendi ülkesi içerisinde kullanması anlamına gelmektedir. Yine üzerinde durulması gereken bir konu da kanunlar ihtilafı kuralları kapsamında, yabancı devletlerin kendi hukuklarının uygulanması amacıyla bir irade göstermelerinin söz konusu olmamasıdır.

Devletlerin uluslararası düzenleme yetkilerini sınır ötesi kapsamda kullanmaları halinde kişilerin farklı ve birbirleri ile çelişkili hukuki yükümlülükler altında kalması hali, önceki başlıklarda da açıklandığı üzere bu çalışmanın konusunu oluşturmaktadır. Bu durumda değerlendirilmesi gereken konu, söz konusu çelişkili durumların kanunlar ihtilafı kuralları vasıtasıyla çözülüp çözilemeyeceğidir.

Her ne kadar kanunlar ihtilafı, kamu düzeni ve doğrudan uygulanan kurallar gibi hukuki kurumlar vasıtasıyla yabancı hukukun uygulanmasına etki edebilmekteyse de bu etki ancak mahkemeler önüne gelmiş belirli özel hukuk uyuşmazlıkları kapsamında ve yine bu kurumların uygulanmasını gerektiren koşullar içerisinde mümkün olabilmektedir. Ancak konunun bir özel hukuk mahkemesi önüne gelmemesi ya da özel hukuka ilişkin olmaması halinde kanunlar ihtilafının herhangi bir etki doğurabilmesi mümkün değildir. Ayrıca daha temel anlamda kanunlar ihtilafı, farklı ülke hukukları arasındaki gerçek çelişkileri çözmeye odaklanmadığından, çalışmamız konusu sorunun çözümünü de bu hukuk alanında aramak kanaatimizce doğru olmayacaktır.

Buraya kadar olan bölümlerde yapılan incelemeler neticesinde, egemen devletlerin egemenliklerini uluslararası düzenleme, yargılama ve uygulama yetkileri vasıtasıyla kullandıkları anlaşılmıştır. Bu uluslararası yetkilerin ülke içerisinde kullanımı mümkün olduğu gibi sınır ötesi etki taşıyacak şekilde kullanılmaları da belirli koşullar altında uluslararası hukuka uygun kabul edilmektedir. Uygulama ve yargılama yetkileri açısından devletler arasında yetki uyuşmazlığı çıkması ihtimali, bu uluslararası yetkilerin ülke dışında kullanımının fiili güç gerektirmesi nedeniyle pek mümkün değildir. Ancak düzenleme yetkisinin ülke dışında kullanımı son derece kolay ve yaygın olduğu için birden fazla devletin aynı olgu üzerinde düzenleme yetkisi iddiasında bulunması çok daha olasıdır. Böyle durumlarda kişiler üzerinde birbirinden

farklı hukuki yükümlölükler ya da birbirleri ile çelişen hukuki yükümlölükler bulunabilecektir. Bir kişinin birden fazla hukuk sistemine tabi olması sorunu internetin, iletişimin ve uluslararası ekonomik ilişkilerin yaygınlaşması ile çok daha yaygın hale gelmiştir. Ancak bu husustan doğan sorunların ne uluslararası hukuk alanında ne de kanunlar ihtilafı alanı içerisinde çözümlenemeyeceği açıktır. İşte bu nedenle öncelikle sorunu tanımlayan yeni bir hukuki kavram, çalışmamız kapsamında ortaya atılacaktır. Daha sonrasında ise bu kavramın tanımladığı hukuki sorunların çözümüne ilişkin öneriler paylaşılacaktır.

## V. YENİ BİR KAVRAM: HUKUKLARIN ÇATIŞMASI

Devletlerin uluslararası düzenleme yetkisini mülkilik ilkesi çerçevesinde ya da müsamahakâr ilkelere uygun olarak sınır ötesi kapsamda kullanmaları uluslararası hukuka uygun kabul edilmektedir. Ancak bu kriterleri kullanarak düzenleme yetkisinin aynı olgu hakkında birden fazla devlet tarafından kullanılması mümkündür. Her bir devletin kendi menfaatlerine uygun şekilde düzenleme yetkisi kullanacağı göz önüne alındığında, devletlerin bireyler üzerinde farklı yükümlölükler öngörme ihtimali yüksektir. Bu yükümlölükler kimi durumlarda birbirleri ile çelişmezken kimi durumlarda ise çelişkili olabilecektir. İşte bu şekilde birbirleriyle çelişen yükümlölükleri adlandırmak amacıyla “hukukların çatışması”<sup>194</sup> (**Conflict of Legal Orders**) kavramı tarafımızca ortaya atılmıştır<sup>195</sup>.

Hukukların çatışması kavramı, mülkilik ilkesi ya da müsamahakâr ilkelere uygun olarak sınır ötesi kapsamda devletlerin düzenleyici yetki kullanmaları neticesinde kişiler üzerinde birbirleriyle çelişen hukuki yükümlölükler doğması şeklinde tanımlanabilecektir. Hukukların çatışması kavramı sadece özel hukuk alanları ile

<sup>194</sup> Devletlerin uluslararası yetkilerini aynı olgu üzerinde kullanmaları “yarışan yetki (**concurrent jurisdiction**)” kavramı ile (bkz. Pazarıcı, **Uluslararası Hukuk**, s. 183, Ryngaert, **Jurisdiction in International Law**, s. 142.) ifade edilmektedir. Hukukların çatışması kavramı ise uluslararası yetkiye ilişkin durumu göz ardı ederek kişiler üzerindeki hukuki yükümlölüklerden doğan çelişkileri ifade etmektedir.

<sup>195</sup> Önemle belirtmek gerekir ki anılan sorun ilk kez tarafımızca tespit edilmiş değildir. Söz konusu problemin daha önce tanımlandığı bir çalışma için bkz. Christopher Kuner, “The Internet and the Global Reach of EU Law”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 01.02.2017, s. 12, doi:10.2139/ssrn.2890930.

sınırlı değildir; kamu hukuku nitelikli kurallar açısından da meydana gelebilmektedir. Hatta ağırlıklı olarak hukukların çatışmasının kamu hukuku içerisinde oluşacağını söylemek de kanaatimizce mümkündür.

Hukukların çatışması kavramının bir diğer özelliği de sadece mahkeme önüne gelen uyuşmazlıklarda meydana gelen bir vakıa olmamasıdır. Hatta tam tersine mahkemelerin önüne gelmeyen ve devlet ile kişiler arasında etki doğuran hukuk kurallarının uygulanması sırasında hukukların çatışmasının daha yoğun olarak meydana geldiğini söylemek mümkündür.

Aşağıdaki başlıklar altında öncelikle hukukların çatışması kavramının devletlerin uluslararası yetkisi ve kanunlar ihtilafı konuları ile ilişkisi incelenecektir. Daha sonra hukukların çatışmasından kaynaklı sorunların çözümü için bir metot öne sürülecek ve hukukların çatışması ile dijital ortam arasındaki bağlantı irdelenecektir.

#### **A. Hukukların Çatışması ile Devletlerin Uluslararası Yetkisinin İlişkisi**

Devletlerin uluslararası yetkisi, devletlerin egemenlik haklarını fiilen kullanmaları anlamına gelmektedir. Uluslararası yetkinin düzenleme, yargılama ve uygulama yetkisi olarak üç farklı görünümü bulunmaktadır. Uluslararası yetki, mülkilik ilkesine göre ülke içerisinde kullanılabileceği gibi çeşitli uluslararası hukuk kuralları çerçevesinde ülke dışında da kullanılabilmektedir.

Düzenleme yetkisinin sınır ötesi kapsamda yani ülke dışında kullanılması ise müsamahakâr ilkeler çerçevesinde uluslararası hukuka uygun kabul edilmektedir. Birden fazla devletin düzenleme yetkisini aynı olgu üzerinde kullanabilmesi de imkân dahilinde olup bu yetki çerçevesinde birbiriyle çelişen hukuki yükümlülükler öngörülmesi halinde hukukların çatışması meydana gelmektedir.

Uluslararası hukuk çerçevesinde hukukların çatışması halinde öngörülmüş herhangi bir somut ve uygulanabilir çözüm mevcut değildir. Her ne kadar çözüm önerisi olarak birçok görüş öne sürülmüşse de bunlar uluslararası hukuk kuralı haline gelmemişlerdir. Uluslararası hukuk tarafından bu konuda çeşitli somut çözümler

önerilmiş olsaydı dahi kanaatimizce hukukların çatışması durumunda bireylerin karşı karşıya kaldığı sorunların çözümünü uluslararası hukukta aramak doğru değildir. Zira uluslararası hukuk esasen devletler arasındaki ilişkilere odaklanmakta olup kişiler ile devletler arasındaki ilişkileri kapsamı dışında tutmaktadır. Dolayısıyla bir kişinin hangi hukuka uygun şekilde fiillerini ve işlemlerini yapması gerektiği konusu uluslararası hukuk alanı dışındadır. Her ne kadar milletlerarası sözleşmelerle, hukukların çatışması sorunları çözülebilecek nitelikte olsa da devletler arasında böyle bir uzlaşının henüz mevcut olmadığını söylemek mümkündür. Hal böyle olunca kanaatimizce milletlerarası sözleşmeler ile hukukların çatışması sorunu çözülene dek<sup>196</sup> çözüm yollarının iç hukuk kuralları vasıtasıyla aranması yerine olacaktır. Her devletin kendi vatandaşını gözetmesi gerektiği düşünüldüğünde, devletlerin iç hukukları vasıtasıyla vatandaşlarını yabancı ülkelerin sınır ötesi uygulama kapsamlı kanunlarından korumalarını beklemek makul bir yaklaşım olacaktır.

Netice itibarıyla devletlerin uluslararası yetkisinin, hukukların çatışması kavramının temelini oluşturduğunu söylemek mümkündür. Ancak hukukların çatışmasından doğan sorunların çözümü kanaatimizce uluslararası hukukta değil, iç hukukta aranmalıdır.

## **B. Hukukların Çatışması ile Kanunlar İhtilafının İlişkisi**

Kanunlar ihtilafı, yabancı hukukun ev sahibi ülkede uygulanmasına yönelik kural ve yaklaşımları yüzyıllar boyunca geliştirmekte olan köklü bir hukuk dalıdır. Ancak kanunlar ihtilafı, yabancı kanunların ev sahibi ülkede yine ev sahibi ülkenin rızası ile uygulanması konusuna odaklanmaktadır. Dolayısıyla kanunlar ihtilafı kuralları, iki farklı devletin hukuk kuralları arasında bulunan çelişkinin yani gerçek bir çatışmanın çözümlenmesini hedeflememektedir. Öte yandan hukukların çatışması kavramı ise birden fazla farklı devletin hukuk kurallarının aynı olgu üzerinde birbiriyle çelişen yükümlülükler öngörmesine dayanmaktadır. Yani burada her devlet kendi hukuk

---

<sup>196</sup> Hukukların çatışması, devletlerin düzenleyici yetkilerini kullanmalarından doğmaktadır. Dolayısıyla her devlet yeni kanunlar çıkardıkça hukuk kurallarının birbirleriyle çatışma ihtimalleri de doğmaktadır. İşte bu nedenle konunun milletlerarası sözleşmelerle çözülebilmesi için ya her yeni kanun tipine uygun milletlerarası sözleşme yapılması ya da hukukların çatışması konusunda genel kuralların yer aldığı bir milletlerarası sözleşme imzalanması gerekmektedir.

kuralının uygulanmasını; diğer devletin rızasını ya da hukuk kurallarını dikkate almadan kendi egemenliğine dayalı olarak sağlamaya çalışmaktadır. İşte bu nedenle hukukların çatışması kavramının farklı hukuki yükümlülükler arasındaki gerçek bir çatışmaya odaklandığı ifade edilmektedir.

Kanunlar ihtilafı gibi yüzyıllardır gelişmekte olan bir hukuk dalının, hukukların çatışması kavramına şimdiye kadar neden değinmediği konusunun irdelenmesi yerinde olacaktır. Öncelikle ifade etmek gerekir ki; yabancı hukuk ile etkileşim konusunun ele alınması için mutlaka devletler arasındaki ilişkilerin yoğun olması gerekmektedir. Roma'nın diğer kavimlerle ilişkisi, İtalyan şehir devletlerinin ilişkileri, Avrupa'daki ülkelerin birbirleri ile ilişkileri ya da ABD'deki eyaletlerin birbirleri ile ilişkileri esasen kanunlar ihtilafı kurallarının gelişimine ön ayak olan tarihi olaylardır. İşte bu tarihi olaylar örgüsü günümüzde ise internet gibi iletişim imkanları ile uluslararası ekonomik ilişkilerin artmasına bağlı olarak tüm devletler arasındaki ilişkilerin artması şeklinde devam etmektedir. 20. yy'da sınır ötesi rekabet hukuku kuralları ile başlayan sınır ötesi uygulama kapsamında sahip kanunların yürürlüğe konması eğilimi günümüzde dijital ortamın önem kazanmasına paralel şekilde artmaktadır. Tıpkı Romalıların diğer kavimlerin hukukunu görmezden geldiği **ius civile – ius gentium** döneminde olduğu gibi, dijital ortama ilişkin kanunlar söz konusu olduğunda günümüzde de devletler diğer devletlerin hukuklarını görmezden gelme eğilimindedir. İşte bu eğilim neticesinde kanunlar ihtilafının uygulanacak hukuka ilişkin metodolojisi ve kuralları, hukukların çatışması kavramından doğan sorunları çözememektedir. Kanunlar ihtilafının tarihi boyunca da benzer bir dönem yaşanmadığı için kanunlar ihtilafı kurallarının gelişimi içerisinde hukukların çatışmasına ilişkin herhangi bir yaklaşım görülememektedir.

Hukukların çatışması kavramı, kanunlar ihtilafı gibi sadece özel hukuka odaklı değildir. Bunun yerine hukukların çatışması kavramı, hukuku özel ya da kamu fark etmeksizin bir bütün olarak ele almaktadır. Yine benzer şekilde hukukların çatışması, sadece yargılama faaliyetleri ile sınırlı olmayıp kişiler üzerinde hukuki yükümlülük doğuran her türlü hukuk kuralından (idari organlar tarafından uygulanan rekabet,



enerji ya da kişisel verilerin korunması gibi hukuki alanlar da dahil) doğabilecek çatışmaları kapsamına almaktadır.

Hukukların çatışması kavramının özel hukuk mahkemelerinin yargılama alanına giren konularda meydana gelmesi halinde mahkemelerin hangi hukuk kurallarını uygulaması gerektiği de üzerinde durulması gereken sorulardan birisidir. Kanunlar ihtilafı kuralları çerçevesinde iç hukuktan bir dayanak olmadığı sürece bir mahkemenin yabancı bir ülke hukukunu uygulaması mümkün değildir. Dolayısıyla yargılamayı yapan mahkemenin uyuşmazlık konusuna diğer bir devletin uluslararası düzenleme yetkisi çerçevesinde uygulanabilecek yabancı hukukları görmezden gelmesi gerekmektedir. Aksi durum ev sahibi devletin egemenlik haklarının zedelenmesine sebep olacaktır. Buradaki görmezden gelme yaklaşımının hukuki dayanağı kamu düzeni ya da doğrudan uygulanan kurallar değil; yabancı hukukun ev sahibi ülke içerisinde bağlayıcılığı olmaması yani tanınmamasıdır. Kamu düzeni ya da doğrudan uygulanan kurallar çerçevesinde yabancı hukuka müdahale edilebilmesi için öncelikle ilgili yabancı hukukun kanunlar ihtilafı kuralları çerçevesinde ülke içerisinde uygulanmasına izin verilmiş olmalıdır. Hukukların çatışması kavramında bu olgu eksik olduğu için kamu düzeni ya da doğrudan uygulanan kurallar kurumlarına başvurulması mümkün olmamaktadır.

Hukukların çatışması kavramının kamu hukukuna ilişkin yargılama (idare ya da ceza mahkemeleri) yapan mahkemeler nezdinde meydana gelmesi halinde de durum, özel hukuk mahkemelerindekinden farklı değildir. Burada özellikle idare ya da ceza mahkemelerinde yabancı hukuklara zaten hiç etki tanınmadığını da belirtmek gerekmektedir.

### **C. Hukukların Çatışmasından Doğan Sorunların Çözümüne Kavuşturulması Gerekliliği**

Hukukların çatışması kavramının kanunlar ihtilafından farkının ortaya konması ya da mahkemelerin bu konudaki yaklaşımının ne olması gerektiği konusundaki açıklamaların birden fazla ülkenin çelişkili hukuki yükümlülükleri altında bulunan

kişilerin problemli durumunu çözmediği açıktır. Aynı şekilde uluslararası hukuk da bu kişilerin içinde bulundukları duruma bir çözüm getirmemektedir.

Yukarıda da açıklandığı üzere kanaatimizce bu tür sorunların çözümü, uluslararası hukukta bir çözüm bulunana dek iç hukukta aranmalıdır. Hukukların çatışması kavramları birçok farklı kanunda meydana gelebileceği için her özel kanuna özgü çözümlerin yani kazuistik yöntemin kullanılması gerekmektedir. Dolayısıyla öncelikli olarak milli menfaatleri tehdit eden hukukların çatışması sorunları tespit edilmeli ve daha sonrasında bu konulardaki iç hukuk kuralları vasıtasıyla hukukların çatışması nedeniyle doğabilecek sorunlar, ilgili devlet ve kişiler açısından asgari düzeye indirilecek biçimde çözümlenmeye çalışılmalıdır. Çalışmamızın ileriki bölümlerinde bu konuda yabancı devletlerce alınan tedbirler de incelenecektir.

Önemle belirtmek gerekir ki hukukların çatışmasından kaynaklı sorunların tamamen ortadan kaldırılması, sadece iç hukuk düzenlemeleri ile mümkün olamaz. Zira birden fazla devletin iradelerinden doğan uyuşmazlıkların tek taraflı iç hukuk kuralları vasıtası ile çözülmesi mümkün olmayacaktır. Ancak tek taraflı iç hukuk kuralları, hukukların çatışmasından doğan sorunların etkilerini kabul edilebilir bir düzeye indirmek amacıyla kullanılabilir.

#### **D. Hukukların Çatışması ile Dijital Ortamın İlişkisi**

İnternetin ve iletişim imkanlarının gelişmesi, yabancılık unsuru taşıyan fiillerin ve işlemlerin de aşırı şekilde artmasına sebep olmuştur. Dijital ortamın yaygınlaşması ve öneminin artması, dijital ortamın hukuki düzenlemelere konu edilmesini de hızlı bir şekilde arttırmıştır. Artık hemen her ülkede kişisel verilerin korunması (her ne kadar dijital ortam dışındaki kişisel verileri de kapsasa da), elektronik haberleşme, elektronik ticaret ya da internet üzerinden işlenen suçlara ilişkin hukuki düzenlemeler bulunmaktadır.

Dijital ortamın çalışmamız açısından en önemli özelliği, dijital ortam içerisinde ülke sınırlarının bulunmamasıdır. Dolayısıyla bir ülke içerisinde gerçekleştirilen bir fiilin diğer ülkede etki doğurması çok kolay hale gelmiştir. Örneği fiziki ortamda İtalya’da

bulunan bir İtalyan'ın Türkiye'de bulunan bir Türk'e yüz yüze hakaret etmesi mümkün değildir. Hakaret fiilinin gerçekleşebilmesi ancak iki kişinin de aynı fiziki ortamda bulunması ile mümkün olabilmektedir. Dolayısıyla bir ülkeden diğer bir ülkeye etki eden fiil meydana gelememektedir. Ancak internet, işte bu tür hakaretleri mümkün kıldığı için bir ülkeden diğer ülkeye etki edebilecek fiillerin meydana gelmesi çok daha kolay hale gelmiştir. Söz konusu fiillerin artışı, uluslararası düzenleme yetkisinin mülkîlik ya da müsamahakâr ilkeler çerçevesinde sınır ötesi kapsamda kullanımını yaygınlaştırmış ve dolayısıyla hukukların çatışması vakıalarının da artmasına sebep olmuştur. Dolayısıyla dijital ortam gelişmeye devam ettikçe hukukların çatışması da hukuk uygulaması içerisinde yaygınlaşacaktır.

Hukukların çatışması vakıalarının dijital ortama ilişkin hukuk kuralları haricinde de meydana gelebilmesi mümkündür. Ancak çalışmamızın konusu sadece dijital ortamı düzenleyen hukuk kuralları ile sınırlı tutulacaktır. Bu kapsamda aşağıdaki bölümlerde öncelikle dijital ortam hakkında daha detaylı bilgi paylaşılacaktır. Daha sonrasında ise hukukların çatışması vakıaları yaratan iki konu üzerinde durulacaktır. Konulardan ilki sınır ötesi uygulama kapsamına sahip kişisel verilerin korunması kanunlarıdır. İkincisi ise ceza mahkemelerinin bilgi taleplerine ilişkin ABD hukukunda yer alan düzenlemelerdir. Sonraki bölümde de hem hukukların çatışmasından kaynaklanan sorunları çözmek amacıyla da kullanılan veri lokalizasyonu konusuna değinilecektir. Her konuya ilişkin ülkemize özgü çözüm önerileri de bu bölümler içerisinde konuya özgü olarak paylaşılacaktır.

## **İKİNCİ BÖLÜM**

### **KİŞİSEL VERİLERİN KORUNMASINA DAİR KANUNLARIN SINIR ÖTESİ UYGULAMA KAPSAMI**

#### **I. GİRİŞ**

21. yüzyılı şekillendirmekte olan internet, günümüzde kişiler arasındaki bilgi paylaşımı ve iletişimin temel altyapısını oluşturmaktadır. İnternet aynı zamanda yerel ve uluslararası ticaret açısından da çok önemli bir rol oynayarak ülke ekonomileri için vazgeçilmez bir yer edinmiştir. İnternet vasıtasıyla ticari faaliyetler artık çok daha kolay ve hızlı gerçekleştirilebilmektedir. Salt internet üzerinden gerçekleştirilen ticari faaliyetler ise çok daha kolay bir şekilde ölçeklenebilmekte ve tek bir merkezden dünyadaki tüm ülkelere sunulabilmektedir. Benzer durum bilgi paylaşımı ile iletişime yönelik faaliyetler için de geçerlidir.

İnternetin etkin bir şekilde işleyebilmesi için olmazsa olmaz koşul, uluslararası veri akışının sağlanmasıdır<sup>197</sup>. Uluslararası veri akışı, internet vasıtasıyla ülkeler arasında verilerin serbestçe dolaşabilmesi anlamına gelmektedir. Verilerin ülkeler arasında serbestçe dolaşabilmesi, internet üzerinden sunulan her türlü hizmetin dünyanın her yerinden erişilebilir olmasını sağlamaktadır. Ancak bu dolaşımın engellenmesi halinde, hizmetlerin erişilebilirliği sınırlanmakta ve bu doğrultuda internetin mevcut yapısı bozulmaktadır.

Uluslararası veri akışının sağlanması, verilerin farklı ülkelerin mevzuatlarına tabi olması sonucunu da doğurmaktadır. Bu da bireylerin kişisel verilerin korunmasına yönelik haklarının korunması sorununu gündeme getiren hususlardan birini teşkil etmektedir. İnternetin yaygınlaşması ve bilgi teknolojilerinin gelişmesine bağlı olarak artan veri işleme kapasitesi, kişisel verilerin korunmasının önemini tüm dünyada

---

<sup>197</sup> Uluslararası veri akışının artan önemi hakkında bkz. W. Gregory Voss, “Cross-Border Data Flows, the GDPR, and Data Governance”, **Washington International Law Journal**, C. 29, S. 3, 2019, s. 487.

arttırmıştır<sup>198</sup>. Bu çalışma tarihi itibarıyla ülkelerin %71’inde kişisel verilerin korunmasına ilişkin yürürlükte kanunlar bulunmaktadır<sup>199</sup>.

Kişisel veri kavramı, bir gerçek kişiye ilişkin her türlü bilgi anlamına gelmektedir. Kişisel verilerin korunmasına ilişkin kanunlar da kişisel verilerin hangi koşullar altında işlenebileceğini<sup>200</sup> ve bu verilerin hukuka aykırı olarak işlenmemesi için ne gibi önlemler alınması gerektiğini düzenlemektedirler.

Kişisel verilerin korunması konusunda, Nazi Almanyası’nın yarattığı acı tecrübeler nedeniyle Avrupa ülkeleri başı çekmektedir. Nitekim ilk kişisel verilerin korunması kanunu, Almanya’nın bir eyaletinde yürürlüğe konmuştur<sup>201</sup>. 108 Sayılı Sözleşme de yine Avrupa Konseyi tarafından hazırlanarak imzaya açılmıştır. 1995 yılında AB Direktifi, 2018 yılında da bir tüzük statüsünde olan GDPR<sup>202</sup>, AB tarafından yürürlüğe konmuştur. Ülkemizde ise 2000’li yıllardan itibaren hazırlanan taslak kanun çalışmaları neticesinde 2016 yılında KVKK kanunlaşmıştır.

İnternet ve bilgi teknolojilerinin gelişimi konusunda daha ileride olan ABD ile bunların kullanıcısı konumu daha ağır basan AB arasında, kişisel verilerin korunması konusunun nasıl ele alınacağı noktasında yaklaşım farklılığı bulunmaktadır<sup>203</sup>. AB

<sup>198</sup> Kişisel verilerin korunması gereksinimine ilişkin detaylı bilgi için bkz. Elif Küzeci, **Kişisel Verilerin Korunması**, 4. bs, İstanbul, On İki Levha Yayıncılık, 2021, s. 19.

<sup>199</sup> “Data Protection and Privacy Legislation Worldwide”, UNCTAD, (01.11.2021), (Çevrimiçi) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>, 01.11.2021.

<sup>200</sup> Kişisel verilerin işlenmesi kavramı, kişisel veriler üzerinde yapılabilecek her türlü işlemi ifade etmektedir. Örneğin kişisel verilerin saklanması, kişisel verilerin paylaşılması ya da kişisel verilerin analiz edilerek belirli sonuçlara ulaşılması gibi faaliyetler; kişisel veri işleme faaliyeti olarak nitelendirilmektedir.

<sup>201</sup> Söz konusu ilk kişisel verilerin korunması yasası, Almanya’nın Hessen eyaletinde yürürlüğe girmiştir, detaylar için bkz. Olga Stepanova, Patricia Jechel, “The Privacy, Data Protection and Cybersecurity Law Review: Germany”, **The Law Reviews**, 2022, (Çevrimiçi) [https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,\(BDSG\)%20entered%20into%20force,28.10.2022](https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,(BDSG)%20entered%20into%20force,28.10.2022).

<sup>202</sup> 25 Mayıs 2018 yılında yürürlüğe giren GDPR hakkında detaylı bilgi için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

<sup>203</sup> Manuel Klar, “Binding E Binding Effects of the E Ects of the European General Data Protection Regulation (GDPR) on U.S. Companies”, **Hastings Science and Technology Law Journal**, C. 11, S. 2, 2020, s. 102. Bununla birlikte son yıllarda ABD’de bölgesel olarak AB düzenlemelerini takip eden kanunlar hayata geçirilmektedir. California veri koruma hukuku

tarafında kişisel verilerin korunması konusu, detaylı ve kapsamlı kanunlarla genel uygulama alanı bulacak şekilde düzenlenmektedir. Buna karşılık ABD’de genel ve detaylı düzenlemeler yerine sadece sorunlu olabilecek veri kategorilerine (örneğin, sağlık verileri veya kredi notuna ilişkin veriler gibi) ilişkin kanuni düzenlemeler yapılmaktadır. Son yıllarda bazı eyaletlerin AB gibi genel ve detaylı kanuni düzenlemeler yaptığı da gözlemlenmektedir.

Kişisel verilerin korunmasına ilişkin kanunların etkin bir şekilde koruma sağlayabilmesi için özellikle ticari faaliyetleri sosyal medya, teknoloji veya veri işleme olan gerçek veya tüzel kişilere uygulanabilir olmaları gerekmektedir. Zira kişisel veri işleme faaliyetlerinin çok büyük kısmı bu tür kişiler tarafından gerçekleştirilmektedir. Ancak bu tür kişiler, internetin sağladığı esneklikten de yararlanarak genellikle yabancı bir ülkeden ev sahibi ülkeye hizmet sunar pozisyondadırlar<sup>204</sup>. Örneğin ABD menşeli sosyal medya şirketleri genel olarak İrlanda veya ABD merkezli olacak şekilde diğer ülkelerdeki kişilere sosyal medya hizmetlerini sunmaktadırlar. Hal böyle olunca kişisel verilerin korunması kanunlarının, yabancı bir ülkede bulunan kişilere uygulanması ihtiyacı doğmaktadır.

İnternetin gelişmesinin bu çalışma açısından doğurduğu en önemli sonuçlardan birisi, ülkeler arasındaki sınırların etkisinin internet ile zayıflamış olmasıdır. Şüphesiz ki bu sonuç serbest ticaret ve globalleşme açısından olumlu etkiler doğurmuştur. Öte yandan sınırların etkisinin zayıflaması aynı zamanda hizmet alan konumunda bulunan devletlerin kendi ülkelerinde sunulan hizmetlere ilişkin denetim ve kontrol imkânlarını de olumsuz yönde etkilemiştir. Ülkemizden örnek vermek gerekirse, **PayPal** Türk

---

hakkında bkz. Dyann Heward- Mills, Helga Turku, “California and the European Union Take the Lead in Data Protection”, **Hastings International and Comparative Law Review**, C. 43, S. 2, 2020, s. 319. Karşılaştırmalı bir çalışma için bkz. Greta Carlson, Jonathan McKinney, Elizabeth Slezak, Esther-Sarah Wilmot: “General Data Protection Regulation and California Consumer Privacy Act: Background Symposium: Compliance in International Corporate Legal Practices”, **Currents: Journal of International Economic Law**, C. 24, S. 1, 2020, s. 67; Jordan M. Blanke, “Protection for ‘Inferences Drawn’: A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act”, **Global Privacy Law Review**, C. 1, S. 2, 2020, s. 81-92.

<sup>204</sup> İnternetin dünyanın her yerinden erişilebilir olması ve. İnternet altyapısı ile veri merkezlerinin AB dışında olması, AB için dahi konuyu oldukça çetrefilli hale getirmektedir. Bu yönde açıklamalar için bkz. Kuner, “The Internet and the Global Reach of EU Law”, s. 5.

mevzuatına uyum sağlamayı reddettiği için Türkiye pazarını terk etmiştir. **YouTube** geçmiş yıllarda içerik kaldırmayı reddettiği için birkaç yıl boyunca ülkemizde erişime kapalı halde tutulmuştur. Kişisel verilerin korunması alanında da yabancı şirketlere Kişisel Verilerin Korunması Kurumu tarafından mevzuat ihlalleri nedeniyle sıklıkla yaptırımlar uygulandığı görülmektedir. Ancak bu idari para cezalarının tahsil edilip edilemediği konusunda kamuya açık bir bilgi bulunmamaktadır.

Kişisel verilerin, ülke dışından kişisel veri işleyen aktörlere karşı korunmasını temin etmek amacıyla kişisel verilerin korunmasına ilişkin kanunlara aynı zamanda sınır ötesi uygulama kapsamı içeren maddeler konulduğu ya da yorum yoluyla kanunların sınır ötesi uygulama kapsamına sahip olacak şekilde genişletildiği gözlemlenmektedir. Böylelikle bireylerin kişisel verilerin korunması hakkı, başka ülkede bulunup internet vasıtasıyla ev sahibi ülkede de korunmuş olmaktadır.

Son olarak veri lokalizasyonu kavramı ile kişisel verilerin korunmasına dair kanunların sınır ötesi uygulama kapsamına sahip olmasını karşılaştırmanın yapılmasının faydalı olacağı düşünülmektedir. Veri lokalizasyonunda, verilerin ülke içerisinde tutulması sağlanarak mülkilik ilkesi çerçevesinde verilerin tabi olacağı kanun belirlenmektedir. Sınır ötesi uygulama kapsamı olan kanunlarda ise uluslararası düzenleme yetkisinin sınır ötesi kullanımı vasıtasıyla yabancı ülkede bulunan verilere ev sahibi ülke kanunları uygulanmaktadır.

Çalışmamızın bu bölümünde, öncelikle sınır ötesi uygulama kapsamına ilişkin hükümler içeren GDPR incelenecektir. Daha sonrasında ise bu konuda açık hükümler içermemesine rağmen sınır ötesi de uygulanan KVKK ve Türk hukukunda bu konuda hükümler içeren diğer kanunlar incelenecektir.

## II. GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMI

### A. GDPR Hakkında Genel Bilgiler

Türkçe adıyla Genel Veri Koruma Tüzüğü olan GDPR, 25 Mayıs 2016 tarihinde AB tarafından kabul edilmiş ve yürürlük tarihi de 25 Mayıs 2018 olarak belirlenmiştir. GDPR, AB'nin kişisel verilerin korunmasına ilişkin ana düzenlemesini oluşturmaktadır. GDPR içerisinde kişisel verilerin işlenmesine ilişkin genel ilkeler, veri sorumluları ve veri işleyenlerin sorumlulukları ile veri sahiplerinin hakları gibi kişisel verilerin korunmasına ilişkin konulara dair hükümler bulunmaktadır<sup>205</sup>.

Bir tüzük statüsüne<sup>206</sup> sahip olması nedeniyle GDPR, tüm AB ülkelerinde doğrudan uygulama alanı bulabilmektedir. Bununla birlikte AB üye ülkelerinin bazı konular için iç hukuklarında düzenleme yapma yetkisi de bulunmaktadır<sup>207</sup>. Yine de GDPR için kişisel verilerin korunması konusunda AB'nin ana hukuki düzenlemesi yorumunu yapmak mümkündür.

Kişisel verilerin korunması hakkı, Avrupa Birliği İnsan Hakları Şartı<sup>208</sup> m. 8, Avrupa Birliği'nin İşleyişine İlişkin Antlaşma<sup>209</sup> m. 16 ve Avrupa İnsan Hakları Sözleşmesi<sup>210</sup>

<sup>205</sup> Detaylı bilgi için bkz. Murat Volkan Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", **Yaşar Hukuk Dergisi**, C.1 S.2 2019, s. 71-174; Andrew Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", **Fordham Law Review**, C. 86, S. 4, 2018, s. 1931.

<sup>206</sup> Sangwoo Lee, "A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing", 2018, s. 71-74, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3442428](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442428), 27.09.2020; Paul Lambert, **Understanding the New European Data Protection Rules**, NW, CRC Press Taylor & Francis Group, 2018, s. 6.

<sup>207</sup> Söz konusu yetkiye ilişkin olarak GDPR'nin 6., 8. ve 9. maddeleri örnek olarak belirtilebilir, bkz. Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>208</sup> Avrupa Birliği İnsan Hakları Şartı hakkında bilgi için bkz. "Charter of Fundamental Rights of the European Union", Official Journal of the European Union, 26.10.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>, 15.08.2021.

<sup>209</sup> AB'nin İşleyişine İlişkin Antlaşma hakkında bilgi için bkz. "The Treaty on the Functioning of the European Union", Official Journal of the European Union, 26.10.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>, 15.08.2021.

<sup>210</sup> Avrupa İnsan Hakları Sözleşmesi hakkında bilgi için bkz. "European Convention on Human Rights", Council of Europe, 03.09.1953, (Çevrimiçi) [https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf), 15.08.2021.



m. 8 uyarınca bir temel insan hakkı olarak kabul edilmektedir. Bu hakkın korunması amacıyla AB içerisinde Kişisel Verilerin Korunmasına İlişkin 95/46 sayılı Direktif<sup>211</sup>, 1995 yılında yürürlüğe konmuştur<sup>212</sup>. Söz konusu düzenlemenin direktif statüsü nedeniyle her üye ülke direktife uygun şekilde kendi iç kanunlarını yürürlüğe sokmuştur<sup>213</sup>. Ancak bu durum AB'nin kişisel verilerin korunması açısından çok parçalı bir ortama dönüşmesine sebebiyet vermiştir.

1995 yılından bu yana veri işleme kapasitesini yükselten teknolojik gelişmeler ile iletişim imkânlarını arttıran internet, 2000'li yıllardan itibaren üretilen ve işlenen veri hacmini çok yüksek miktarlara çıkarmıştır<sup>214</sup>. Globalleşmenin getirdiği mal ve hizmet ticareti hacminin yükselişi de kişisel verilerin ekonomik amaçlarla kullanımını arttırmıştır<sup>215</sup>. Tüm bu gelişmeler, kişisel verilerin gerçek kişiler açısından önem ve etkisinin yükselmesi sonucunu doğurmuştur. Söz konusu gelişmelerin yarattığı yeni hukuki sorunlar kişisel verilerin korunması konusunda yeni mevzuata olan ihtiyacı arttırmıştır<sup>216</sup>. 95/46 sayılı Direktif'in yorumlanması yoluyla söz konusu yeni sorunlar çözülmeye çalışıldıysa da reform ihtiyacının önüne geçilemez hale gelmesi üzerine GDPR doğmuştur. Bu yönüyle GDPR, 95/46 sayılı Direktif'ten elde edilen tecrübelerin yeni ihtiyaçlarla birleştirildiği bir belge olma özelliğine sahiptir<sup>217</sup>. GDPR aynı zamanda, tüzük statüsü sayesinde, AB ülkelerinin kişisel verilerin korunması açısından parçalı olan yapısını bütünleştirerek kişisel verilerin korunması konusunda

<sup>211</sup> 24 Ekim 1995 tarihli ve 95/46/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi'ne ilişkin detaylı bilgi için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>.

<sup>212</sup> 1960 ve 1980 yılları arasında kişisel verilerin korunması alanında hayata geçirilen yerel düzenlemeler için bkz. Eduardo Ustaran (ed.), **European Data Protection Law and Practice**, Portsmouth NH USA, International Association of Privacy Professionals, 2018, s. 20.

<sup>213</sup> Detaylı bilgi için bkz. Europäische Union, Europarat (ed.), **Handbook on European Data Protection Law**, 2018 edition, Luxembourg, Publications Office of the European Union, 2018, s. 29-30; Paul Voigt, Axel von dem Bussche, **The EU General Data Protection Regulation A Practical Guide**, Switzerland, Springer International Publishing, 2017, s. 1-6.; Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", s. 79.

<sup>214</sup> Wei Chen Lin, "Where Are Your Papers: The Fourth Amendmnet, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption", **DePaul Law Review**, C. 65, S. 3, 2016, s. 1115.

<sup>215</sup> Mira Burri, Rahel Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", **Journal of Information Policy**, C. Vol. 6, 2016, s. 480.

<sup>216</sup> Graça Canto Moniz, "Finally: A Coherent Framework for the Extraterritorial Scope of EU Data Protection Law - the End of the Linguistic Conundrum of Article 3(2) of the GDPR", **UNIO – EU Law Journal**, C. 4, S. 2, 2018, s. 110.

<sup>217</sup> Moniz, **a.g.e.**, s. 110-111.

tüm AB'nin tek bir hukuk düzenini benimsemesini sağlamıştır. Bu yaklaşım, GDPR'ın uygulanabilirlik gücünü önemli derecede arttırmıştır<sup>218</sup>.

GDPR'ın konusu, konu ve yer bakımından uygulanmasına ilişkin hususlar, ilk üç madde içerisinde düzenlenmektedir. GDPR m. 1, GDPR'ın amacını gerçek kişilerin kişisel verilerin korunması ve işlenmesine ilişkin kurallar ile verilerin AB sınırları içerisinde serbestçe dolaşabilmesine ilişkin kuralları tespit etmek olarak belirlemektedir. Aynı madde içerisinde GDPR'ın bireylerin temel hak ve özgürlüklerinin korunmasına ilişkin bir düzenleme olduğu ifade edilmiştir.

GDPR m. 2 ise GDPR'ın konu bakımından kapsamını belirlemektedir. Anılan maddeye göre kısmen ya da tamamen otomatik yollarla kişisel verilerin işlenmesi veya bir dosyalama sisteminin parçası olarak ya da parçası olması niyetiyle otomatik olmayan yollarla kişisel verilerin işlenmesi; GDPR'ın konu bakımından kapsamına girmektedir. Buna karşın, yetkili makamlarca suç ile mücadele edilmesi için kişisel veri işleme faaliyetleri ya da gerçek kişilerin salt kendilerine veya ailelerine ilişkin gerçekleştirdiği kişisel veri işleme faaliyetleri gibi birtakım hususlar, GDPR'ın konu bakımından kapsamının dışına çıkarılmıştır.

Çalışmamızın konusunu oluşturan GDPR'ın bölgesel uygulama alanı ise GDPR m. 3 altında düzenlenmektedir. Herhangi bir hukuki düzenleme açısından da değerlendirilme yapıldığında varılan olağan sonuç, ilgili düzenlemenin, o düzenlemeyi çıkaran devletin, hâkim olduğu ülkedeki tüm kişilere mülkilik ilkesi gereği uygulanmasıdır. Söz konusu madde GDPR'ın bu niteliğini belirlemenin yanında, GDPR'ın AB üye devletlerinin, ülkesel sınırları dışında uygulanacağı halleri de tespit etmektedir. Çalışmamızın konusu açısından GDPR'ın önemi de işte bu madde ile çerçevesi çizilen sınır ötesi uygulama kapsamıdır. Aşağıdaki başlıklar altında GDPR'ın sınır ötesi uygulama kapsamına ilişkin olarak detaylı açıklamalar yapılacaktır.

---

<sup>218</sup> Christopher Kuner Lee A. Bygrave, Christopher Docksey, Laura Drechsler, (ed.), **The EU General Data Protection Regulation (GDPR): A Commentary**, Oxford, New York, Oxford University Press, 2020, s. 76.

## B. GDPR’ın Sınır Ötesi Uygulama Kapsamına Sahip Olmasının Sebepleri

GDPR’ın kabulü ile sonuçlanan AB’nin kişisel verilerin korunmasına ilişkin reform çalışmaları sırasında üzerinde durulan konulardan birisi de teknolojik gelişmelere uygun çözümler üretilebilecek bir hukuki düzenleme yapılması hususudur<sup>219</sup>. Bu kapsamda özel olarak teknolojik gelişmeler ışığında veri işleme faaliyetlerinin, ülkesel sınırlardan bağımsız olarak gerçekleştirilebildiğine değinilerek kişisel verilerin korunması hakkının etkin şekilde tesis edilebilmesi için sınır ötesi uygulama kapsamına ihtiyaç olduğu öne sürülmüştür<sup>220</sup>. GDPR’ın yürürlüğe girmesi bütün dünyada veri koruma standartlarının tekrardan tartışılmasına neden olmuştur<sup>221</sup>.

İnternetin yapısı göz önüne alındığında, artık veri işleme faaliyetlerinin ülkesel sınırlarla bağlı olmadığı açıkça görülebilmektedir<sup>222</sup>. Özellikle ABD merkezli teknoloji şirketlerinin, ABD’de kurulu tüzel kişiler vasıtasıyla tüm dünyaya hizmet sunabildiği düşünülünce; AB sınırları içerisinde bulunan bireylerin kişisel verilerin korunması haklarının tesisi ancak GDPR’ın sınır ötesi uygulama kapsamına sahip

<sup>219</sup> “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”, European Commission, 19.02.2020, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&qid=1634039084372&from=EN>, 17.07.2021; “Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century”, Brussels, European Commission, 25.01.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en>, 09.12.2020; “Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)”, 2012/0011, (2012), s. 4, (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF>, 11.01.2021.

<sup>220</sup> European Commission, “How Will the EU’s Data Protection Reform Make International Cooperation Easier?”, Görüş, 01.2016, s. 2, (Çevrimiçi) <https://op.europa.eu/en/publication-detail/-/publication/43a3511e-f681-11e7-b8f5-01aa75ed71a1/language-en/format-PDF>, 29.05.2020; EDPS, “Opinion of the European Data Protection Supervisor on the data protection reform package”, Görüş, Brüksel, EDPS, 07.03.2012, par. 12, (Çevrimiçi) [https://edps.europa.eu/sites/edp/files/publication/12-03-07\\_edps\\_reform\\_package\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf).

<sup>221</sup> GDPR’ın küresel olarak etkilerine ve orta doğu, kuzey Amerika gibi pek çok bölgedeki etkilerine ilişkin olarak bkz. Michael L. Rustad, Thomas H. Koenig, “Towards a Global Data Privacy Standard”, **Florida Law Review**, C. 71, S. 2, 2019, s. 431. AB kişisel verileri koruma hukukunun 95/46 sayılı Direktif’ten bu yana dünyada veri koruma hukuku bakımından bir standart belirleyici konumunda olduğu yönünde bkz. Orla Lynskey, **The foundations of EU data protection law**, 1. bs, United Kingdom, Oxford University Press, 2015, s. 41.

<sup>222</sup> Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, **German Law Journal**, C. 18, S. 4, 2017, s. 882.

olmasına bağlı olduğu sonucuna ulaşılabilmektedir<sup>223</sup>. Aksi durumda kişisel verilerin korunmasına ilişkin tüm hukuki yükümlülüklerden, sadece AB sınırları dışında bir tüzel kişi vasıtasıyla hizmet sunulurken kaçınılmazdır. Hemen belirtmek gerekir ki böyle bir ihtiyaç olması, kanaatimizce söz konusu sınır ötesi uygulama kapsamını; devletlerin egemenliği ve uluslararası yetkisine ilişkin uluslararası hukuka uygun hale getirmeye tek başına yeterli olmayacaktır.

GDPR'ın sınır ötesi uygulama kapsamına sahip olmasına dair bir diğer gerekçe olarak AB'de yerleşik işletmeler ile AB dışında yerleşik olmasına rağmen AB'ye mal ya da hizmet sunan işletmelerin eşit şartlarda faaliyette bulunabilmeleri gösterilmiştir<sup>224</sup>. Bu fikre göre GDPR'ın sınır ötesi uygulama kapsamı, AB pazarında faaliyet gösteren kişilerin adil şekilde rekabet etmelerini sağlayacaktır<sup>225</sup>. GDPR'ın sınır ötesi uygulama kapsamının olmadığı varsayıldığında, AB sınırları içerisinde bulunan kişiler, GDPR kurallarına uyum sağlamak zorunda kalacakken; AB sınırları dışından AB'ye hizmet sunan kişiler, bu kurallardan muaf olarak faaliyet gösterebilecektir<sup>226</sup>. Özellikle veri temelli hizmetler sunan sosyal medya ve bulut bilişim şirketleri açısından, söz konusu durumun çok büyük bir avantaj sağlayacağı şüphesizdir. Basit bir örnekle açıklamak

---

<sup>223</sup> GDPR m. 3'ün AB sınırları dışında faaliyet gösteren veri sorumluları ve veri işleyenler açısından en önemli hüküm olduğu yönünde bkz. Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. bs, İstanbul, On İki Levha Yayıncılık, 2019; Kimberly A. Houser, W. Gregory Voss, "GDPR: The End of Google and Facebook Or a New Paradigm in Data Privacy", **Richmond Journal of Law & Technology**, C. 25, S. 1, 2018, s. 10; Burri, Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", s. 496.

<sup>224</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 76. "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", European Data Protection Board, 12.11.2019, (Çevrimiçi)

[https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_after\\_public\\_consultation\\_en\\_1.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

<sup>225</sup> W. Gregory Voss, Kimberly A. Houser, "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies", **American Business Law Journal**, C. 56, S. 2, 2019, s. 288.

<sup>226</sup> 4 Mart 2014 tarihinde Avrupa Komisyonu Başkan Yardımcısı Reding bu konuya konuşmasında değinmiştir. Konuşmanın özgün hali şöyledir: "On territorial scope I recall the broad support that was voiced for making sure that non-European companies, when offering services to European consumers, apply the same rules and adhere to the same levels of protection of personal data as European companies. This is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world". "Speech - The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights", **European Commission**, 2014. Dan Jerker B. Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation", **International Data Privacy Law**, C. 5, S. 4, 2015, s. 230-231; Roman Beletski, "Critical assessment of the extraterritoriality of the EU General Data Protection Regulation", 2019, s. 61.

gerekirse, GDPR’a tabi olmayan bir sosyal medya şirketi, kişisel verileri reklam faaliyetleri için analiz etmek amacıyla veri sahibi olan kişilerden açık rıza almaya ihtiyaç duymayacakken; GDPR’a tabi olan diğer bir sosyal medya şirketi açık rıza almak zorunda kalabilecektir. Bu rızaların milyonlarca kişiden toplanması hem ekstra maliyetler yaratacak hem de rıza vermeyen kişilerin verilerinin işlenememesine sebep olacaktır. Netice itibarıyla GDPR’a tabi olan şirket, diğer şirkete kıyasla daha fazla maliyete katlanarak daha az kişinin verisini işleyebilir hale gelecektir. Bu durum da söz konusu şirketin, GDPR’a tabi olmayan şirketle rekabet etmesini imkânsız hale getirecektir.

### **C. GDPR’ın Sınır Ötesi Uygulama Kapsamına Sahip Olabilmesinin Şartları**

GDPR’ın sınır ötesi uygulama kapsamı m. 3 altında düzenlenmektedir. Bu kapsamda iki temel kriter esas alınmaktadır. Bu kriterler GDPR m. 3/1 uyarınca “kuruluş” kriteri ve GDPR m. 3/2 uyarınca “hedefleme” kriteridir. Bu iki kriterden birinin sağlanması halinde veri işleme faaliyeti, veri sorumlusu ve veri işleyene GDPR hükümleri uygulanacaktır. İlave olarak, GDPR m. 3/3’te ise AB sınırları içinde yerleşik olmasa dahi uluslararası kamu hukuku uyarınca üye devlet hukukunun uygulama alanı (örneğin konsolosluklar) bulduğu veri sorumluları bakımından da GDPR’ın uygulanacağı düzenlenmektedir. Çalışmamız açısından önem arz eden maddeler ise GDPR m. 3/1 ve m. 3/2’dir.

GDPR’ın bölgesel<sup>227</sup> olarak uygulama alanına ilişkin 3. maddesi, 95/46 sayılı Direktif m. 4’ün devamı niteliğindedir<sup>228</sup>. Ancak yukarıda da açıklandığı üzere Direktif, her AB üyesi ülkenin kendi kişisel verilerin korunması kanununu yürürlüğe sokmasını gerektiren bir AB mevzuatıdır. Dolayısıyla AB içerisinde gerçekleşen bir olaya hangi

---

<sup>227</sup> GDPR m. 3’ün başlığı “Bölgesel Kapsam” (**territorial scope**)’dır. Ancak madde hükmünde ifade edilen “bölgesel” kelime anlamı olan sınırlı karasal bütünü ifade etmemektedir. Hüküm GDPR’ın AB içinde ve dışındaki uygulama alanının hangi hallerde söz konusu olacağını belirlemektedir (Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 76).

<sup>228</sup> 95/46 sayılı Direktif’in m.4’e ilişkin olarak bkz. Moniz, “Finally: A Coherent Framework for the Extraterritorial Scope of EU Data Protection Law - the End of the Linguistic Conundrum of Article 3(2) of the GDPR”, s. 107; Maja Brkan, “Data Protection and Conflict-of-Laws: A Challenging Relationship”, **European Data Protection Law Review (EDPL)**, C. 2, S. 3, 2016, s. 325.

ülkenin hukukunun uygulanacağını tespiti için kurallara ihtiyaç duyulmaktadır. İşte bu kurallar da Direktif m. 4 içerisinde belirlenmektedir. Halbuki tüzük niteliği taşıyan GDPR, her AB ülkesinde ayrı bir kanun çıkarılması ihtiyacını ortadan kaldırarak tüm AB üye devletleri içerisinde direkt olarak uygulanmaktadır. Dolayısıyla Direktif m. 4'te yer alan hangi ülke hukukunun uygulanacağına dair kurallara GDPR içerisinde yer verilmemiştir<sup>229</sup>.

GDPR'ın bölgesel uygulama alanına ilişkin maddesinin son şeklini almasında önem arz eden iki ABAD<sup>230</sup> kararı bulunmaktadır. ABAD'ın **Google İspanya Kararı**<sup>231</sup> (unutulma hakkı kararı<sup>232</sup> olarak da bilinmektedir) ile **Weltimmo** kararı<sup>233</sup> hangi durumlarda AB sınırları dışında bulunan kişilerin 95/46 sayılı Direktif kapsamına (yani sınır ötesi uygulama kapsamına) gireceğini belirlemiştir. Söz konusu kararlarda belirlenen kriterler, GDPR'ın sınır ötesi uygulama kapsamına ilişkin maddesinin şekillenmesi noktasında önemli roller oynamışlardır.

GDPR'ın ilk taslağında<sup>234</sup> GDPR hükümlerinin, AB dışında yerleşik veri sorumlularına uygulanabilmesi için AB'de yerleşik kişilere “yöneltilmiş faaliyetler” bulunması veya AB'de yerleşik kişilerin davranışlarının izlenmesi kriterleri benimsenmiştir<sup>235</sup>. Bu kriterler ABAD'ın tüketici hukukuna ilişkin kurallarının uygulanmasına ilişkin verdiği 2010 tarihli kararından<sup>236</sup> esinlenilerek önerilmiştir<sup>237</sup>. Ancak daha sonradan taslak üzerine hazırlanan raporlardan birisinde, söz konusu kriterler herhangi bir ödeme karşılığı olmasa da mal ve hizmet sunan veri sorumluları

<sup>229</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 4.

<sup>230</sup> Avrupa Birliği Adalet Divanı hakkında bilgi için bkz. [https://curia.europa.eu/jcms/jcms/j\\_6/en/](https://curia.europa.eu/jcms/jcms/j_6/en/).

<sup>231</sup> Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, (European Court of Justice 13 Mayıs 2014).

<sup>232</sup> Dülger, “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, s. 155-157.

<sup>233</sup> Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság., (CJEU 01 Ekim 2015). Bilgi için bkz. Alan Toy, Gehan Gunasekara, “Is There a Better Option than the Data Transfer Model to Protect Data Privacy”, **University of New South Wales Law Journal**, C. 42, S. 2, 2019, s. 735-737.

<sup>234</sup> Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).

<sup>235</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 17.

<sup>236</sup> Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09), (Grand Chamber 07 Aralık 2010).

<sup>237</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 17.

ile davranışlarla sınırlı olmaksızın her türlü izleme faaliyeti yürüten veri sorumlularını kapsayacak şekilde genişletilmiştir<sup>238</sup>. Sunulan raporların ve AB üye devletlerinin önerilerinin birleştirilmesi sonucunda oluşturulan son taslakta ise sınır ötesi uygulama kapsamı kriterleri ödeme gerekliliğinden bağımsız olarak AB'deki kişilere hizmet sunulması ya da kişilerin izlenmesi (takip ve profil oluşturmaları içeren) olarak belirlenmiştir<sup>239</sup>. Söz konusu kriterler, büyük ölçüde kabul edilerek GDPR'a dahil edilmiştir.

Aşağıdaki başlıklar altında GDPR'ın sınır ötesi uygulama kapsamına sahip olmasına ilişkin belirlenen kriterler detaylı şekilde incelenecektir<sup>240</sup>.

### 1. Kuruluş Kriteri

GDPR m. 3/1 gereği AB sınırları içerisinde yerleşik bir kuruluşun faaliyetleri çerçevesinde gerçekleştirilen kişisel veri işleme faaliyetleri, GDPR'ın bölgesel uygulama kapsamı içerisine girmektedir. Bu kapsamda kuruluşun, veri sorumlusu ya da veri işleyen rollerine sahip olması önemli değildir<sup>241</sup>. Benzer şekilde söz konusu kişisel veri işleme faaliyeti AB sınırları içerisinde gerçekleşme dahi GDPR uygulama alanı bulabilmektedir. İşte bu kriter nedeniyle GDPR, sınır ötesi uygulama kapsamı kazanmaktadır.

<sup>238</sup> Avrupa Parlamentosu, Alman Yeşiller Partisi Milletvekili Jan Philipp Albrecht'i söz konusu teklifin ana raportörü olarak atayarak GDPR teklifine yanıt hazırlamaya başlamıştır. Albrecht, 8 Ocak 2013 tarihinde Avrupa Parlamentosu'nun Sivil Özgürlükler, Adalet ve İçişleri Komitesi ("LIBE" Komitesi, bkz. <https://www.europarl.europa.eu/committees/en/libe/home/highlights>) için GDPR teklifine ilişkin taslak raporunu yayınlamıştır. Rapor resmi olarak 10 Ocak 2013 tarihinde LIBE Komitesi'nin toplantısında sunulmuştur. "EP Draft Report LIBE 2012", European Parliament, 2012, (Çevrimiçi) [https://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/pr/922/922387/922387en.pdf](https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf), 14.12.2021.

<sup>239</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 12. Bkz. "EP Resolution GDPR 2014", European Parliament, 12.03.2014, (Çevrimiçi) [https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html), 14.12.2021.

<sup>240</sup> GDPR m. 3/3, GDPR'ın AB sınırları içerisinde bulunmayan, ancak uluslararası hukuk gereği AB üye ülkelerinden birinin hukukunun uygulandığı yerlerde bulunan veri sorumlularına da uygulanacağını hüküm altına almıştır. Bu kapsamda örnek olarak AB üye ülkelerinin elçilik ve konsolosluk binaları gösterilmektedir (bkz. "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", s. 22.). Ancak söz konusu kriterin çalışmamız açısından bir önemi olmadığı için, bu kriter için ayrı bir başlık açılmamıştır.

<sup>241</sup> Douwe Korff, "The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service", SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 19.08.2019, s. 22, doi:10.2139/ssrn.3439293.

GDPR m. 3/1 hükmü, 95/46 sayılı Direktif'te de büyük ölçüde aynı şekilde yer almaktadır. Bu kapsamda söz konusu kriter birçok ABAD içtihatlarına da konu olmuştur<sup>242</sup>.

GDPR m. 3/1'de yer alan kuruluş ifadesinden ne anlaşılması gerektiği, üzerinde değerlendirme yapılmasını gerektiren bir konudur<sup>243</sup>. Madde metninde kapsayıcılığı sağlamak adına özellikle kuruluş kelimesi kullanılmıştır. Zira GDPR, AB sınırları dışında bulunan veri sorumlusu ya da veri işleyen AB sınırları içerisinde kurabileceği, sadece hukuki statüye sahip tüzel kişilik ya da şubeleri kapsamayı hedeflememektedir. Bunun yerine kuruluş kelimesinden istikrarlı planlamalar çerçevesinde etkili ve gerçek faaliyetler yürüten organizasyonların anlaşılması gerektiği, GDPR'ın gerekçesinde ifade edilmiştir<sup>244</sup>. Gerekçeye göre organizasyonun hukuki statüsü önemli değildir. Dolayısıyla organizasyonun sadece kiralanmış bir ofiste bulunan birkaç kişiden ibaret olması mümkün olabileceği gibi bir bağlı şirket, irtibat bürosu ya da şube olması da mümkün olabilecektir<sup>245</sup>. Söz konusu geniş kapsam sayesinde, AB sınırları içerisinde bulunan organizasyonun hukuki statüsünün değiştirilmesi yoluyla GDPR'ın uygulama kapsamından çıkmaya yönelik girişimlerin önüne geçilmiş bulunmaktadır.

---

<sup>242</sup> Detaylı bilgi için bkz. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információs Zsábadság Hatóság.; Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Ayrıca bkz. Moniz, "Finally: A Coherent Framework for the Extraterritorial Scope of EU Data Protection Law - the End of the Linguistic Conundrum of Article 3(2) of the GDPR", s. 107-108; Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 79; Brendan Van Alsenoy, **Reconciling the (Extra)Territorial Reach of the GDPR with Public International Law**, Maklu, 2017, s. 81-84; Kararlar hakkında değerlendirme ve veri koruma reformuna etkisi hakkında bkz. Dan Jerker B. Svantesson, "Article 4(1)(a) 'establishment of the controller' in EU data privacy law—time to rein in this expanding concept?", **International Data Privacy Law**, C. 6, S. 3, 2016, s. 210-221.

<sup>243</sup> Brkan, "Data Protection and Conflict-of-Laws", s. 328; Korff, "The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service", s. 6.

<sup>244</sup> GDPR m. 22 orijinal hali ile şu şekildedir: "*Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.*"; "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", s. 7; Korff, "The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service", s. 6.

<sup>245</sup> German case Facebook v Independent Data Protection Authority of Schleswig Holstein hakkında açıklamalar için bkz. Brkan, "Data Protection and Conflict-of-Laws", s. 328.



Kuruluş kriterinin vurgulandığı en önemli ABAD kararı, unutulma hakkını da doğuran ABAD’ın **Google** İspanya<sup>246</sup> kararıdır. Bu karar kapsamında **Google**’ın İspanya’da bulunan şirketinin sadece tanıtım ve pazarlama faaliyetleri yürüttüğü, veri işleme faaliyetinin ise **Google**’ın ABD’de bulunan ana şirket tarafından gerçekleştirildiği öne sürülerek **Google**’ın ABD’de bulunan şirketinin 95/46 sayılı Direktif çerçevesinde AB hukuku kapsamında olmadığı savunması **Google** tarafından yapılmıştır<sup>247</sup>. ABAD ise, **Google**’ın İspanya’da bulunan şirketi ile **Google**’ın ABD’de bulunan şirketinin İspanya’daki faaliyetlerini ilişkili olarak kabul etmiştir. Bu değerlendirme çerçevesinde **Google** İspanya şirketinin, ABD’deki **Google** şirketinin AB sınırları içerisinde bulunan kuruluşu olduğuna ve bu kapsamda ABD’deki **Google** şirketinin de 95/46 sayılı Direktife tabi olduğu sonucuna varmıştır<sup>248</sup>. Böylelikle Direktifin sınır ötesi uygulama kapsamı olduğu yönünde içtihat oluşmuştur.

Öte yandan EDPB<sup>249</sup>, AB sınırları dışında bulunan bir veri sorumlusunun; AB sınırları içerisindeki bir veri işleyenden sadece veri işleme hizmeti almasının; o veri sorumlusunu GDPR’a tabi kılmayacağını da açıkça belirtmektedir<sup>250</sup>. Bu yorumdan hareketle AB içerisindeki kişilerle kurulan her türlü ilişkinin, AB dışında bulunan kişiyi GDPR’a tabi kılmayacağı sonucuna varmak da kanaatimizce mümkündür. Dolayısıyla başta veri işleyenlerden hizmet almak olmak üzere, AB içerisindeki kişilerle kurulan çeşitli ilişkilerin, kuruluş kriteri çerçevesinde AB dışındaki kişileri GDPR’a tabi kılıp kılmayacağının her olay üzerinde ayrıca denetlenmesi gerekmektedir<sup>251</sup>.

---

<sup>246</sup> Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

<sup>247</sup> a.y.

<sup>248</sup> a.y.

<sup>249</sup> EDPB, orijinal hali ile European Data Protection Board olarak adlandırılmaktadır, detaylı bilgi için bkz. [https://edpb.europa.eu/edpb\\_en](https://edpb.europa.eu/edpb_en).

<sup>250</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”.

<sup>251</sup> Korff, “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, s. 8; Voss, “Cross-Border Data Flows, the GDPR, and Data Governance”, s. 496; Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 74-100.

GDPR ile 95/46 sayılı Direktif arasında kuruluş kriteri açısından önemli bir farklılık bulunmaktadır. Direktife göre sadece veri sorumlularının kuruluşları, direktifin bölgesel uygulama kapsamında değerlendirilebilmektedir. GDPR ise veri sorumlularının yanında veri işleyenlerin kuruluşlarını da bölgesel uygulama kapsamına almaktadır. Dolayısıyla AB sınırları içerisinde bulunan bir kuruluş vesilesiyle AB sınırları dışında yerleşik bir veri işleyenin de GDPR'a tabi olması mümkün olabilecektir<sup>252</sup>.

Doktrinde yer alan bir görüşe göre, GDPR'ın veri işleyenler açısından da kuruluş kriterini benimsemesi, GDPR'ın uygulanması açısından boşluk yaratabilecek niteliktedir<sup>253</sup>. Bu kapsamda örnek olarak AB sınırları içerisinde bulunan veri işleyenin, GDPR'ın AB sınırları içerisinde doğrudan uygulanabilir olması nedeniyle, bir veri ihlali durumunu derhal veri sorumlusuna bildirmesi yükümlülüğü gösterilmektedir<sup>254</sup>. Bu bildirimle rağmen, AB sınırları dışında bulunan ve GDPR'a tabi olmayan veri sorumlusunun; veri ihlalini GDPR kapsamında ilgili AB üye ülkesi veri koruma otoritesine bildirme yükümlülüğü bulunmayacaktır<sup>255</sup>. Kanaatimizce GDPR'ın veri işleyenleri de kuruluş kriteri kapsamında GDPR'ın sınır ötesi uygulama kapsamı içerisine alabilmesinin, adli ve idari makamlara uygulamada yorum yapma imkânı bırakarak son derece dinamik bir alan olan kişisel verilerin korunması hukukunun etkin bir şekilde uygulanmasına yardımcı olacağı açıktır. Ancak bu yaklaşım, GDPR'ın sınır ötesi uygulama kapsamını her zaman için muğlak bıraktığından dolayı muhtemel yükümlülerin kendilerinin GDPR'a tabi olup olmadıklarını tam olarak kestirememesi şeklinde olumsuz bir sonuç da doğurmaktadır<sup>256</sup>. Ayrıca düşüncemize göre yukarıda bahsedilen örnekte, ilgili AB üye ülkesine veri ihlal bildirimi yapılması yoluyla korunabilecek bir hukuki yarar zaten bulunmamaktadır. Zira AB sınırları dışında bulunan bir veri sorumlusunun işlediği kişisel veriler, zaten GDPR m. 3 kapsamına girmiyorsa, bu kişisel verilerin

---

<sup>252</sup> Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, s. 34; "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", s. 11.

<sup>253</sup> Kuner vd., *The EU General Data Protection Regulation (GDPR)*, s. 86.

<sup>254</sup> "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", s. 13.

<sup>255</sup> Kuner vd., *The EU General Data Protection Regulation (GDPR)*, s. 87.

<sup>256</sup> Kuner vd., *a.g.e.*, s. 76-77.

ihlaline ilişkin bildirimlerin de AB otoritelerine yapılmasının bir faydası olmayacaktır. Çünkü bu kişilerin kişisel verilerin korunması haklarının tesisi, AB'nin menfaatine olmayacaktır. Dolayısıyla bu konuda rol alması gereken devlet, söz konusu kişilerin tabi olduğu ülkede egemen olan devlettir. Örneğin, bir Türk vatandaşının kişisel verilerinin, Türkiye'de yerleşik bir veri sorumlusu tarafından AB'de bulunan bir veri işleyene gönderilmesi ile bu veri işleyenin siber saldırı sonucunda verileri kaybetmesi halinde, Türk vatandaşı veri sahibi ile Türk vatandaşı veri sorumlusunun hak ve sorumlulukları GDPR'a göre değil, KVKK'ya göre belirlenmelidir. AB bu ilişkiye müdahil olacak şekilde bir düzenleme getirmiş olması varsayımı, kanaatimizce AB'nin kendi uluslararası yargı yetkisini bariz bir şekilde aşkın kullanması olarak kabul edilebilecek niteliktedir.

Son olarak belirtmek gerekir ki GDPR m. 3/1'in uygulanması açısından kişisel veri işleme faaliyetinin hangi ülkede gerçekleştiğinin ya da kişisel verisi işlenen kişilerin vatandaşlıklarının bir önemi bulunmamaktadır<sup>257</sup>. Kuruluş kriterinin şartları sağlandığı takdirde, AB sınırları dışında bulunan veri sorumlusu ya da veri işleyenler için de GDPR uygulanacaktır<sup>258</sup>.

## 2. AB'ye Yönelik Mal veya Hizmet Sunmayı Hedefleme Kriteri

GDPR m. 3/2/a kapsamında, GDPR'ın sınır ötesi uygulamaya sahip olmasını sağlayan kriterlerden birisi de AB sınırları dışarısında bulunan veri sorumlusu ya da veri işleyenlerin; AB sınırları içerisinde bulunan kişilere yönelik olarak mal veya hizmet sunmasıdır<sup>259</sup>. Bu duruma örnek olarak Türkiye'de yerleşik olan bir şirketin, AB pazarına hitap edecek şekilde bir elektronik ticaret sitesi işletmesi gösterilebilmektedir.

<sup>257</sup> Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, s. 35; "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1", s. 14.

<sup>258</sup> Kuruluş kriteri bakımından GDPR'ın uygulama alanına ilişkin örnekler için bkz Voigt, von dem Bussche, *The EU General Data Protection Regulation A Practical Guide*, s. 23.

<sup>259</sup> Ayrıca bkz. Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", s. 96-97.

Kriter kapsamında GDPR'ın uygulanabilir hale gelmesi için mal ya da hizmet sunulan kişilerin AB sınırları içerisinde bulunması yeterli kabul edilmektedir<sup>260</sup>. Kişilerin geçici ya da kalıcı olarak AB'de bulunması ya da vatandaşlıklarının farklı olması gibi hususlar, bu kriter çerçevesinde GDPR'ın uygulanmasını engellememektedir<sup>261</sup>. Öte yandan AB sınırları içerisinde bulunan bir kişinin kişisel verilerinin işleniyor olması, tek başına söz konusu kriterin gerçekleştiği ve GDPR'ın sınır ötesi olarak uygulanacağı anlamına gelmemektedir<sup>262</sup>. Kriterin gerçekleşebilmesi için, bahse konu kişisel veri işleme faaliyetinin, AB pazarını hedefleyen bir mal ya da hizmet sunma işlemi ile ilişkili olarak gerçekleştirilmesi gerekmektedir.

GDPR m. 3/2/a'nın uygulanabilmesi için, AB sınırları içerisinde bulunan kişilere yönelik mal ya da hizmet sunma kavramından ne anlaşılması gerektiğinin değerlendirilmesi gerekmektedir. Söz konusu kavram, AB'nin tüketicinin korunması mevzuatından esinlenilerek GDPR'a eklenmiştir<sup>263</sup>. Kavramın özünde anlatmak istediği husus, AB sınırları dışında bulunan kişilerin, AB pazarını hedefleyen ticari faaliyetlerinin de GDPR kapsamında olacağı şeklindedir<sup>264</sup>. Temel olarak sosyal medya, elektronik ticaret ya da dijital hizmetler sunan şirketler, AB sınırları dışında kurulu olmalarına rağmen AB pazarına yönelik mal ya da hizmet sunan kişilerin başında gelmektedirler<sup>265</sup>.

---

<sup>260</sup> Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, s. 36; “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 16; Korff, “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, s. 11.

<sup>261</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 14.

<sup>262</sup> Kuner vd., *The EU General Data Protection Regulation (GDPR)*, s. 88. Bu yönde örnekler için bkz. “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 16; Korff, “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, s. 17.

<sup>263</sup> Kuner vd., *The EU General Data Protection Regulation (GDPR)*, s. 89.

<sup>264</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 13; Gert Vermeulen, Eva Lievens, *Data Protection and Privacy under Pressure*, Antwerp Belgium, Maklu, 2017, s. 86.

<sup>265</sup> Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, s. 36; Örnekler için bkz. “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 8-9.

Özellikle interneti kullanarak mal ya da hizmet satışı yapan kişiler açısından konuya bakıldığında, hangi ülke pazarının hedeflendiğini belirleyebilmek; basitçe anlaşılabilir bir husus değildir<sup>266</sup>. İnternetin tüm dünyadan erişilebilir olduğu göz önüne alındığında, herhangi bir internet sitesinde sunulan hizmetlerin; internete erişimi bulunan tüm insanlarca kullanılabilir olduğu sonucuna varılmaktadır. Bu durumda hangi şartların sağlanması halinde ilgili hizmetlerin ya da malların AB pazarına hitaben sunulmuş kabul edileceğinin belirlenmesi gerekmektedir<sup>267</sup>. EDPB bu şartları AB ya da üye ülkelerden birinin adının kullanılması, AB sınırları içerisinde reklam yapılması, AB'den iletişim kurulması için iletişim kanalları kurulması, alan adlarında AB üye ülkelerinin kodlarının kullanılması, AB para birimleri ile ödeme alınması, AB sınırları içerisine teslimat seçenekleri sunulması ya da AB dillerinin kullanılması gibi örneklerle açıklamıştır<sup>268</sup>.

EDPB, söz konusu kriterlerin her birinin tek tek ya da birlikte olarak bulunmasının, AB'ye yönelik olarak mal ya da hizmet sunumunu ispatlama konusunda yeterli olmadığını da ifade etmektedir<sup>269</sup>. EDPB'ye göre her bir somut olay, kendi şartları içerisinde değerlendirilerek bir sonuca varılması gerekmektedir<sup>270</sup>. Yukarıda sayılan örnekler de bu değerlendirme çerçevesinde üzerinde durulması gereken hususlar olarak sayılmaktadır. Bizim de katıldığımız doktrinde yer alan görüşlere göre, GDPR m. 3/2/a kapsamına girilip girilmediğinin değerlendirilmesi son derece karmaşık ve tahmin edilemez bir durum yaratmaktadır<sup>271</sup>. Dolayısıyla söz konusu kriterin hukuk güvenliği ilkesini zedelediğini söylemek mümkündür. Ancak bu kriter kapsamında değerlendirilecek kişilerin AB ile bağının olmaması ve maddenin esas amacının AB

---

<sup>266</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 14.

<sup>267</sup> Voigt, von dem Bussche, **The EU General Data Protection Regulation A Practical Guide**, s. 27.

<sup>268</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”; Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, s. 37.

<sup>269</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 14.

<sup>270</sup> Korff, “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, s. 17; “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 14.

<sup>271</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 81; Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 97.

makamlarına esneklik sağlayabilmesi göz önüne alındığında, hukuk güvenliği ilkesinin zedelenmesinin önemsenmediği sonucuna da düşüncemizce varılabilecektir.

GDPR’ın gerekçesinde yer alan ifadeler nedeniyle, hedefleme kriterine ilişkin olarak objektif hitap etme ve sübjektif hitap etme olmak üzere iki farklı yaklaşımın bulunabileceği öne sürülmektedir<sup>272</sup>. Söz konusu ifadelere göre veri sorumlusu ya da veri işleyen, AB sınırları içerisinde bulunan veri sahiplerine yönelik olarak mal ya da hizmet sunmayı tasarlaması gerekmektedir<sup>273</sup>. Bu durum, veri sorumlusu ya da veri işleyen sübjektif anlayışına göre mal ve hizmetin yöneltildiği bölgenin neresi olduğunun değerlendirilmesi gerektiği sonucunu doğurmaktadır. Dolayısıyla üçüncü bir kişinin yapacağı objektif değerlendirmenin, bu kapsamda önem arz etmeyeceği anlaşılmaktadır. Kanaatimizce burada objektif ya da sübjektif olarak AB pazarına hitap etme durumlarından en az birinin gerçekleşmesi halinde, GDPR’ın sınır ötesi uygulama kapsamı kazanacağı sonucuna varmak yerinde olacaktır. Zira GDPR’ın sınır ötesi uygulama kapsamına ilişkin kurallarının temel amacı, kişisel verilerin korunması hakkının etkin şekilde tesisini sağlamaktır. Dolayısıyla olabilecek en geniş uygulama kapsamının kabul edilmesi, kanun koyucunun amacına daha uygun düşecektir.

### 3. AB İçerisindeki Bir Kişinin Takip Edilmesi Kriteri

GDPR m. 3/2/b çerçevesinde sınır ötesi uygulama kapsamı öngören bir diğer kriter de AB sınırları içerisinde bulunan gerçek kişilerin yine AB sınırları içerisinde gerçekleşen davranışlarının, AB sınırları dışında bulunan veri işleyenler ya da veri sorumlularınca takip edilmesi olarak belirlenmiştir.

Anılan kriter çerçevesinde değerlendirilmesi gereken en önemli husus, takip etme teriminden ne anlaşılması gerektiğidir<sup>274</sup>. GDPR gerekçesinde, gerçek kişilerin internet üzerindeki davranışlarının çeşitli teknolojilerle takip edilmesinin madde

---

<sup>272</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 90; Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 90.

<sup>273</sup> Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 89.

<sup>274</sup> Özellikle AB merkezli olmayan bankaların müşterilerinin AB’de yaptığı işlemleri takip etmesi bakımından görüş ve değerlendirmeler için bkz. Korff, “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, s. 21.

kapsamına gireceği ifade edilmiştir<sup>275</sup>. Bu çerçevede özellikle kişiler hakkında kararlar almaya ya da kişilerin seçim, tavır ve davranışlarının tahmin edilmesine imkân verecek profillemeye faaliyetlerine de özellikle dikkat çekilmiştir<sup>276</sup>.

Profillemeye kavramı ise GDPR m. 4/4'te, otomatik yollarla kişisel verilerin işlenerek bir gerçek kişinin özellikle işyerindeki performansının, ekonomik durumunun, sağlığının, kişiler tercih ve ilgilerinin, güvenilirliğinin, davranışlarının, konumunun ya da hareketlerinin analizi ya da tahmini olmak üzere çeşitli açılardan değerlendirilmesi olarak tanımlanmıştır.

Profillemeye işlemlerinde kullanılmak üzere kişisel veri toplamaya en elverişli araç, çerez olarak adlandırılan yazılımlardır<sup>277</sup>. Çerezler, internet sitelerinde kullanılmakta olup kişilerin internet sitelerini kullanımlarına ilişkin veri toplanmasına imkân vermektedirler. Her ne kadar çok yaygın kullanılsalar da takip etme kavramının kapsamı, sadece çerezlerin kullanılması vasıtasıyla profillemeye yapılması ile sınırlı değildir<sup>278</sup>. EDPB tarafından verilen diğer örnekler davranış ya da konum bazlı reklam faaliyetleri, güvenlik kameraları ile izleme faaliyeti yapılması, anket ve diğer davranış analizi çalışmaları ya da kişinin sağlık durumunun takibi gibi hususları da kapsamaktadır<sup>279</sup>. EDPB, bu tür örnekler verirken, veri sorumlusunun veri işleme için özel olarak bir niyet gütmesi gerektiğini belirtmiş ve böyle bir niyet olmaması halinde GDPR m. 3/2/b kapsamında bir takip faaliyetinden bahsedilemeyeceğini ifade etmiştir<sup>280</sup>. Dolayısıyla AB sınırları içerisindeki bir kişinin davranışlarının, bu yönde bir niyet olmaksızın takip edilmesi (örneğin, AB ile hiçbir bağlantısı olmayan internet

---

<sup>275</sup> Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 88; Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, s. 38.

<sup>276</sup> Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 88.

<sup>277</sup> Çerezler hakkında detaylı bilgi için bkz. “Çerez Uygulamaları Hakkında Rehber”, **Kişisel Verileri Koruma Kurumu**, 2022, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf>, 11.11.2022.

<sup>278</sup> Diğer örnekler için bkz. Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, s. 39; Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 88.

<sup>279</sup> “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, s. 20.

<sup>280</sup> **a.g.e.**, s. 15.

sitesine, AB sınırları içerisinde birisinin girmesi ve buradaki çerezlerin takip yapmasına izin vermesi durumu<sup>281</sup>), ilgili veri sorumlusunu GDPR'ın sınır ötesi uygulama kapsamına sokmayacaktır<sup>282</sup>.

#### **D. GDPR'ın Sınır Ötesi Uygulama Kurallarının Pratikte Yarattığı Sorunlar**

GDPR'ın genişleyen uygulama alanının AB'de yerleşik kişilerin kişisel verilerinin korunması için bir gereklilik olduğu aksi takdirde Avrupa Birliği İnsan Hakları Şartı ile teminat altına alınan kişisel verilerin korunması hakkına ilişkin taahhütlerin yerine getirilmesinde sorunlar ortaya çıkabileceği ifade edilmektedir<sup>283</sup>. Bununla birlikte GDPR'ın sınır ötesi uygulama kapsamını belirleyen 3 numaralı maddesi, doktrinde çeşitli açılardan eleştirilere konu olmaktadır<sup>284</sup>. Bu eleştirilerden en önemlisi, GDPR'ın teorik olarak çok geniş olan uygulama kapsamının pratikteki sınırlarının kolaylıkla tespit edilememesi sorunudur<sup>285</sup>. Dolayısıyla, özellikle AB sınırları dışında

<sup>281</sup> a.g.e., s. 7.

<sup>282</sup> a.g.e., s. 17; Vermeulen, Lievens, **Data Protection and Privacy under Pressure**, s. 88-90.

<sup>283</sup> Lynskey, **The foundations of EU data protection law**, s. 43; Christopher Kuner vd., "The Extraterritoriality of Data Privacy Laws—an Explosive Issue yet to Detonate", **International Data Privacy Law**, C. 3, S. 3, 2013, s. 147; Mistale Taylor, "The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect", **International Data Privacy Law**, C. 5, S. 4, 2015, s. 255-256.

<sup>284</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 81; Van Alsenoy, **Reconciling the (Extra)Territorial Reach of the GDPR with Public International Law**, s. 97; Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", **International Data Privacy Law**, C. 5, S. 4, 2015, s. 235-236; Beletski, "Critical assessment of the extraterritoriality of the EU General Data Protection Regulation", s. 33; Burri, Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", s. 502. GDPR yaklaşımının uzun dönem bir strateji olarak sürdürülebilir olmadığı yönünde bkz. Oskar Josef Gstrein, Andrej Zwitter, "Extraterritorial Application of the GDPR", **Internet Policy Review** 2021, C. 10, S. 3, 2021, s. 20, (Çevrimiçi) <https://research.rug.nl/en/publications/extraterritorial-application-of-the-gdpr-promoting-european-value>, 18.01.2023; Orla Lynskey, "Extraterritorial Impact in Data Protection Law through an EU Law Lens", **Brexit Institute Working Paper Series**, 2020, s. 15, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3674413](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3674413), 25.09.2020. Kriterlerin net olmadığı ve bu nedenle hukuki belirliliğin sağlanmadığı yönünde bkz. E. J. Kindt, "Why Research May No Longer Be the Same: About the Territorial Scope of the New Data Protection Regulation", **Computer Law & Security Review**, C. 32, S. 5, 2016, s. 746-748. Veri koruma hukukuna ilişkin olarak getirilen geniş uygulama alanı düzenlemelerinin ayrıca kişisel verisi korunan bireylerin diğer temel hak ve özgürlükleri bakımından da önem taşıdığı ve bu dengenin korunması gerektiği yönünde bkz. Maja Brkan, "The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?", **Maastricht Journal of European and Comparative Law**, C. 23, S. 5, 2016, s. 841.

<sup>285</sup> Burri, Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", s. 502.



faaliyet gösteren veri sorumlularının GDPR'a tabi olup olmadıklarını tespit etmelerinde sorunlar ve belirsizlikler yaşanmaktadır. GDPR gibi geniş kapsamlı bir yasal düzenlemeye uyum sağlamanın çok yüksek maliyetleri olabileceği ve organizasyonel açıdan kapsamlı değişiklikleri gerektirebileceği düşünüldüğünde, bu sorunun ticari hayat açısından oldukça kritik olduğu sonucuna varılmaktadır<sup>286</sup>. GDPR'ın yürürlüğe girmesinden sonra yapılan çalışmalarda Avrupa Komisyonu'nun GDPR m. 97 uyarınca yapacağı ilk değerlendirme sürecinde GDPR'ın bölgesel kapsamını dikkatlice incelemesi gerektiği pratikte sağladığı hukuki kesinliğin değerlendirmeye muhtaç olduğu ifade edilmiştir<sup>287</sup>.

GDPR'ın sınır ötesi uygulama kapsamı için yöneltilen diğer bir eleştiri de çok geniş olan uygulama kapsamının, uluslararası hukuk açısından makul görünmemesidir<sup>288</sup>. Bu kapsamdaki detaylı değerlendirmeler aşağıdaki başlıklar altında sunulacaktır.

Sınır ötesi uygulama kapsamı olan her düzenlemede olduğu gibi GDPR'ın da AB sınırları dışında fiilen uygulanması konusunda sorunlar yaşanmaktadır<sup>289</sup>. Daha

---

<sup>286</sup> Burri, Schär, a.y.

<sup>287</sup> Paul de Hert, Michal Czerwinski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context", **International Data Privacy Law**, C. 6, S. 3, 2016, s. 243.

<sup>288</sup> Burri, Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", s. 502. Aynı yönde bkz. Ufuk Dal, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti", **Kişisel Verileri Koruma Dergisi**, C. 1, S. 1, 2019, s. 30; Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 95. GDPR'ın uygulama alanına ilişkin olarak taslak aşamasında getirilen uygulama alanının çok geniş olduğu yönünde eleştiriler için bkz. Svantesson, "Extraterritoriality and Targeting in EU Data Privacy Law", s. 234. Aksi yönde bkz. Dan Jerker B. Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses", **Stanford Journal of International Law**, C. 50, S. 1, 2014, s. 75-102.

<sup>289</sup> Lynskey, "Extraterritorial Impact in Data Protection Law through an EU Law Lens", s. 4. Belirtmek gerekir ki bu sorun sadece kişisel verilerin işlenmesi ve aktarılması ile de sınırlı değildir. Dijital dünyaya ilişkin alınan mahkeme kararları ifade özgürlüğü ve haberleşme özgürlüğü gibi temel hak ve özgürlükleri dengelemek ve noktada uygulama alanını gözetmek durumdadır. Federico Fabbrini, Edoardo Celeste, "The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders", **German Law Journal**, C. 21, S. S1, 2020, s. 62; Cedric Ryngaert, Mistale Taylor, "Symposium on The GDPR And International Law The GDPR as Global Data Protection Regulation?", **AJIL Unbound**, C. 114, 2020, s. 9; Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses", s. 74-102; Omer Tene, "Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation", **Future of Privacy Forum**, 2013, s. 4, (Çevrimiçi) [https://wiki.laquadrature.net/images/5/59/Future\\_of\\_Privacy\\_Forum\\_White\\_Paper\\_on\\_Jurisdiction.pdf](https://wiki.laquadrature.net/images/5/59/Future_of_Privacy_Forum_White_Paper_on_Jurisdiction.pdf), 22.09.2020.

önceki bölümlerde açıklandığı üzere devletlerin uluslararası düzenleme yetkisi çerçevesinde sınır ötesi uygulama kapsamlı bir düzenleme yapmak nispeten kolayken, bu düzenlemeyi fiilen uygulamak çok zor bir işlemdir<sup>290</sup>. Zira bir devletin sınırları dışında fiziki güç kullanması uluslararası hukuk kapsamında imkansıza yakındır<sup>291</sup>. Dolayısıyla GDPR kapsamında bir para cezasının fiilen tahsili, ilgili veri sorumlusunun bulunduğu yabancı ülkede her zaman mümkün olmayabilecektir<sup>292</sup>. Bu durumun da fiili uygulamaya imkân olan ülkeler ile olmayan ülkelerde bulunan veri sorumluları ya da veri işleyenler arasında ayrımcılığa sebep olduğu düşünülmektedir.<sup>293</sup>

GDPR’ın AB dışında fiilen uygulanmasının zorluklarını azaltabilmek adına doktrinde öne sürülen bir görüş, GDPR’ın sadece ciddi seviyedeki ihlallerine GDPR’ın uygulanmasının sağlanmasıdır<sup>294</sup>. Bu görüşün, AB Komisyonu’nun iç hukukların sınır ötesi uygulama kapsamı olması halinde, bu uygulamanın uluslararası hukuka ve milletlerarası nezakete uygun olması gerektiği yönündeki görüşüne<sup>295</sup> de uygun olacağı öne sürülmektedir<sup>296</sup>. Ancak kanaatimizce böyle bir yaklaşım, GDPR’ın teorik

---

<sup>290</sup> ABD merkezli şirketler bakımından uygulama sorununa ilişkin olarak açıklama ve değerlendirme için bkz. Kurt Wimmer, “The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?”, **Communications Lawyer**, 2017, s. 19.

<sup>291</sup> Adele Azzi, “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, C. 9, S. 2, 2018, s. 133.

<sup>292</sup> İsviçre örneği üzerinden GDPR kapsamında para cezalarının uygulanmasına ilişkin olarak bkz. Yaniv Benhamou, “GDPR on the Swiss Territory Cooperation with European Authorities and Enforcement of Monetary Fines”, **Jusletter-it**, 2018, s. 10. ABD’li şirketler üzerinde AB kararlarının uygulanabilirliği hakkında bkz. Kurt Wimmer, “Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers First Amendment Symposium”, **Syracuse Law Review**, C. 68, S. 3, 2018, s. 571-578. Her iki çalışmadan da anlaşıldığı kadarıyla, GDPR kapsamında verilen kararların AB sınırları dışında nasıl uygulanacağı hakkında netlik olmayan bir konudur.

<sup>293</sup> AB dışındaki veri sorumlularının bazılarının uygulanabilirlik kaygısından ziyade repütasyon için GDPR ile uyumlu olmayı önemseydiği yönünde bkz. Benjamin Greze, “The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives”, **International Data Privacy Law**, C. 9, S. 2, 2019, s. 127.

<sup>294</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 95.

<sup>295</sup> Söz konusu görüş, AB Komisyonu tarafından ABD Yüksek Mahkemesinde, Microsoft hakkında görülecek davaya sunulan dilekçe içerisinde ifade edilmiştir. Görüşe erişmek için (Çevrimiçi) bkz. [https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791\\_17-2%20,04.03.2022](https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20,04.03.2022), s. 7.

<sup>296</sup> Kuner vd., **The EU General Data Protection Regulation (GDPR)**, s. 96. Ayrıca uluslararası veri aktarımlarında kişisel bilgiler için yüksek düzeyde koruma sağlamaya yönelik strateji ve ortaklık önerileri hakkında bkz. Joel R. Riedenberg, “Resolving Conflicting International Data Privacy Rules in Cyberspace”, **Stanford Law Review**, C. 52, S. 5, 2000, s. 1362.

ve pratik uygulama kapsamının sınırlarının çizilmesini daha da zorlaştıracak ve belirsizliklerin daha da artmasına sebebiyet verebilecektir.

### **III. KVKK’NIN SINIR ÖTESİ UYGULAMA KAPSAMI**

Daha önceki başlıklarda açıklandığı üzere hem 95/46 sayılı Direktif’te hem de GDPR içerisinde GDPR’ın bölgesel uygulama alanını düzenleyen özel bir madde bulunmasına rağmen, KVKK içerisinde böyle bir madde bulunmamaktadır. Dolayısıyla KVKK’nın sınır ötesi uygulama kapsamı olup olmadığı konusu, GDPR’da olduğu kadar net değildir. Yine de Kişisel Verileri Koruma Kurulu’nun vermiş olduğu kararlarda, KVKK’nın yurtdışında bulunan veri sorumlularına da uygulanacağını kabul edildiği görülmektedir. Ancak kurulun bu kararları dayandığı hukuki gerekçelerin net olmadığı gözlemlenmektedir. Bu çerçevede aşağıdaki başlıklar altında öncelikle kurulun, KVKK’yı yurtdışında bulunan veri sorumlularına uyguladığı kararlar incelenecektir. Daha sonrasında ise uluslararası hukuk kuralları ile TCK’nın yer bakımından uygulama kuralları değerlendirilerek KVKK’nın sınır ötesi uygulama kapsamına sahip olup olmadığı tespit edilmeye çalışılacaktır.

#### **A. KVKK’nın Yurtdışında Bulunan Veri Sorumlularına Uygulandığı Durumlar**

Kişisel verilerin korunması açısından düzenleyici ve denetleyici idari makam, Kişisel Verileri Koruma Kurumu’dur. Bu kurumun karar organı olan Kişisel Verileri Koruma Kurulu, kişisel verilerin korunmasına ilişkin başvuru ve şikayetleri karara bağlayarak, KVKK’nın nasıl uygulanması gerektiği konusunda yol gösterici bir rol oynamaktadır. Kişisel Verileri Koruma Kurumu aynı zamanda çeşitli yönetmelik ve tebliğler de çıkararak KVKK’nın uygulanmasına ilişkin hususları düzenlemektedir. Tüm bu ikincil düzenleme ve kararlar içerisinde, KVKK’nın yurtdışında bulunan veri sorumlularına da uygulanacağını gösteren hükümler bulunmakta olup bu hükümler aşağıda başlıklar halinde incelenecektir.

## 1. Veri Sorumluları Sicili

Veri Sorumluları Sicili Hakkında Yönetmelik<sup>297</sup> m. 5/b, Türkiye’de yerleşik olmayan veri sorumlularının, veri işlemeye başlamadan önce veri sorumlusu temsilcisi marifetiyle Veri Sorumluları Sicili’ne kaydolmalarını zorunlu kılmaktadır. Bu yönetmelik içerisindeki hükümler ile, Türkiye’de yerleşik olmayan veri sorumlularının temsilci ataması gerektiği ve iletişimlerin bu temsilciler üzerinden yapılması gibi konularda düzenlemeler bulunmaktadır. Ayrıca Kişisel Verileri Koruma Kurumu tarafından Veri Sorumluları Sicili’ne kayıt yükümlülüğünün yerine getirilmesi tarihine ilişkin verilen kararlarda da Türkiye’de yerleşik olmayan veri sorumlularının kaydına ilişkin son tarihler belirtilmiştir<sup>298</sup>.

Kişisel Verileri Koruma Kurulu tarafından, yurtdışında yerleşik veri sorumlularının Veri Sorumluları Sicili’ne kaydına ilişkin olarak 2019 ve 2020 yılları içerisinde iki farklı karar yayınlanmıştır. 2019 yılında yayınlanan kararda<sup>299</sup> kurul, yurtdışında yerleşik olup Türkiye’de doğrudan ya da şubeleri aracılığıyla kişisel veri işleme faaliyetinde bulunan tüzel kişilerin, Veri Sorumluları Sicili’ne kaydolması gerektiğini ifade etmiştir. 2020 tarihli kararda<sup>300</sup> ise kurul, veri koruma düzenlemelerinin yer bakımından uygulama alanının belirlenmesinde, bireylere en üst düzeyde ve en geniş kapsamda korumayı sağlayan bir yaklaşım benimsenmesi gerektiğini açıklamıştır.

Veri Sorumluları Sicili’ne kayıt yükümlülüğü, aynı zamanda kayıtlı olan veri sorumlularının, KVKK ve ikincil düzenlemelerinde belirtilen tüm yükümlülüklerle

<sup>297</sup> “Veri Sorumluları Sicili Hakkında Yönetmelik”, Kişisel Verileri Koruma Kurumu, 30.12.2017, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5442/VERI-SORUMLULARI-SICILI-HAKKINDA-YONETMELIK>, 10.02.2021.

<sup>298</sup> Türkiye’de yerleşik olmayan veri sorumlularının VERBİS kaydına ilişkin söz konusu son tarihler hakkında bilgi için bkz. “Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması İle İlgili Kişisel Verileri Koruma Kurulunun 11/03/2021 Tarihli ve 2021/238 Sayılı Kararı”, **Kişisel Verilerin Korunması Kurulu**, 2021.

<sup>299</sup> “Yurtdışında yerleşik Tüzel kişilerin Türkiye’deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulu 2019/225 Sayılı Kararı”, Kişisel Verileri Koruma Kurumu, KVKK, 23.07.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5545/2019-225>, 18.03.2020.

<sup>300</sup> “Ülkemizde temsilciliği bulunan bir yabancı bankanın KVKK kapsamında veri sorumlusu sayılıp sayılmayacağı ve Veri Sorumluları Siciline kayıt yükümlülüğü hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 2020/471 Sayılı Kararı”, Kişisel Verileri Koruma Kurumu, 23.06.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6772/2020-471>, 10.02.2021.

uymak zorunda oldukları sonucunu doğurmaktadır. Dolayısıyla yurtdışında yerleşik veri sorumluları da KVKK ve tüm ikincil düzenlemelerine uymakla yükümlü hale gelmektedir. Bu durum da KVKK'nın sınır ötesi uygulama kapsamına sahip olduğu neticesini ortaya çıkarmaktadır. Ancak söz konusu sınır ötesi uygulama kapsamının sınırları, GDPR'da olduğu gibi nispeten net bir şekilde çizilmemiştir. Kurul kararlarından anlaşıldığı kadarıyla yurtdışında yerleşik kişilerin Türkiye'de gerçekleştirdiği kişisel veri işleme faaliyetleri KVKK kapsamında değerlendirilmelidir ve yer bakımından uygulama alanının belirlenmesinde mümkün olduğunca geniş yorum yapılması gerekmektedir.

## **2. Veri Güvenliği İhlali Bildirimi**

Kişisel Verileri Koruma Kurulu, 2019 yılında verdiği Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Karar<sup>301</sup> ile veri güvenliği ihlallerine ilişkin düzenlemeler yapmıştır. Kişisel veri ihlali, KVKK m. 12'de düzenlenmekte olan bir kavram olup, kişisel verilere üçüncü kişilerin hukuka aykırı olarak erişmesi anlamına gelmektedir<sup>302</sup>. Kamuoyunda özellikle “hacklenme” olarak bilinen olaylar, veri ihlallerinin tipik örneklerini oluşturmaktadır. Bu tür olaylara örnek olarak bir şirketin çalışan bilgilerinin başka bir kişi tarafından çalınması gösterebilecektir.

Kurulun bahse konu kararında, yurtdışında yerleşik olan veri sorumlularının veri ihlallerine ilişkin hangi durumlarda bildirim yapma yükümlülüğü altında olacağına dair kriterler belirlenmiştir. Eğer ihlalin sonuçları, Türkiye'de yerleşik ilgili kişileri (veri sahipleri) etkiliyorsa ve ilgili kişiler de yurtdışında yerleşik olan veri sorumlusu tarafından sunulan ürün ve hizmetlerden Türkiye'de faydalaniyorsa; veri ihlalinin nezdinde gerçekleştiği yurtdışında yerleşik veri sorumlusu, Türkiye'de de veri ihlali

<sup>301</sup> “Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru”, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>, 01.05.2022.

<sup>302</sup> KVKK m.12 için bkz. “6698 Sayılı Kişisel Verilerin Korunması Kanunu”, 07.04.2016, (Çevrimiçi) [mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5](http://mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5).

bildirimi yapmakla yükümlü kılınmıştır. Bu kurallar çerçevesinde de yurtdışında yerleşik veri sorumluları tarafından çok sayıda bildirim yapıldığı görülmektedir<sup>303</sup>.

<sup>303</sup> “Kişisel Verileri Koruma Kurumu Veri İhlali Bildirimleri”, Kişisel Verileri Koruma Kurumu, (Çevrimiçi) <https://kvkk.gov.tr/veri-ihlali-bildirimi/?&page=14>, 10.11.2021; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Industries S.p.A.”, Kişisel Verileri Koruma Kurumu, 27.01.2022, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7165/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Industries-S-p-A->, 22.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – GoDaddy.com, LLC”, Kişisel Verileri Koruma Kurumu, 23.12.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7127/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-GoDaddy-com-LLC-GoDaddy->, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Panasonic Business Support Europe GmbH”, Kişisel Verileri Koruma Kurumu, 07.10.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7060/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Panasonic-Business-Support-Europe-GmbH>, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Subway International B.V.”, Kişisel Verileri Koruma Kurumu, 18.08.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7039/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Subway-International-B-V->, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Pied Piper Fansub (piedpiperfb.com)”, Kişisel Verileri Koruma Kurumu, 18.08.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7040/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pied-Piper-Fansub-piedpiperfb-com->, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Motor Trend Group LLC”, Kişisel Verileri Koruma Kurumu, 03.08.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7024/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Motor-Trend-Group-LLC>, 10.02.2022; “Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 18.09.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5534/2019-269>, 18.03.2020; “Dubsmash Inc. hakkında Kişisel Verileri Koruma Kurulunun 17/07/2019 Tarihli ve 2019/222 Sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 17.07.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5523/-Dubsmash-Inc-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-17-07-2019-Tarihli-ve-2019-222-Sayili-Karari-Ozeti>, 18.03.2020; “Cathay Pasific Airway Limited hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/144 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 16.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5480/2019-144>, 18.03.2020; “Facebook hakkında Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 11.04.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5481/2019-104>, 18.03.2020; “Marriott International Inc. hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 16.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5479/2019-143>, 18.03.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – ClearVoiceResearch.com, LLC”, Kişisel Verileri Koruma Kurumu, 04.05.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6964/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-ClearVoiceResearch-com-LLC>, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Air India Limited”, Kişisel Verileri Koruma Kurumu, 01.04.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6942/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Air-India-Limited>, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Acer Sales International SA”, Kişisel Verileri Koruma Kurumu, 18.03.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6908/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Acer-Sales-International-SA>, 10.02.2022; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – UiPath SRL”, Kişisel Verileri Koruma Kurumu, 22.12.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6848/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-UiPath-SRL>, 10.02.2021; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co.”, Kişisel Verileri Koruma Kurumu, 27.10.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6829/Hanon-Automotive-Climate-Sys-Manufacturing-Industrial-and-Commercial-Co->, 10.02.2021; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Fluke Corporation ve Fluke Electronics Corporation”, Kişisel Verileri Koruma Kurumu, 16.07.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6775/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Fluke-Corporation-ve-Fluke-Electronics-Corporation>, 22.10.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) – EasyJet Plc”, Kişisel Verileri Koruma Kurumu, 28.05.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6744/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-EasyJet-Plc>, 18.03.2021; “Kamuoyu Duyurusu (Veri İhlali Bildirimi, 2020) – Microsoft Corporation”, Kişisel Verileri Koruma Kurumu, 04.02.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6670/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation>,

## **B. TCK'nın Yer Bakımından Uygulama Kuralları Çerçevesinde KVKK'nın Sınır Ötesi Uygulama Kapsamına Sahip Olma İmkânı**

KVKK m. 17 ve 18, kişisel verilerin işlenmesine ilişkin suç ve kabahatleri belirlemektedir. Dolayısıyla KVKK'nın yaptırımlarının bölgesel uygulama alanı açısından, TCK ve Kabahatler Kanunu'nun bu konuya ilişkin hükümleri uygulanmaktadır<sup>304</sup>. Aşağıda da açıklanacağı üzere TCK ve Kabahatler Kanunu'nun bölgesel uygulama maddeleri, bu kanunların Türkiye Cumhuriyeti sınırları dışındaki kişi ve fiillere de uygulanabilmesine imkân vermektedir. Dolayısıyla değerlendirilmesi gereken konu, KVKK'daki yaptırım maddelerinden yola çıkarak, KVKK'nın TCK ve Kabahatler Kanunu çerçevesinde sınır ötesi uygulama kapsamına sahip olup olamayacağıdır.

Kabahatler Kanunu m. 3, bu kanunun idari para cezaları açısından genel kanun niteliğinde olduğunu ifade etmektedir. Dolayısıyla KVKK m. 18'de düzenlenen idari para cezaları açısından Kabahatler Kanunu genel kanun olarak uygulanmaktadır. Kabahatler Kanunu m. 6 ise kanunlarda aksine hüküm bulunmadıkça, TCK m. 8'in de Kabahatler Kanunu'nun yer bakımından uygulanması konusunda uygulanacağını hüküm altına almaktadır. Dolayısıyla KVKK'daki idari para cezalarının yer bakımından uygulanması açısından da TCK m. 8 uygulama alanı bulacaktır. Ancak vatandaş ve yabancı tarafından işlenen suçlara ilişkin uygulama alanının sınırlarını

---

18.03.2021; “<https://kvkk.gov.tr/Icerik/5533/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim-Zynga-Game-Ireland-Limited>”, Kişisel Verileri Koruma Kurumu, 26.09.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5533/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim-Zynga-Game-Ireland-Limited>, 18.03.2021; “Kamuoyu Duyurusu (Veri İhlali Bildirimi, 2019) – Microsoft Corporation”, Kişisel Verileri Koruma Kurumu, 10.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5451/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim-Microsoft-Corporation>, 18.03.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) - ANIMOTO Inc. (Animoto)”, Kişisel Verileri Koruma Kurumu, 24.01.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5349/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim->, 18.03.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Marriott International, Inc.”, Kişisel Verileri Koruma Kurumu, 05.12.2018, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5322/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim->, 18.03.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Ticketmaster UK”, Kişisel Verileri Koruma Kurumu, 29.06.2018, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5244/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim->, 18.03.2020; “Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Cathay Pacific Airways Limited”, Kişisel Verileri Koruma Kurumu, 30.10.2018, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5297/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirim->, 18.03.2020.

<sup>304</sup> Söz konusu hükümlere KVKK'nın “Suçlar ve Kabahatler” başlıklı beşinci bölümünden ulaşabilirsiniz, bilgi için bkz. “6698 sayılı Kanun”.

izen TCK m. 11 ve 12, Kabahatler Kanunu m. 6'nın sadece TCK m. 8'e atıf yapması nedeniyle KVKK'da yer alan idari para cezaları aısından uygulanamayacaktır.

TCK m. 8 gereęi Trkiye'de iřlenen sular hakkında Trk kanunları uygulanmaktadır. Bu kural, mlkillik esası gereęi Trk devletinin egemen olduęu tm yerleri (yani kara, deniz ve hava lkeleri ile Trk bayraęı olan hava ve deniz araları) kapsamaktadır. Kabahatler Kanunu'nda yer alan atıf nedeniyle KVKK'da yer alan kabahatlerin de Trkiye'de iřlenmesi halinde Trk kanunları uygulanacaktır. Ancak bu kural, sınır tesi uygulama kapsamıyla ilgili olmadıęı iin alıřmamız kapsamı dıřında kalmaktadır. Ancak devletlerin uluslararası dzenleme yetkisine iliřkin olarak birinci blmde aıklanan msamahakr ilkeler, TCK maddeleri ierisinde kendilerine yer bulmuř durumdadır. Bu erevede aktif kiřilik ilkesi TCK m. 10 ve 11'de, pasif kiřilik ilkesi TCK m. 12/2'de, koruma ilkesi TCK m. 12/1 ve 13/1-b'de, evrensellik ilkesi ise TCK m. 13'te Trk hukukundaki yansımalarını bulmaktadır. İřte bu nedenle ayrı bir bařlık altında ayrıca uluslararası hukuk kuralları erevesinde KVKK'nın sınır tesi uygulama kapsamı zerinde durulmayacaktır. Zira kanun koyucu TCK ierisinde, uluslararası hukukta yer alan msamahakr ilkelerin lkemizce hangi durumlarda ne kapsamda uygulanacaęını zaten dzenlemiř durumdadır. Yrtme ve yargı organlarının da bu ereve dıřına ıkması mmkn olmadıęı iin KVKK'nın da TCK'dan baęımsız olarak msamahakr ilkeler erevesinde sınır tesi uygulama kapsamına sahip olup olmayacaęının deęerlendirilmesi beyhude olacaktır.

KVKK m. 18'de yer alan kabahatler aydınlatma ykmllęnn yerine getirilmemesi, veri gvenlięine iliřkin ykmllklerin yerine getirilmemesi, Kiřisel Verileri Koruma Kurulu tarafından verilen kararların yerine getirilmemesi ve Veri Sorumluları Sicili'ne bildirim ve kayıt ykmllęnn yerine getirilmemesi řeklindedir. Tm bu aıklamalardan anlařılan, kabahatlerin icrai davranıřlarla deęil, ihmali davranıřlarla iřlenebileceęidir. Yani KVKK'nın kabahat olarak kabul ettięi hususlar, veri sorumlularının gerekleřtirmeleri gereken fiilleri gerekleřtirmemeleri zerine kurgulanmıřtır.



TCK m. 8/1'in ikinci cümlesi, TCK'ya ve dolayısıyla idari yaptırımlar açısından KVKK'ya sınır ötesi uygulama kapsamı getirebileceği için çalışmamız açısından önem taşımaktadır. Bu cümleye göre, suç teşkil eden fiilin kısmen ya da tamamen Türkiye'de işlenmesi ya da neticenin Türkiye'de gerçekleşmesi gerekmektedir. Anılan cümleden aynı zamanda anlaşılan, bazı durumlarda fiillerin bir kısmının yurtdışında gerçekleşmiş olması veya fiilin tamamen yurtdışında gerçekleşmiş olması hallerinde dahi TCK'nın uygulanabileceğidir<sup>305</sup>. Dolayısıyla bu cümle çerçevesinde TCK'nın ve yukarıda açıklandığı şekilde buna bağlı olarak da KVKK'nın idari para cezaları açısından sınır ötesi uygulama kapsamının mevcut olduğu sonucuna varılabilecektir.

Daha önce de açıklandığı üzere KVKK'da düzenlenen idari para cezaları, ihmali davranışlarla işlenebilen kabahatlere ilişkindir. Bir başka deyişle, kabahatlerin işlenebilmesi için bazı fiillerin gerçekleştirilmesi değil; gerçekleştirilmemesi gerekmektedir. TCK m. 8'in ikinci cümlesinde yer alan fiilin kısmen ya da tamamen Türkiye'de gerçekleşmesi kriteri, KVKK'daki kabahatler bakımından herhangi bir anlam ifade etmemektedir. Ancak TCK m. 8'in ikinci cümlesinde yer alan neticenin Türkiye'de gerçekleşmesi kuralı, KVKK'daki kabahatlerin sınır ötesi uygulama kapsamına sahip olmalarına kanaatimizce imkân vermektedir. Zira KVKK'nın amacı, KVKK m. 1'de de belirtildiği üzere başta özel hayatın gizliliği hakkı olmak üzere kişilerin temel hak ve özgürlüklerini korumaktır. KVKK'da yer alan kabahatlerin işlenmesi halinde aynı zamanda Türkiye'de bulunan kişilerin temel hak ve özgürlükleri zedelenmiş olacaktır. Bu durumun sonucu olarak da ilgili kabahatin neticesi Türkiye'de doğmuş olacaktır<sup>306</sup>.

---

<sup>305</sup> Sinem Göçmen Uyarer, "6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 5237 sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", 2019, s. 139-209, (Çevrimiçi) <https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>, 24.05.2020.

<sup>306</sup> Aydınlatma yükümlülüğünün ihlali ve veri güvenliğini sağlama yükümlülüğünün ihlali açısından bahse konu ifade oldukça nettir. Ancak Veri Sorumluları Sicili'ne kaydolmamanın nasıl Türkiye'de bulunan kişilerin haklarını zedelediği akla gelebilecek bir sorudur. Veri Sorumluları Sicili'ne kaydolmama ile birlikte Türkiye'de bulunan kişilerin, kişisel verileri ile ilgili olarak edinebilecekleri bilgiler azalmış olmakta ve dolayısıyla netice Türkiye'de gerçekleşmiş olmaktadır. Yine Türkiye'deki bir sicil kaydı eksik kaldığı için neticenin Türkiye'de gerçekleştiğini söylemek kanaatimizce mümkün olacaktır. Kurul kararlarına aykırılıklarda da yine Kurul kararının amacının Türkiye'de bulunan kişilerin haklarının korunması olacağı göz önüne alındığında, aynı şekilde değerlendirilmeleri gerekmektedir.

Yukarıdaki açıklamalar ışığında, KVKK’da düzenlenen kabahatlere ilişkin kuralların sınır ötesi uygulama kapsamına bağlı olarak yabancı ülkelerde bulunan veri sorumlularına da uygulanabileceği sonucuna varılabilmektedir. Ancak kabahatlerin sınır ötesi uygulama kapsamının tüm KVKK’ya da sınır ötesi uygulama kapsamı kazandırıp kazandırmayacağı sorusunun da netleştirilmesi gerekmektedir. KVKK’da düzenlenen aydınlatma yükümlülüğünün yerine getirilmemesi, Veri Sorumluları Sicili’ne kayıt olunmaması ya da kurul kararlarına uyulmamasına ilişkin kabahatler, KVKK’nın belirli maddelerine (ya da özel bir kurul kararına) ilişkindir. Dolayısıyla bu maddelere ilişkin kabahatlerin, KVKK’nın bütününe sınır ötesi uygulama kapsamı kazandırması kanaatimizce mümkün olmayacaktır.

Diğer yandan, KVKK m. 18/b maddesi, KVKK m. 12’de yer alan veri güvenliğine ilişkin yükümlülüklerle atıf yapmaktadır. Veri güvenliğine ilişkin yükümlülüklerden birisi de KVKK m. 12/1/a’da yer alan kişisel verilerin hukuka aykırı olarak işlenmesini engellemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almaktır. Bu yükümlülükten, veri sorumlusunun kişisel verilerin hukuka uygun şekilde işlenmesini sağlaması gerektiği anlaşılmaktadır. Kişisel verilerin Türk hukukuna uygun olarak işlenebilmesi için, veri sorumlusunun başta KVKK olmak üzere kişisel verilerle ilgili her türlü mevzuata uygun hareket etmesi gerekmektedir. Yani söz konusu hukuka aykırı işlenmeyi engelleme yükümlülüğü içerisinde “hukuk” ifadesinden kasıt Türk hukuku ise KVKK dahil kişisel verilere ilişkin tüm mevzuatımızın sınır ötesi uygulama kapsamı olacaktır. Eğer burada kullanılan “hukuk” tabiri, veri sorumlusunun tabi olduğu yabancı hukukları<sup>307</sup> da kapsıyorsa, bu durumda KVKK dahil kişisel verilere ilişkin tüm mevzuatımızın sınır ötesi uygulama kapsamı olmayacaktır. Kanaatimizce bahse konu maddede yer alan “hukuk” ifadesi, Türk hukukunu kastetmektedir. Zira KVKK’nın amacı Türkiye sınırları içerisinde Türk Anayasası ile güvenceye alınan temel hak ve özgürlükleri

---

<sup>307</sup> Önemle belirtmek gerekir ki Kıta Avrupası Hukuk Sistemine dahil olan Türk Hukuku, milletlerarası özel hukuk çerçevesinde yabancı hukukları, bir hukuk sistemi olarak kabul etmekte ve hâkimin bu hukukları da bildiğini varsaymaktadır. Ancak Anglo-Sakson Hukuk Sistemine dahil olan ülke hukuklarında yabancı hukuk, ispatlanması gereken bir vakıa olarak kabul edilmektedir. Dolayısıyla söz konusu ifadenin veri sorumlusunun bulunduğu ülkede geçerli hukuk sistemi kastetmesi de teorik olarak mümkündür.

korumaktır. Dolayısıyla veri sorumlusunun yabancı bir hukuka uygun kişisel veri işleme faaliyetlerinin, Türk hukukunun Türkiye’deki kişilere sağladığı hak ve özgürlüklerle eşdeğer bir koruma sağlayacağını varsaymak uygun olmayacaktır. Türkiye’deki kişilerin hak ve özgürlüklerinin Türk Anayasası’na ve kanunlarına uygun şekilde korunabildiğinden emin olmak adına söz konusu “hukuk” ifadesinin Türk hukuku olduğunu kabul etmek, kanaatimizce en doğru yaklaşım olacaktır.

Üzerinde durulması gereken bir diğer konu da bu başlık altında yer alan açıklamaların tamamının, devletlerin uluslararası düzenleme yetkisine ilişkin olduğudur. Yani burada sadece hukuki düzenlemelerin sınır ötesi uygulama kapsamı üzerine değerlendirmeler yapılmıştır. Ancak bu kanunlara ilişkin devletlerin sınır ötesi uygulama yetkisi, birinci bölümde de açıklandığı üzere sadece ülke içerisinde geçerli olacak şekilde sınırlı kalmaya devam etmektedir. Örneğin Veri Sorumluları Sicili’ne kaydolmama bir kabahat olarak sınır ötesi uygulama kapsamına sahip şekilde düzenlenmiş olmasına rağmen, bu yükümlülüğe aykırılığın yaptırımını teşkil eden idari para cezasının tahsili yine Türkiye Cumhuriyeti ülkesi dışında Türk devletinin uygulama gücüyle mümkün olmayacaktır.

### **C. KVKK’nın Sınır Ötesi Uygulama Kapsamına Dair Değerlendirmeler**

Daha önceki başlıklarda da detaylıca açıklandığı üzere KVKK’nın sınır ötesi uygulama kapsamına sahip olup olmadığı konusunda hukukumuzda bir netlik bulunmamaktadır. Doktrinde de öne sürülen ve bizim de katıldığımız görüşe göre KVKK’nın yer bakımından uygulama kapsamını düzenleyen kurallarının açıkça kanun metnine eklenmesi yerinde olacaktır<sup>308</sup>. Böylelikle konuya ilişkin mevcut belirsizliklerin giderilebilecektir.

Değerlendirilmesi gereken bir diğer husus da KVKK’da sınır ötesi uygulama kapsamına ilişkin herhangi bir hüküm olmamasına rağmen Kişisel Verileri Koruma Kurulu tarafından çıkarılan yönetmelik ve kararlarla yurtdışında bulunan veri sorumluları için yükümlülükler getirilip getirilemeyeceğidir. Doktrinde de ifade

---

<sup>308</sup> Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, s. 35.

edildiği üzere, yer bakımından uygulama kuralları mevcut olmadığında, mülkilik esası gereği KVKK'nın Türk hukukunun uygulandığı her yerde uygulanacağı sonucuna varılmaktadır<sup>309</sup>. Bu durum da yabancı bir ülkede bulunan kişilerin KVKK veya buna dayalı ikincil düzenlemeler ile bağlanamayacağı sonucunu doğurmaktadır. Bu yorum ve düşünce kanaatimizce yerinde değildir. Şöyle ki TCK ve Kabahatler Kanunu çerçevesinde düzenlenen KVKK'daki idari yaptırımlara ilişkin sınır ötesi uygulama kapsamı yaratan kurallar, fikrimizce KVKK'nın tamamına sınır ötesi uygulama imkânı vermektedir. Dolayısıyla kurul da bu kapsama dayanarak yurtdışında bulunan kişiler için de geçerli olabilecek yönetmelik ve kararlar çıkarabilecektir. Yine de hukuki belirlilik ilkesinin temini adına KVKK'ya da yer bakımından uygulama alanını gösteren maddelerin eklenmesinin uygun olacağı düşünülmektedir.

#### **IV. KVKK'NIN VE GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMI İLE MİLLETLERARASI ÖZEL HUKUK İLİŞKİSİ**

KVKK ve GDPR gibi düzenlemeler çerçevesinde bulunan sınır ötesi uygulama kapsamı kuralları, devletlerin uluslararası düzenleme yetkilerini sınır ötesi uygulama kapsamı ile kullanmalarının birer örneklerini teşkil etmektedirler. Dolayısıyla burada düzenlemeyi yapan devletler, diğer devletlerin rızasını dikkate almaksızın kendi uluslararası yetkilerini kullanmaktadırlar.

Milletlerarası özel hukuk kuralları ise devletlerin kendi rızaları ile yabancı hukukların kendi ülkeleri içerisinde uygulanmalarını sağlayan kurallardır<sup>310</sup>. Kimi ülkelerde kişisel verilerin korunmasına ilişkin olarak da milletlerarası özel hukuk kurallarının yürürlükte bulunduğu gözlemlenmektedir. Örneğin MÖHUK m. 35/3, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere uygulanacak hukuku tespit etmektedir<sup>311</sup>.

---

<sup>309</sup> Çekin, **a.g.e.**, s. 33.

<sup>310</sup> Türk mevzuatına konu edilen milletlerarası özel hukuk kuralları için bkz. 5718 Sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun.

<sup>311</sup> Milletlerarası özel hukukumuzda kişisel verilerin korunması hakkında detaylı bilgi için bkz. Ayşe Yasemin Aydoğmuş Gisoldi, **Milletlerarası Özel Hukukta Kişisel Verilerin Korunması**, 1. bs, İstanbul, On İki Levha Yayıncılık, 2022, s. 191.

Benzer bir hüküm, İsviçre Federal Milletlerarası Özel Hukuk Kanunu m. 139<sup>312</sup>, da ve Çin Milletlerarası Özel Hukuk Kanunu m. 46<sup>313</sup>, da yer almaktadır. Önemle belirtmek gerekir ki bu kurallar, sadece kişisel verilerin korunması hakkının ihlali sebebiyle meydana gelen haksız fiillere ilişkin talepleri kapsamaktadır.

Öte yandan Roma II Tüzüğü<sup>314</sup>, m. 1/1/g ile özel hayatın gizliliğine ilişkin olarak, sözleşme harici borç kaynaklarından doğan tüm taleplerin; Regülasyon kapsamı dışında olduğunu ifade etmiştir<sup>315</sup>. Özel hayatın gizliliği hakkının, kişisel verilerin korunmasını hakkını da kapsadığı AB doktrininde ve yargı kararlarında kabul edilmektedir<sup>316</sup>. Almanya ve Fransa milletlerarası özel hukuk mevzuatında da MÖHUK m. 35/3 benzeri bir hükme yer verilmemektedir. Bu açıklamalardan da anlaşılacağı üzere GDPR'ın<sup>317</sup> geçerli olduğu AB ülkelerinin milletlerarası özel hukuk kuralları içerisinde kişisel verilere ilişkin milletlerarası özel hukuk kuralları bulunmamaktadır. Bir başka deyişle, söz konusu ülkelerde kişisel verilerin korunmasına ilişkin uyumsuzluklarda yabancılık unsuru uygulanacak hukukun tespitinde dikkate alınmamaktadır.

Kişisel verilerin korunmasına ilişkin milletlerarası özel hukuk kuralları açısından AB ülkeleri ile AB dışındaki ülkeler arasındaki bu farklılığın temel sebebi, kanaatimizce kişisel verilerin korunmasına dair düzenlemelerin niteliği ile ilgilidir. AB dışındaki ülkeler, ağırlıklı olarak kamu hukuku nitelikli kişisel verilerin korunması kanunları ile ülke içerisinde kişisel verilerin korunması konusunu düzenlemeye çalışmaktadırlar.

---

<sup>312</sup> İlgili hüküm için bkz. "Swiss Federal Act on Private International Law", (1989), (Çevrimiçi) [https://www.fedlex.admin.ch/eli/cc/1988/1776\\_1776\\_1776/en](https://www.fedlex.admin.ch/eli/cc/1988/1776_1776_1776/en), 12.12.2021.

<sup>313</sup> Zhengxin Huo, "Highlights of China's New Private International Law Act: From the Perspective of Comparative Law", 2011, (Çevrimiçi) [https://ssl.editionsthemis.com/uploaded/revue/article/5973\\_45-3%20Huo.pdf](https://ssl.editionsthemis.com/uploaded/revue/article/5973_45-3%20Huo.pdf), 18.03.2020.

<sup>314</sup> Roma II Tüzüğü hakkında detaylı bilgi için bkz. Adrian Briggs, **The Conflict of Laws**, 3. bs, Oxford, United Kingdom, Oxford University Press, 2013, s. 266-292.

<sup>315</sup> Briggs, **a.g.e.**, s. 264.

<sup>316</sup> Brkan, "Data Protection and Conflict-of-Laws", s. 331.

<sup>317</sup> Önemle belirtmek gerekir ki GDPR öncesinde yürürlükte bulunan 95/46 sayılı Direktif içerisinde uygulanacak hukuka ilişkin hükümlere yer verilmiştir. Zira söz konusu düzenlemenin geçerli olabilmesi için, GDPR aksine, her AB üyesi ülke içerisinde ayrı bir kanun çıkarılarak yürürlüğe konması gerekmektedir. Böylelikle her AB üye ülkesi içerisinde farklı bir kanun olacağı için doğabilecek kanunlar ihtilafı sorunları, Direktif içerisine eklenen m. 4 ile hangi durumlarda hangi üye ülke hukukunun uygulanacağını belirlenmesi suretiyle çözülmeye çalışılmıştır.

Her ne kadar bu tür kanunlar genellikle özel hukuka ilişkin talep haklarını da içermekteyse de söz konusu devletler kişisel verilerin korunmasına dair özel hukuk taleplerinde de yabancılık unsurunu dikkate alarak, milletlerarası özel hukuk kuralları vasıtasıyla ilgili uyuşmazlığa uygulanacak hukukun tespit edilmesine de izin vermektedirler. Buna karşılık AB içerisinde tüm üye ülkelerde uygulanan tek bir düzenleme olan GDPR, üye ülkeler içerisinde yabancılık unsurunu dikkate almaya ihtiyaç duymamaktadır. Zira GDPR tüm üye ülkelerin zaten ortak kanunudur. AB dışı ülkelere ilişkin yabancılık unsuru da GDPR’da dikkate alınmamakta; bölgesel uygulamaya ilişkin kurallar vasıtasıyla GDPR’ın uygulanacağı durumlar tek taraflı olarak belirlenmektedir. Üstelik bu belirleme, kamu hukuku ya da özel hukuk ayrımı yapmaksızın GDPR’ın getirdiği tüm kuralları kapsamaktadır.

Yukarıdaki duruma örnek vermek gerekirse, Türkiye’de bulunan bir Türk vatandaşının kişisel verilerinin işlenmesi nedeniyle İrlanda’da bulunan bir veri sorumlusu tarafından zarara uğratılması ve olayın Türk mahkemelerine intikal etmesi halinde; Türk mahkemesi tarafından öncelikle MÖHUK m. 35/3’e göre ilgili uyuşmazlığa uygulanacak hukuk tespit edilecek ve akabinde bu hukuka göre uyuşmazlık çözümlenecektir. Eğer konu İrlanda mahkemelerine intikal ederse, GDPR m. 3 çerçevesinde zarar veren veri sorumlusunun AB sınırları içerisinde bulunması nedeniyle konu direkt olarak GDPR hükümlerine göre çözümlenecektir. Dolayısıyla İrlanda mahkemeleri olaydaki yabancılık unsurunu dikkate almayacak ve buna bağlı olarak uygulanacak hukuku araştırmayacaktır.

Kişisel verilerin korunmasına ilişkin milletlerarası hukuk kuralları ile kişisel verilerin korunmasına ilişkin düzenlemelerin bölgesel uygulama alanını belirleyen kuralların ikinci farklılığı, kamu hukukuna ilişkin kuralların uygulama alanının tespiti bakımından gündeme gelmektedir. Söz konusu kamu hukukuna ilişkin kurallara GDPR’da veya KVKK’da yer alan aydınlatma yapma ve açık rıza alma, veri güvenliğinin sağlanması ya da verilerin imhasına ilişkin düzenlemeler örnek gösterilebilmektedir. Kişisel verilerin korunmasına ilişkin kamu hukuku niteliğindeki kurallara uyum sağlanması, son derece pahalı olup birkaç yıllık uyum çalışmaları

neticesinde mümkün olabilecek bir husustur<sup>318</sup>. Milletlerarası özel hukuk kuralları da uygulanacak hukukun bir bütün olarak uygulanmasını kabul etmektedir. Örneğin MÖHUK m. 35/3, kişisel verileri hakkında bilgi edinme hakkının sınırlandırılması ile kişilik hakkının ihlalden bahsetmektedir<sup>319</sup>. Bu durumda kişisel veriler hakkında bilgi edinme hakkının kapsamı, kanaatimizce aynı madde gereği uygulanacak olan hukuka göre belirlenmelidir. Dolayısıyla o hukukun bilgi edinme hakkına ilişkin kamu hukuku niteliğindeki kuralları, bu uyumsuzluk çerçevesinde de uygulama alanı bulacaktır. Ancak kişisel verilerin korunmasına ilişkin hukuki düzenlemesi bulunmayan bir ülkede bulunan bir kişinin taraf olduğu uyumsuzluk, böyle bir milletlerarası özel hukuk kuralı vasıtasıyla GDPR'ı içeren bir AB ülkesi hukukuna tabi olursa; zarar veren kişi, uyum sağlaması esasında gerekmeyen ve uyum maliyeti milyonlarca avroyu bulabilen GDPR'a uyum sağlamadığı için tazminat ödemek zorunda kalabilecektir. Zira GDPR'ın sağladığı kişisel verilere ilişkin bilgi edinme haklarının kapsamı çok geniş olmasına rağmen, kişisel verilerin korunmasına ilişkin bir düzenleme bulunmayan ülkede söz konusu hakkın varlığından dahi bahsedilemeyecektir.

Kanaatimizce yukarıda açıklanan durum, teknolojinin ve yabancılık unsuru içeren ilişkilerinin günümüzdeki yaygınlaşma seviyesinin yarattığı ihtiyaçları karşılamaktan uzaktır. Zira MÖHUK m. 35/3 gibi milletlerarası özel hukuk kuralları, teorik olarak veri işleme faaliyeti gösteren kişilerin dünyadaki tüm kişisel verilerin korunması kurallarına (kamu hukuku kuralları da dahil), kişisel uyumsuzluklar özelinde uyum sağlamalarını gerektirebilecektir. Böyle bir durum hem çok ağır maddi külfetler yaratacak hem de bu kanunların birbirleriyle çelişme ihtimallerinden dolayı fiilen imkânsız olacaktır. Dolayısıyla, kanaatimizce AB tarafından GDPR vasıtasıyla benimsenen bölgesel uygulama kuralları düzeni, MÖHUK m. 35/3 gibi kurallara

---

<sup>318</sup> Söz konusu uyum sürecinin kolaylaştırılması adına Kişisel Verileri Koruma Kurumu tarafından birçok duyuru, rehber ve doküman kurumun resmi internet sitesi üzerinden yayınlanmıştır. Bilgi için bkz. <https://www.kvkk.gov.tr/Icerik/6554/Kisisel-Verilerin-Korunmasi-Kanunu-Uyum-Surecine-Iliskin-Duyuru>.

<sup>319</sup> MÖHUK m.35 şu şekildedir: “(1) Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlalden doğan taleplere, zarar görenin seçimine göre; (...) uygulanır. (...) (3) Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere de uygulanır.”

kıyasen daha yerinde bir yaklaşım teşkil etmektedir. Bu nedenle KVKK'ya bölgesel uygulama kapsamı kuralları eklenmesinin ve MÖHUK m. 35/3'ün mülgasının yerinde olacağı düşünülmektedir.

## **V. KVKK'NIN VE GDPR'IN SINIR ÖTESİ UYGULAMA KAPSAMININ DEVLETLERİN ULUSLARARASI YETKİSİ AÇISINDAN DEĞERLENDİRİLMESİ**

KVKK ve GDPR'ın sınır ötesi uygulama kapsamına sahip olmaları, aynı zamanda bu düzenlemeleri yapan devletlerin (ya da devlet topluluklarının) de uluslararası yetkilerini sınır ötesi olarak kullandığını göstermektedirler. Dolayısıyla yapılan düzenlemelerin, uluslararası yetkinin kullanımına ilişkin uluslararası hukuk kuralları açısından uygun olup olmadığının değerlendirilmesine ihtiyaç bulunmaktadır.

Daha önceki bölümlerde açıklandığı üzere, sınır ötesi düzenleme yetkisinin kullanımı uluslararası teamül hukukunda kural olarak yasaktır. Ancak müsamahakâr ilkeler kapsamında değerlendirilen durumların varlığı halinde, istisnai olarak sınır ötesi uygulama kapsamına sahip düzenlemeler; aynı zamanda uluslararası hukuka da uygun kabul edilmektedir. Müsamahakâr ilkeler; devletlerin vatandaşlarına kurallar koymasına imkân veren aktif kişilik ilkesi, devletlerin kendi vatandaşlarını korumak amacıyla yabancılara kurallar koymasını mümkün kılan pasif kişilik ilkesi, devletin kendi egemenlik ve bağımsızlığını korumak için kurallar koymasına izin veren koruma ilkesi ve insanlığa karşı suçların engellenmesi adına devletin kural koyabildiği evrensellik ilkesi olarak dört adet ilkedен oluşmaktadır.

Açıklanan bu ilkelere aktif kişilik ilkesi, koruma ilkesi ve evrensellik ilkesi nitelikleri itibarıyla KVKK ve GDPR'ın içeriği ya da sınır ötesi uygulama kapsamı kuralları ile ilgili değildir. Her ne kadar ülke dışından ilgili ülkelere hizmet sunan bir Türk ya da AB üye ülkesi vatandaşının da söz konusu düzenlemelere tabi olması söz konusu olursa da buradaki uygulamayı belirleyen kriter, söz konusu kişilerin vatandaşlıkları değil; bulundukları konumlarıdır. Dolayısıyla aktif kişilik ilkesinin uygulama alanı bulunduğu bahsetmek de mümkün değildir.



Pasif kişilik ilkesinin, GDPR ile KVKK'nın sınır ötesi uygulama kapsamına sahip olmasının dayanağını teşkil edebilecek nitelikte olduğu düşünülmektedir. Zira bu düzenlemelerle, ülke dışından fiillerde bulunan kişilerin, ilgili devlet vatandaşlarının temel hak ve özgürlüklerine müdahale etmeleri söz konusu olmaktadır. Dolayısıyla ilgili devletlerin kendi vatandaşlarının temel hak ve özgürlüklerini korumak adına düzenlemeler yapmaları, uluslararası hukuk çerçevesinde uygun kabul edilebilecek niteliktedir.

Öte yandan belirtmek gerekir ki, KVKK ve GDPR sadece ilgili devletlerin vatandaşlarının haklarını koruyan düzenlemeler değildir. Bunlar, ilgili ülkelerde bulunan tüm kişilerin temel hak ve özgürlüklerini korumaktadırlar. Örneğin AB'de yerleşik olan bir Türk vatandaşı, GDPR'ın sağladığı hak ve korumalardan da yararlanabilmektedir. O halde pasif kişilik ilkesinin, tek başına bahse konu düzenlemelerin uluslararası hukuka uygunluğunu gösteremeyeceği sonucuna varılmaktadır. Ancak anılan koruma kapsamı, uluslararası yetkinin ülke içerisinde kullanımı olarak kabul edilen objektif mülkilik ilkesi (yani etki doktrini) içerisinde değerlendirilebilecek niteliktedir. Objektif mülkilik ilkesi, başka ülkede gerçekleşen bir fiil hakkında, fiilin etkilerinin doğduğu ülkede egemen olan devletin uluslararası yetkisini kullanabilmesi anlamına gelmektedir<sup>320</sup>. Ülke dışından yapılan ve ülke içerisindeki kişilere ilişkin olan kişisel veri işleme faaliyetleri, ülke içerisinde etki doğurdukları için objektif mülkilik ilkesi çerçevesinde değerlendirilebilecek niteliktedir.

Netice itibarıyla KVKK ve GDPR'ın sınır ötesi uygulama kapsamlarına sahip olmalarının, devletlerin uluslararası yetkilerinin alt başlıklarından birisi olan düzenleme yetkisinin sınır ötesi kullanımına ilişkin uluslararası hukuk kurallarına uygun olduğu sonucuna varılmaktadır. Ancak söz konusu uluslararası hukuk kurallarının teamül niteliğinde olup herhangi bir uluslararası anlaşma ile kabul edilmemiş olmaları<sup>321</sup> ve pasif kişilik ilkesine yönelik çok fazla eleştirisi<sup>322</sup> bulunması

---

<sup>320</sup> Bkz. Yuk. s. 25.

<sup>321</sup> Bkz. Yuk. s. 29 vd.

<sup>322</sup> Bkz. Yuk. s. 32 vd.

nedeniyle bahse konu uygunluğun uluslararası hukukun gelişimi ile birlikte ortadan kalkabileceğini de unutmamak gerekmektedir.

Hukuki düzenlemelerin gücü, bu düzenlemelerin uygulanmasını zorlayabilen bir kamu gücünün varlığından gelmektedir. Bir kanunun çıkarılması, o kanunu uygulayacak yetkili adli ve idari makamlar olmazsa, pratikte herhangi bir anlam ifade etmeyecektir. KVKK ve GDPR özelinde bakıldığında ise bu kanunların, kişisel verilerin korunması konusunda yetkilendirilmiş bağımsız idari otoritelerce uygulanmakta olduğu görülmektedir. Söz konusu otoriteler denetim yapabilmekte, veri işleme faaliyetlerinin nasıl olması gerektiği konusunda talimatlar verebilmekte ve para cezaları kesebilmektedir. Adli makamların yaptığı yargılama faaliyetlerinin ise KVKK ve GDPR'ın uygulanması noktasında çok daha sınırlı olduğu gözlemlenmektedir. İdare ve ceza mahkemeleri, idari makamların hukuki işlemlerini denetlemekteyken, hukuk mahkemeleri ise kişiler arasındaki uyuşmazlıklarla ilgilenmektedirler.

Uluslararası hukuk çerçevesinde idari makamların başka ülkede kamu gücü kullanması, ev sahibi ülkenin rızasına bağlanmıştır. Dolayısıyla KVKK ve GDPR'ı uygulamakla görevli olan idari makamların, sadece kendi inisiyatiflerine dayanarak bir başka ülkede faaliyet göstermesi uluslararası hukuka aykırılık sonucunu doğurabilecektir. Adli makamlar açısından bakıldığında da KVKK ve GDPR çerçevesindeki genel rolleri gereği sınır ötesi yetki kullanımı senaryolarının gündeme gelemeyeceği düşünülmektedir. Zira bu mevzuatta idari otoritelerin karar ve yaptırımlarının yargı denetimine tabi olması söz konusudur. Bir devletin idari otoritesinin verdiği kararların yargısal denetiminin, başka bir devlet mahkemesinde yapılması hukuken mümkün olmayacağı için sınır ötesi yetki kullanımı gündeme gelmeyecektir<sup>323</sup>.

---

<sup>323</sup> Öte yandan belirtmek gerekir ki kişisel verilerin korunmasına ilişkin ceza davaları ya da kişiler arasındaki hukuk davaları için mahkemeler kendi milletlerarası yetki kuralları çerçevesinde yargılama yapabilecektir.

## **VI. KVKK’NIN VE GDPR’IN SINIR ÖTESİ UYGULAMA KAPSAMININ HUKUKLARIN ÇATIŞMASI KAVRAMI AÇISINDAN DEĞERLENDİRİLMESİ**

### **A. KVKK ve GDPR’ın Sınır Ötesi Uygulama Kapsamının Hukukların Çatışması Durumu Yaratması**

Çalışmamızın daha önceki bölümlerinde de açıklandığı üzere, devletlerin düzenleme yetkilerini sınır ötesi kapsamlı olarak aynı olgu üzerinde kullanmaları halinde ortaya çıkan durum hukukların çatışması olarak adlandırılmıştır. İçinde bulunduğumuz internet çağının yapısı ve imkânları, verilerin farklı ülkelerde bulunmasını son derece yaygın hale getirmektedir. Bir başka deyişle, her ülkeye ilişkin veriler o ülkede bulunmamakta, tam aksine genellikle bir ülkeye ilişkin veriler; diğer ülke ya da ülkelerde bulunan veri merkezleri içerisinde bulunmaktadır. Bu yapının temel sebebi, çalışmamızın üçüncü bölümünde detaylı olarak açıklanan bulut bilişim yapılarının kullanımıdır.

GDPR ve KVKK’nın temel düzenleme alanı, bir gerçek kişiyi belirleyen ya da belirlenebilir kılan her türlü veri anlamına gelen kişisel verilerdir. Kişisel verilerin korunması vatandaşların temel hak ve özgürlüklerinden birisi olarak kabul edilmektedir. Ancak kişisel verilere ilişkin kurallar getiren tek hukuki düzenlemeler, Türkiye için KVKK; AB için GDPR değildir. Aynı şekilde kişisel verilerin korunmasına ilişkin kanunu bulunan yaklaşık 132 adet ülke<sup>324</sup> bulunmakta olmasına rağmen bu ülkelerde de kişisel verilere ilişkin tek düzenleme, o ülkenin kişisel verilerinin korunması kanunları değildir. Zira kişisel veriler, bilgi ve iletişim teknolojileri çağında o kadar yaygın olarak kullanılmaktadır ki birçok hukuki düzenleme kişisel veriler üzerinde etki doğurmaktadır. Örnek vermek gerekirse, TTK’da yer alan Ticaret Sicili Gazetesi’nde ilan edilmesi gereken bilgiler dahi esasen kişisel verileri ilgilendiren bir düzenleme niteliğindedir.

---

<sup>324</sup> Graham Greenleaf, “Global Data Privacy Laws 2019: 132 National Laws & Many Bills”, **Privacy Laws & Business International Report**, C. 157, 2019.

Kişisel verilere dair çok sayıda düzenleme olması ile bunların bir kısmının (örneğin GDPR ve KVKK) sınır ötesi uygulama kapsamına sahip olması, söz konusu düzenlemelerin birbirleriyle çelişme ihtimalini ciddi derecede arttıracaktır. Özellikle çalışmamızın dördüncü bölümünde detaylıca açıklanacak olan veri lokalizasyonu içeren hukuk düzenlemeleri ile sınır ötesi uygulama kapsamına sahip KVKK ve GDPR gibi hukuki düzenlemeler arasında çelişki olması kaçınılmazdır<sup>325</sup>. Örneğin Bankacılık Kanunu m. 73, Türk bankalarının yurtdışına veri aktarımını yasaklamaktadır. Öte yandan GDPR’da yer alan veri taşınabilirliği hakkı çerçevesinde kişisel verisi işlenen kişilerin, kendi verilerinin başka bir veri sorumlusuna aktarılmasını talep etme hakkı bulunmaktadır. O halde GDPR’a tabi olduğu iddia edilen bir bankanın veri taşınabilirliği talebi ile karşı karşıya kalması halinde ya GDPR’ı ya da Bankacılık Kanunu’nu ihlal etmesi gerekecektir. İşte bu durum, yaşanabilecek hukukların çatışması durumlarına bir örnek teşkil etmektedir.

Birinci bölümde de açıklandığı ve yukarıda verilen örnekte de görülebileceği üzere bu tür hukukların çatışması durumlarının çözümüne ilişkin iç hukuk kuralları bulunmamaktadır. Zira devletler, iç hukuk kurallarını koyarken, yabancı devletlerin sınır ötesi uygulama kapsamına sahip kanunlarını dikkate almamaktadırlar. Kanaatimizce GDPR ve Bankacılık Kanunu arasında yaşanabilecek olan gibi hukukların çatışması olaylarında, muhatap tarafından yapılacak bir risk değerlendirmesi neticesinde her iki hukuki düzenlemeye de uyum sağlanmaya çalışılacak; eğer bu mümkün olmuyorsa yaptırım riskleri değerlendirilerek bir düzenlemeye uyum sağlanması amacıyla diğer düzenleme ihlal edilecektir.

Kanaatimizce internet ve bilgi teknolojileri kullanımı arttıkça nasıl bu konudaki hukuki düzenleme sayısı artıyorsa, söz konusu hukuki düzenlemeler arasındaki hukukların çatışması durumları da artacaktır. O halde hukukların çatışması durumlarının iç hukuk sistemleri tarafından göz önüne alınmasının, yukarıda açıklandığı şekilde konuyu sadece buna muhatap olan kişilerin problemi olmaktan çıkarılacağı düşünülmektedir.

---

<sup>325</sup> Riedenberg, “Resolving Conflicting International Data Privacy Rules in Cyberspace”, s. 1337.

## **B. KVKK ve GDPR’ın Sınır Ötesi Uygulama Kapsamlarının Yarattığı Hukukların Çatışması Durumlarına Yönelik Çözüm Önerileri**

Sınır ötesi uygulama kapsamına sahip olan KVKK ve GDPR gibi kişisel verilerin korunmasına ilişkin kanunların, diğer ülke hukuklarındaki kişisel verilerin korunmasına dair yükümlülüklerle çelişen durumlar yaratması ve bu kapsamda hukukların çatışması durumlarının oluşmasının kaçınılmaz olduğu kanaatimizce açıktır. Söz konusu hukukların çatışması durumları da özellikle veri sorumlusu ya da veri işleyen gibi rollerde bulunan Türk vatandaşları ile şirketleri açısından (ya da aynı rollerde bulunan yabancılar açısından) ciddi mağduriyetler yaratabilecektir. O halde ülkemizin kişisel verilerin korunmasına ilişkin hukuk politikasının da bu çatışma durumunu düzenleyecek şekilde geliştirilmesi gerektiği düşünülmektedir. Aksi durum, yabancı devlet kaynaklı iç hukuk yoluyla, Türk vatandaşları ve şirketlerine zarar verilmesi ihtimalini doğuracaktır.

Kişisel verilerin korunmasına ilişkin düzenlemelere uyum sağlamanın maliyeti oldukça yüksektir. Ayrıca bu düzenlemelerin kısıtlayıcı etkileri, birçok durumda teknolojik gelişme ve inovasyonun da önünü kapatabilmektedir. Dolayısıyla kişisel verilerin korunması düzenlemelerinin getirilmesine ya da kapsamına ilişkin kararlar esasen ülke ekonomisine de etki etmektedir. Örnek vermek gerekirse, GDPR gibi kapsamlı bir düzenlemenin ülkemizde direkt olarak uygulanması, veri sorumlusu ya da veri işleyen gibi rollerde bulunan Türk şirketleri için çok fazla uyum maliyeti ya da para cezası maliyeti doğurabilecek niteliktedir.

Ayrıca ifade etmek gerekir ki yabancı kanun ve ikincil mevzuatın ülkemiz sınırları içerisinde uygulanmasına göz yumulmasının, hem Türkiye Cumhuriyeti’nin egemenlik haklarının zedelenmesine hem de adeta yeni bir kapitülasyonun tanınmasına sebebiyet vereceği öngörülmektedir.

GDPR gibi kişisel verilerin korunmasına dair düzenlemelerin Türk hukuk kuralları ile kanunların çatışması durumu yaratması halinde Türk vatandaş ve şirketlerinin korunması gereksinimi kanaatimizce açık bir ihtiyaçtır. Kanaatimizce bu kapsamda alınması gereken ilk önlem, Türkiye Cumhuriyeti sınırları içerisinde kişisel verilerin

korunmasına dair hiçbir yabancı kanunun ya da diğer düzenlemenin uygulanmayacağına dair açık bir kanuni düzenleme yapılmasıdır. Aynı düzenleme içerisinde yabancı adli ya da idari makamların, Türkiye’deki faaliyetlerine ilişkin soruşturmalarıyla muhatap olan Türk vatandaş veya şirketlerinin, söz konusu soruşturmalarını ilgili Türk devlet makamlarına bildirmesi yükümlülüğünün getirilmesi önerilmektedir. Böylelikle hem diplomatik seviyede Türk vatandaş ve şirketlerinin hakları korunabilecektir hem de anılan hukukların çatışması durumlarının içerisinde kalan kişilere devlet tarafından rehberlik yapılabilecektir. Ayrıca kanuni düzenleme ile yabancı devletlerin uyguladıkları para cezalarını Türkiye’de tahsil etmelerinin önlenmesi adına söz konusu cezalara dair mahkeme kararlarının ya da idari makam kararlarının tanınması veya tenfizinin önlenmesinin yerinde olacağı düşünülmektedir.

Önerilen kanuni düzenleme ile KVKK’ya veya sektörel kanunlar çerçevesinde kendi sektörlerindeki kişisel veri işleme faaliyetlerini düzenlemeye yetkili kılınan BDDK ya da BTK gibi kurumlara, kişisel verilere ilişkin yükümlülüklerin ihlali halinde uygulanacak idari yaptırımları belirlerken, muhatapların yabancı kanunlar sebebiyle uğradıkları idari yaptırımların da dikkate almaları yükümlülüğü getirilmesi önerilmektedir. Böylelikle yabancı devletlerin sınır ötesi uygulama kapsamlı kanunlarının Türkiye içerisinde uygulanması engellenememişse, en azından Türk vatandaş ve şirketlerin aynı fiilden dolayı birden çok kez yaptırımla karşılaşmalarının önüne geçilmiş ve bu yolla mağduriyetler azaltılmış olacaktır.

Yabancı devletlerin sınır ötesi uygulama kapsamına sahip kanunlarının Türkiye Cumhuriyeti sınırları içerisinde uygulanmasının engellenmesi yönündeki en güçlü silahlardan birisinin de mütekabiliyet ilkesi olduğu değerlendirilmektedir. Bu nedenle anılan kanuni düzenleme önerisi çerçevesinde ilgili yabancı devletin adli ya da idari soruşturma veya yaptırımlarına karşı Türkiye Cumhuriyeti sınırları içerisinde mütekabiliyete dayalı önlemler alınmasına imkân verilmesinin yerinde olacağı düşünülmektedir. Söz konusu önlemler, ilgili yabancı devlet vatandaş ve şirketlerinin Türkiye’deki kişisel veri işleme faaliyetlerinin sınırlandırılmasına yönelik erişim engelleme, bant daraltma, reklam alma ya da verme yasağı, bankacılık sistemine

eriřim yasađı gibi yaptırımlar olabileceđi düşünölmektedir. KVKK'nın sınır ötesi uygulama kapsamının da net bir şekilde çizilmesi yoluyla mütekabiliyet geređi ilgili yabancı devlet sınırları içerisinde Türk kanunlarının uygulanması da sağlanabilecektir. Ayrıca KVKK'nın yaptırımlarının, yabancı ölkelerle eş seviyeye (örneğin GDPR ile) çıkarılması yoluyla yabancı devletlerin Türk vatandaş ve şirketlerine uygulayabilecekleri yaptırımların aynısı ilgili yabancı devletin vatandaş ve şirketlerine uygulanabilecektir.



## ÜÇÜNCÜ BÖLÜM

### ABD HUKUKUNDA CEZA YARGILAMASI KAPSAMINDA ADLİ MAKAMLARIN DİJİTAL ORTAMDAKİ BİLGİLERE ERİŞMESİ

#### I. GİRİŞ

##### A. Dijital Ortamdaki Bilgilere Erişmeye Yönelik İhtiyaçlar ve Karşılaşılan Sorunlar

Günümüzde kişiler arasındaki iletişim ve haberleşmenin çok önemli bir kısmı, dijital ortamda faaliyet gösteren çok uluslu şirketlerin sunduğu hizmetler vasıtasıyla gerçekleştirilmektedir<sup>326</sup>. Yine dijital ortam üzerinden yayınlanan yazı, fotoğraf veya video içerikleri ile kitle iletişimi de söz konusu hizmetler vasıtasıyla etkili bir şekilde gerçekleştirilebilmektedir. Gerçek ve tüzel kişilerin kendilerine ya da faaliyetlerine ilişkin bilgileri de yaygın şekilde dijital ortamda sakladıkları veya yayınlamak dahil çeşitli işlemlere tabi tuttukları gözlemlenmektedir.

Dijital ortamın kişiler hakkında bu denli fazla bilgi içeriyor olması ve toplumların çok büyük kısımları tarafından erişilebilir hale gelmesi, adli makamların<sup>327</sup> da dijital ortamdaki bilgi toplama ihtiyacını arttırmıştır<sup>328</sup>. Zira artık işlenen suçlar mutlaka dijital ortamla ilişkili hale gelmektedir. Dijital ortam haricindeki telefon ya da posta gibi iletişim araçlarını izleyebilen ya da bilgi talebi, arama veya el koyma gibi yollarla

<sup>326</sup> Facebook, Twitter, Instagram, WeChat veya Sina Weibo gibi sosyal ağlar, Skype ve WhatsApp gibi mesajlaşma uygulamaları ya da Gmail veya Hotmail gibi e-posta servisleri, günümüzde yoğun olarak kullanılan iletişim hizmetlerine örnekler teşkil etmektedir.

<sup>327</sup> Buradaki adli makamlar terimi sadece ceza yargılamasına ilişkin mahkemeler, savcılıklar ve adli kolluğu kapsamaktadır. Çünkü ceza yargılaması kapsamında verilen kararların yerine getirilmesine ilişkin zorunluluk getiren düzenlemeler, bu çalışmanın esas konusunu teşkil eden kanunlar ihtilafı sorununu meydana getirmektedir. Oysa hukuk yargılamasında delilleri sunmak zorunlu olmayıp temel olarak tarafların iradesine bırakılmaktadır. Bu nedenle hukuk yargılaması kapsamındaki bilgi talepleri çalışmamız kapsamı dışında bırakılmıştır. Nitekim yabancı ülkelerde veya milletlerarası anlaşmalarda da bu konuya ilişkin düzenlemeler (adli istinabe hariç) görülmemektedir.

<sup>328</sup> “Transparency Report: Search Removals Under European Privacy Law”, Google, (Çevrimiçi) <https://transparencyreport.google.com/eu-privacy/overview>, 27.08.2016.; Dylan Cors, “National Security Data Access and Global Legitimacy”, **United States Attorneys’ Bulletin**, C. 67, S. 4, 2019, s. 257.



kişiler hakkında bilgi toplayabilen adli makamlar, dijital ortamda bu yetkilerini kullanmakta büyük zorluklarla karşılaşmaktadır.

Adli makamların dijital ortamdaki bilgilere erişme konusunda yaşadığı zorlukların başında, iletişim ve saklama da dahil olmak üzere dijital ortamda gerçekleştirilen işlemlerin neredeyse tamamının bulut bilişim sistemleri vasıtasıyla gerçekleştirilmesi gelmektedir<sup>329</sup>. Bulut bilişim sayesinde verilerin ülke sınırları dışında saklanması mümkün hale geldiğinden adli makamlarca yapılacak bilgi talepleri farklı bir devletin egemenlik alanına etki etmekte ve bilgi taleplerinin yerine getirilebilmesi için çeşitli uluslararası anlaşmaların uygulanması ihtiyacı doğmaktadır. Birkaç saatin dahi çok uzun bir zaman olarak kabul edildiği dijital ortamın dinamikleri düşünüldüğünde, uzun diplomatik ve bürokratik süreçlerin dijital ortamda etkin bir şekilde delil toplayabilmek için faydasız kalacağı açıktır. Nitekim aşağıdaki başlıklar altında inceleneceği üzere ABD hukukunda bu soruna çözüm bulunmasına yönelik mevzuat yürürlüğe konmuştur<sup>330</sup>.

Öte yandan belirtmek gerekir ki bulut bilişim sistemlerinin coğrafi olarak tüm dünyaya yayılmış yapısı sayesinde dijital ortam günümüzdeki gelişmişlik seviyesine erişebilmiştir<sup>331</sup>. Bulut bilişim sistemleri başta yapay zekâ olmak üzere birçok teknolojik gelişmeyi mümkün kılan teknoloji altyapısını sağlamaktadır. Yüksek maliyetli altyapı gereksinimlerinden dolayı dijital ortamda büyük ölçekli olarak hizmet sağlayabilmek için bulut bilişim sistemlerinden yararlanmak neredeyse bir ticari mecburiyet haline gelmiştir<sup>332</sup>. Dolayısıyla yukarıda açıklanan sorunlara rağmen bulut bilişimin kullanılmasından vazgeçilmesi mümkün olmamaktadır.

---

<sup>329</sup> Bu çalışmanın hazırlandığı tarih itibarıyla global pazarın büyük çoğunluğu Amazon Web Services, Microsoft Azure ve Google Cloud adlı üç büyük bulut hizmeti sağlayıcısı arasında bölünmüş durumdadır.

<sup>330</sup> Bkz. Aş. s. 120 vd.

<sup>331</sup> Bulut bilişim sistemlerinin teknolojik gelişmelerle olan bağlantısı hakkında bilgi için bkz. David Linthicum, "How Cloud Computing Impacts Technology Evolution", **InfoWorld**, 01.10.2021, (Çevrimiçi) <https://www.infoworld.com/article/3635092/how-cloud-computing-impacts-technology-evolution.html>, 01.11.2021.

<sup>332</sup> Örneğin bulut bilişim sistemlerinin getirdiği esneklik sayesinde dijital ortamda sunulan bir hizmetin en çok talep gördüğü dönemlerde, bu hizmete ilişkin bilişim kapasitesini genişletip, talebin az olduğu dönemlerde daraltarak maliyetleri düşürmek mümkündür. Halbuki bulut bilişim kullanımı yerine

## B. Bölümün İnceleme Konusu ve Kapsamı

Çalışmamızın bu bölümünün temel konusu, ceza yargılaması kapsamında ABD adli makamların; dijital ortamda bulunan ve veri konumu olarak yabancı ülkelerdeki veri merkezlerinde saklanan bilgilere erişme imkanlarının incelenmesidir. Yine bu kapsamda doğabilecek hukukların çatışması sorunları da analiz edilecektir. Nihai olarak ise konunun Türk hukuku çerçevesinde nasıl ele alınması gerektiğine yönelik çözüm önerileri oluşturulması hedeflenmektedir.

Öte yandan çalışmamızın amacı adli makamların bilgi taleplerini düzenleyen mevcut adli istinabe sözleşmelerinin incelenmesi<sup>333</sup> değildir. Adli istinabe sözleşmeleri vasıtasıyla sonuç almak yıllarca sürebilmekte ve bu nedenle de bilgi talepleri konusunda etkili bir yöntem olarak kullanılmaları mümkün olmamaktadır.

Çalışma kapsamının netleştirilmesi açısından üzerinde durulması gereken bir diğer nokta da yabancı mahkeme kararlarının tanınması ya da tenfizi ile milletlerarası tebligat konularının da kapsam dışında tutulduğudur. Çünkü adli makamların bilgi taleplerinin kesin mahkeme kararı olmamaları nedeniyle tanıma ya da tenfize konu olması mümkün olmayacağı gibi tebliğ edilmeleri de yabancı devletlerin egemenlik alanında bulunan kişiler üzerinde bağlayıcı olmalarını sağlamayacaktır.

Aşağıdaki başlıklar altında, öncelikle mevcut dijital ortam yapısı gereği dijital ortamdaki bilgilere erişim konusunda önem arz eden bulut bilişim hakkında genel bilgiler verilecektir. Bulut bilişim sağlayıcılarının işletmekte oldukları bulut bilişim sistemleri, üçüncü kişilere ait devasa miktarlarda bilgi tuttukları için bu bölümün odak noktasını oluşturmaktadırlar<sup>334</sup>. İkinci aşamada ise adli makamlarının dijital ortamdaki yapacağı bilgi talepleri konusunda oldukça zengin düzenlemelere sahip olan ABD

---

hizmet sağlayıcı kendi bilişim sistemini kurmuş olsaydı; talebin en yüksek olduğu günün ihtiyaçlarına göre kurulan bilişim sistemi, talebin düşük olduğu dönemlerde atıl olarak bekleyecektir.

<sup>333</sup> Adli istinabe sözleşmelerinin incelenmesi hakkında bilgi için bkz. Ali Gümrah Toker, **Milletlerarası Özel Hukukta İstinabe**, 1. bs, Adalet Yayınevi, 2015.

<sup>334</sup> Renee Berry, Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing", **Journal of International Commerce & Economics**, C. 4, S. 2, 2012, s. 1-38.

hukuku incelenecektir. Daha sonra da sırasıyla ABD hukukundaki düzenlemelerin yarattığı etkiler üzerinde durulacaktır.

## II. BULUT BİLİŞİM SİSTEMLERİNE GENEL BAKIŞ

Bulut bilişim<sup>335</sup> sistemleri günümüz dijital ortamının temel taşı oluşturmaktadır. Dijital ortamda sunulan hizmetlerin hemen hepsi bulut bilişim sistemleri vasıtasıyla çalışmaktadır. Sosyal medyadan yapay zekaya kadar sosyal, siyasal ve ekonomik hayatı etkileyen birçok güncel teknolojik gelişme gücünü bulut bilişimden almaktadır. Dolayısıyla dijital ortamın anlaşılabilmesi bulut bilişim sistemlerinin çalışma modellerinin iyi bir şekilde anlaşılmasına bağlıdır. Bu kapsamda öncelikle bulut bilişimin tanımı üzerinde durulacaktır. Sonrasında da sunulan hizmetler açısından bulut bilişim sistemleri ile veri saklama modelleri açısından bulut bilişim sistemleri sınıflandırmaları incelenecektir.

### A. Bulut Bilişimin Tanımı

ABD Ulusal Teknoloji ve Standartlar Enstitüsü, bulut bilişimi şöyle tanımlamaktadır<sup>336</sup>:

*“Bulut bilişim her zaman herhangi bir yerde pratik şekilde ve ihtiyaç seviyesine bağlı olarak ağ erişimine açık; sağladığı kaynakların asgari miktarda yönetim çalışması veya hizmet sağlayıcı iletişimi ile hızlı bir şekilde artırılıp azaltılabilmesi mümkün olan, paylaşımlı kullanılan ve adapte edilebilir bir bilgisayar kaynakları (örneğin ağlar, sunucular, depolama birimleri, uygulama ve hizmetler) havuzudur<sup>337</sup>.”*

Türk Standartları Enstitüsü tarafından yayınlanan Bulut Bilişim Güvenlik ve Kullanım Standardı Taslağı ise bulut bilişimi şöyle tanımlamaktadır<sup>338</sup>:

<sup>335</sup> Bulut bilişime ilişkin detaylı bilgi için bkz. Lin, “Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption”, s. 1106-1112.

<sup>336</sup> Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, Recommendations of the National Institute of Standards and Technology, The National Institute of Standards and Technology, 2011, s. 2, (Çevrimiçi) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, 12.02.2017.; Paul M. Schwartz, “Legal Access To The Global Cloud”, **Columbia Law Review**, C. 118, S. 6, 2018, s. 1689.

<sup>337</sup> Tanımın orijinal hali şu şekildedir: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

<sup>338</sup> “Bulut Bilişim Güvenlik ve Kullanım Standardı”, Türk Standartları Enstitüsü, 07.03.2014, s. 5, (Çevrimiçi) <https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf>, 10.03.2022.

*İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde artırılıp azaltılabildiği kaynaklarının kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür.*

Alternatif ve daha kısa bir tanıma göre, bulut bilişim temel olarak çeşitli donanım ve yazılım kaynaklarının uzaktan internet yoluyla ücretli ya da ücretsiz olarak kullanıma sunulmasıdır<sup>339</sup>.

ABD Yüksek Mahkemesi<sup>340</sup> de bulut bilişimi şu şekilde tanımlamaktadır<sup>341</sup>:

*“İnternete bağlı cihazların kendi hafızalarında değil uzakta bulunan sunucularda bulunan verileri gösterme imkânı”*

## **B. Sunulan Hizmetler Açısından Bulut Bilişim Sistemleri Çeşitleri**

Bulut bilişim sistemleri, sunulan hizmetler açısından yazılım hizmeti (**Software as a Service - SaaS**), platform hizmeti (**Platform as a Service - PaaS**), ve altyapı hizmeti (**Infrastructure as a Service - IaaS**) olarak üç alt kategoriye ayrılmaktadır<sup>342</sup>. Bu kategorilerle ilgili olarak bulut bilişime ilişkin katmanlı bir sınıflandırma da

<sup>339</sup> Miranda Mowbray, ‘The Fog over the Grimpen Mire: Cloud Computing and the Law’ (2009) 6 SCRIPTed: A Journal of Law, Technology and Society 132, 133, <[http://heinonline.org/HOL/Page?handle=hein.journals/scripted6&div=11&g\\_sent=1&collection=journals](http://heinonline.org/HOL/Page?handle=hein.journals/scripted6&div=11&g_sent=1&collection=journals)> accessed 8 August 2017.

<sup>340</sup> Özgün adı Supreme Court of the United States şeklindedir. İnternet sitesi için bkz. (Çevrimiçi) <https://www.supremecourt.gov>, 04 Ağustos 2019.

<sup>341</sup> Orijinal metindeki hali ile şu şekildedir: “[c]loud computing” as “the capacity of Internet- connected devices to display data stored on remote servers rather than on the device itself.” Riley v. California, C. 1, C. 1 U.S. Reports, (U.S. Supreme Court 2014).

<sup>342</sup> Mell, Grance, “The NIST Definition of Cloud Computing”, s. 2; “Bulut Bilişim Güvenlik ve Kullanım Standardı”, s. 22; Berry, Reisman, “Policy Challenges of Cross-Border Cloud Computing”, s. 3-4; Urs Gasser, “Cloud Innovation and the Law: Issues, Approaches, and Interplay”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 17.03.2014, s. 3-4, (Çevrimiçi) <https://papers.ssrn.com/abstract=2410271>, 10.07.2017.; Paul M. Schwartz, “Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies”, **Bloomberg BNA Privacy and Security Law Report**, 2016, s. 3, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2862648](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862648), 14.05.2019; Heidi Bohaker Lisa Austin, Andrew Clement, Stephanie Perrin, **Seeing Through the Cloud**, Canada, Creative Commons, 2015, s. 11; Marcin Rojszczak, “CLOUD act agreements from an EU perspective”, **Computer Law & Security Review**, C. 38, 2020, s. 3, (Çevrimiçi) <https://www.sciencedirect.com/science/article/pii/S0267364920300479>, 27.09.2020.

mevcuttur<sup>343</sup>. Bu katmanlar: donanım katmanı, altyapı katmanı, platform katmanı ve uygulama katmanıdır.

Donanım katmanı, bulut bilişim sistemini meydana getiren gerçek donanım kaynaklarının (sunucular, ağ sistemleri, güç sistemleri gibi) sınıflandırıldığı katmandır. Donanım katmanından yararlanmak isteyen kullanıcılar; bulut bilişim sağlayıcıdan belirli işlemci ya da depolama donanımlarını kullanmaya ilişkin sözleşmeler yapmaktadır. Altyapı katmanı da donanım katmanı ile son derece benzer şekilde, bulut bilişim sisteminin işlemci ya da depolama kaynaklarının kullanılmasına imkân vermektedir. Altyapı katmanının farklılığı, kullanılan donanım kaynaklarının fiziksel olarak değil mantıksal olarak bölünmesi noktasında görülmektedir<sup>344</sup>. Her iki katmanda da kullanıcı kendisine tahsis edilen kaynakları kendi ihtiyaçlarına göre kullanabilmektedir. Donanım ve altyapı katmanları, altyapı hizmeti kategorisine dahildir.

Platform katmanı, işletim sistemlerinin veya uygulama altyapılarının çalıştırıldığı kısımdır. Bir başka deyişle platform katmanı, kullanıcılarına yazılım altyapısı sağlamaktadır. Bu katmanda bulut bilişim sağlayıcı, kullanıcının kendine özgü ihtiyaçları için kendi yazılımını geliştirmesine ve çalıştırmasına imkân veren bir yazılım platformu sunmaktadır. Söz konusu platformlara örnekler **Microsoft Azure**<sup>345</sup> ve **Google AppEngine**<sup>346</sup> olarak gösterilebilir. Platform katmanı, platform hizmeti kategorisine dahildir.

Uygulama katmanı, doğrudan son kullanıcılar tarafından kullanılabilen **Facebook**, **YouTube** ve **Spotify** gibi uygulamalardan ya da platformlardan oluşturmaktadır. Bu katman üzerinde sunulan uygulamalar veya platformlar, bulut bilişim sistemleri üzerinde çalışmakta ve çeşitli kullanıcı cihazları (bilgisayar, tablet ya da akıllı telefon

---

<sup>343</sup> Qi Zhang, Lu Cheng, Raouf Boutaba, “Cloud Computing: State-of-the-Art and Research Challenges”, **Journal of Internet Services and Applications**, C. 1, S. 1, 2010, s. 9.

<sup>344</sup> Örnek vermek gerekirse donanım katmanından yararlanan bir kullanıcı, tek bir fiziksel cihazın tamamından yararlanırken; altyapı katmanından yararlanan kullanıcı ise tek bir fiziksel cihazın belirli bir kısmından yararlanmaktadır.

<sup>345</sup> Microsoft Azure hakkında detaylı bilgi için bkz. <https://azure.microsoft.com>.

<sup>346</sup> Google AppEngine hakkında detaylı bilgi için bkz. <https://cloud.google.com/appengine/>.

gibi) vasıtasıyla bu uygulamalardan yararlanmak mümkün olabilmektedir. Uygulama katmanı, yazılım hizmeti kategorisine dahildir.

Bulut bilişim sağlayıcılara örnek olarak **Amazon Web Services**, **Microsoft** ya da **Google** gibi bulut bilişim hizmetleri konusunda dünyada önde gelen şirketler gösterilebilir<sup>347</sup>. Bunlar yanında **Facebook**, **Twitter** ya da **Instagram** gibi sosyal medya platformları, **Amazon** ya da **Alibaba** gibi elektronik ticaret platformları veya da **Google** ya da **Yandex** tarafından sunulan arama motorları da bulut bilişim sistemleri kullanılarak çalıştırılmakta ve bulut bilişim hizmetleri olarak son kullanıcılara sunulmaktadır.

Ayrıca önemle belirtmek gerekir ki bir şirketin<sup>348</sup> değişik katmanlarda aynı anda hizmet sağlaması önünde herhangi bir engel bulunmamaktadır. Hatta çoğu durumda bir şirketin tüm katmanlarda birden hizmet sağladığı görülmektedir. Örnekle açıklamak gerekirse **Microsoft** sunduğu **Microsoft 365** hizmetleri ile hem kurumsal müşterilerinin kendi kullanıcılarına e-posta hizmeti sunabilmesine imkân sağlamakta hem de sunduğu **Hotmail** ya da **Outlook** gibi e-posta hizmetleri ile doğrudan kendisi kendi müşterileri olan son kullanıcılara e-posta hizmeti sunmaktadır<sup>349</sup>. **Microsoft** ilk örnekte platform ve altyapı katmanı sağlarken ikinci örnekte uygulama katmanı çerçevesinde hizmet sağlamaktadır. Bunlara ek olarak bir şirket, bir bulut bilişim sağlayıcıdan hizmet alıp bunları üçüncü kişilerin kullanımına sunmak suretiyle uygulama katmanı hizmeti de sunabilmektedir. Örneğin, son kullanıcılara uygulama katmanı kapsamında hizmet sunmakta olan **Netflix**, hizmetlerini sunabilmek için

---

<sup>347</sup> Bohaker Lisa Austin, Andrew Clement, Stephanie Perrin, **Seeing Through the Cloud**, s. 14; Katherine Graber, "Where in the World Is Your Data: Who Can Access It?", **Federal Communications Law Journal**, C. 70, S. 1, 2018, s. 159.; Bohaker Lisa Austin, Andrew Clement, Stephanie Perrin, **Seeing Through the Cloud**, s. 14. Ayrıca bkz. David Goldman, "What Is the Cloud?", **CNN Business**, 04.09.2014, (Çevrimiçi) <https://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/index.html>, 09.07.2022.

<sup>348</sup> Her ne kadar gerçek kişilerin de bu tür hizmetlerin gerçek kişiler veya diğer tüzel kişi tipleri tarafından da sunulması mümkün olmasına rağmen uygulamada böyle bir durum söz konusu olmadığı için şirket terimi kullanılmıştır.

<sup>349</sup> Bohaker Lisa Austin, Andrew Clement, Stephanie Perrin, **Seeing Through the Cloud**, s. 11.

**Amazon Web Services** tarafından sağlanan altyapı katmanı hizmetlerinden yararlanmaktadır<sup>350</sup>.

### **C. Veri Saklama Yöntemleri Açısından Bulut Bilişim Sistemleri Çeşitleri**

Bulut bilişim sistemlerinin verileri nasıl sakladıkları, adli makamların bulut bilişim sistemlerinde saklanan bilgilere erişim talepleri açısından çok büyük önem arz etmektedir. Zira bulut bilişim sistemlerindeki verileri barındıran veri merkezlerinin konumu, adli istinabe sözleşmelerindeki süreçlerin işletilmesi açısından kritiktir.

Bulut bilişim sistemlerinin veri saklama yöntemlerine göre sınıflandırılması, esasen bulut bilişim sistemlerinin ABD’deki bir takım mahkeme kararlarına konu olmaları<sup>351</sup> ya da çeşitli hukuki yükümlülüklerle uyum sağlanması neticesinde ortaya çıkmıştır<sup>352</sup>. Bu kapsamda üçlü bir ayrıma gidilmektedir. Bunlar verilerin bir bütün olarak tek bir konumda saklandığı lokal bulut bilişim sistemi, verilerin parçalara bölünerek tek başına anlamsız parçalar halinde çeşitli ülkelerde bulunan veri merkezlerinde saklandığı dağınık bulut bilişim sistemi ile erişim yetkilerinin bulut bilişim sağlayıcıdan başka bir üçüncü kişiye devredildiği erişim yetkisi ayrıştırılmış bulut bilişim sistemidir. Aşağıdaki başlıklar altında her bir model ile ilgili bilgiler paylaşılacaktır.

#### **1. Lokal Bulut Bilişim Sistemi**

Lokal bulut bilişim sistemi modelinde, kullanıcıların bulut bilişim sistemine aktardığı veriler, bir bütün olarak tek bir ülkede ya da bölgede bulunan veri merkezinde saklanır<sup>353</sup>. Her ne kadar kullanıcının ilgili verileri çeşitli ülkelere bölmesi mümkün

---

<sup>350</sup> “Netflix on AWS”, Amazon Web Servies, (04.03.2022), (Çevrimiçi) <https://aws.amazon.com/tr/solutions/case-studies/netflix/>, 04.03.2022.; Steven Musil, “Amazon Cloud Outage Downs Netflix, Quora”, CNET, 2011, (Çevrimiçi) <https://www.cnet.com/tech/services-and-software/amazon-cloud-outage-downs-netflix-quora/>, 17.03.2022.

<sup>351</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google, Case 2:16-mj-01061-TJR, (The United States District Court for the Eastern District of Pennsylvania 03 Şubat 2017); Microsoft Corp v. United States, (Supreme Court of the United States 17 Nisan 2018).

<sup>352</sup> Bkz. Aş. s. 120 vd.

<sup>353</sup> Patrick S. Ryan, Sarah Falvey, Ronak Merchant, “When the Cloud Goes Local: The Global Problem with Data Localization”, **IEEE Computer Society**, 2013, s. 54-57; Schwartz, “Legal Access To The Global Cloud”, s. 1696.; Ata Umur Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, **Kişisel Verileri Koruma Dergisi**, C. 2, 2020, s. 100.

olsa da ilgili veriler anlamsız parçalara bölünmez. Yani her veri merkezinde bulunan veriler, tek başlarına anlamlıdır. Basit bir örnek vermek gerekirse, iki kişi arasında geçen bir konuşmada, ilgili uygulamada bulunan profil fotoğrafı bir veri merkezinde saklanabilirken konuşma içerikleri diğer bir ülkede saklanabilir. Profil fotoğrafı ya da konuşma verilerinin parçalanması (bir fotoğrafa ilişkin verilerin tek başına anlam ifade etmeyen çok sayıda parçaya bölünmesi) söz konusu değildir.

Lokal bulut bilişim sistemleri modeli, adli makamların adli istinabe yoluyla bilgi taleplerinde bulunmasına uygundur. Zira burada veri merkezinin bulunduğu ülkeye yapılacak tek bir talep ile ihtiyaç duyulan verilere erişmek mümkün olabilecektir.

Lokal bulut bilişim sistemleri, özellikle veri merkezine ev sahipliği yapan ülkelerin gerekli verilere erişimi konusunda büyük kolaylıklar sağlamaktadır. Yine bununla bağlantılı olarak diğer ülkelerin ihtiyaç halinde bu verilere erişmesi de son derece güçtür. Zira adli istinabe anlaşmaları her zaman ve hızlı netice doğuramamaktadır<sup>354</sup>. Bunun üzerine bir de devletlerin istihbarat faaliyetlerinin yarattığı güvensizlikler eklenince, dünyanın her yerinde veri lokalizasyonunu zorunlu tutan hukuk kurallarının ortaya çıkması şeklinde bir eğilim doğmuştur<sup>355</sup>. Ülkemizde de veri lokalizasyonuna ilişkin birçok düzenleme bulunmaktadır<sup>356</sup>. Söz konusu kurallar bilgi sistemlerinin ya da verilerin ilgili ülkelerin sınırları içerisinde tutulmasını zorunlu kılmaktadır. Lokal bulut bilişim sistemleri de bu veri lokalizasyonu kurallarına uyum sağlamaya elverişlidir.

---

<sup>354</sup> Önemle belirtmek gerekir ki adli istinabe anlaşmaları genellikle sadece adli makamların taleplerini karşılayabilmektedir. Oysaki verilere erişim ihtiyacı her zaman sadece adli makamların görevleri gereği doğmamaktadır. İdari makamların da bu verilere çeşitli sebeplerle erişme ihtiyacı vardır.

<sup>355</sup> Önemle belirtmek gerekir ki söz konusu kuralların faydaları ve zararları konusunda birçok tartışma bulunmaktadır. Ancak söz konusu tartışmalar bu çalışmanın kapsamı dışında olduğu için bunlara değinilmeyecektir. Detaylı bilgi için bkz. “Understanding Data Localization Laws”, **Big Bang 360**, (04.09.2020), (Çevrimiçi) <https://bigbang360.com/data-localization-laws/>, 04.09.2020; Arindrajit Basu, “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam”, **The Diplomat**, (10.01.2020), (Çevrimiçi) <https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/>, 15.05.2020; Julia Yoon, “South Korean Data Localization: Shaped by Conflict”, **Henry M. Jackson School of International Studies**, (28.02.2018), (Çevrimiçi) <https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/>, 14.04.2020; Alexander Savelyev, “Russia’s new personal data localization regulations: A step forward or a self-imposed sanction?”, **Computer Law & Security Review**, C. 32, S. 1, 2016, s. 128-145; “Data Protection Laws of The World Angola vs Brazil”, **DLA Piper**, 2017, s. 14.

<sup>356</sup> Bkz. Aş. s.223 vd.



Lokal bulut bilişim sistemi modelini kullanan başlıca bulut bilişim sağlayıcılar **Microsoft** ve **Amazon**'dur<sup>357</sup>. Her iki şirketin de birçok ülkede veri merkezleri bulunmakta olup bunlar vasıtasıyla müşterilerine hizmet sunmaktadırlar<sup>358</sup>. Söz konusu şirketlerden hizmet alınırken genellikle veriler bir ülkedeki merkezinde tutulmakta ve diğer bir ülkede de yedeklenmektedir. Verilere erişim ise kurulan teknik altyapıya bağlı olarak bir ya da birden fazla ülkeden sağlanabilmektedir. Örnek vermek gerekirse, **Microsoft** ve **Amazon**'un AB sınırları içerisinde bulunan veri merkezlerine ABD'den erişim mümkün değildir<sup>359</sup>.

## 2. Dağınk Bulut Bilişim Sistemi

Dağınk bulut bilişim sistemi modelinde, kullanıcıların bulut bilişim sistemine aktardığı veriler çok sayıda parçaya bölünmektedir<sup>360</sup>. Bu parçalar bulut bilişim sistemine dahil olan veri merkezleri arasında dağıtılarak saklanmaktadır. Veri parçaları tekrar bütünleştirilmeden, anlamlı bir bilgiye erişmek mümkün olmamaktadır.

Dağınk bulut bilişim sistemi modelinin kullanılmasındaki temel amaçlar verimliliğin sağlanması olarak belirtilmiştir<sup>361</sup>. Söz konusu bölme işlemi, yapay zekâ ve

---

<sup>357</sup> Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1929-1930; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 100; Schwartz, "Legal Access To The Global Cloud", s. 1696.

<sup>358</sup> Schwartz, "Legal Access To The Global Cloud", s. 1696; "AWS Global Infrastructure", 01.10.2023, (Çevrimiçi) [https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h\\_ls](https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls), 11.01.2023. Microsoft veri merkezleri hakkında güncel bilgi için bkz. "Availability Zone Service and Regional Support", 01.10.2023, (Çevrimiçi) <https://learn.microsoft.com/en-us/azure/reliability/availability-zones-service-support>, 11.01.2023. Ayrıca bkz. Schwartz, "Legal Access To The Global Cloud", s. 1696.

<sup>359</sup> Schwartz, "Legal Access To The Global Cloud", s. 1697; "Choosing a Cloud Platform", **Amazon Web Services**, 26.07.2018, (Çevrimiçi) <https://perma.cc/97WA-QTFM>, 30.05.2021; "Microsoft Azure Germany", **Microsoft**, 26.07.2018, (Çevrimiçi) <https://perma.cc/A3K9-HYM8>, 30.05.2021.; Schwartz, "Legal Access To The Global Cloud", s. 1697.

<sup>360</sup> Kristen E. Eichensehr, "Data Extraterritoriality", **Texas Law Review**, C. 95, 2017, s. 146; Schwartz, "Legal Access To The Global Cloud", s. 1695; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 100; Schwartz, "Legal Access To The Global Cloud", s. 1695; Kristen E. Eichensehr, "Data Extraterritoriality", **Texas Law Review**, C. 95, 2017, s. 146.

<sup>361</sup> Cory Isaacson, "Database Sharding: The Key to Database Scalability", **Database Trends and Applications**, 14.08.2009, (Çevrimiçi) <https://www.dbta.com/Editorial/Trends-and-Applications/Database-Sharding--The-Key-to-Database-Scalability-55615.aspx>, 03.09.2021.

algoritmalar yardımıyla gerçekleştirilmekte ve yine aynı teknolojiler vasıtasıyla veri parçalarının yerleri, veri merkezleri arasında sürekli değiştirilmektedir<sup>362</sup>.

Yukarıda yapılan açıklamalardan anlaşılacağı üzere, dağınık bulut bilişim sistemi modelinde, adli makamlar tarafından talep edilen bir bilginin sağlanabilmesi için öncelikle ilgili veri parçalarının birleştirilmesi gerekmektedir. Ancak bu birleştirme işlemi, sadece çeşitli veri merkezlerinde bulunan verilerin tek bir yerde toplanabilmesi ile mümkün olabilecektir. Dolayısıyla, bu modeli kullanan bulut bilişim sağlayıcılarından yapılacak bilgi taleplerinin, verinin konumuna bağlı olarak kullanılabilir adli istinabe sözleşmelerine kapsamında işleme alınması mümkün olmayacaktır. Zira verilerin yerleri sürekli olarak değiştirilmekte ve tüm parçalar toplanabilse dahi bunların birleştirilmesi yine bir sorun olarak karşımıza çıkmaktadır. Dağınık bulut bilişim sistemi modelinin adli makamlar tarafından yapılan bilgi talepleri açısından en büyük sonucu, bilgi taleplerinin verinin bulunduğu yere göre değil; veriye erişilebilen yere göre yapılması ihtiyacını doğurmuş olmasıdır.

Dağınık bulut bilişim modelini kullanan en önemli bulut bilişim sağlayıcı **Google**'dir<sup>363</sup>. **Google** şirketler topluluğuna ait veri merkezleri<sup>364</sup> bu modelde çalışmakta olup bu veri merkezleri üzerinden sunulan hizmetler kapsamındaki veriler de bu şekilde saklanmaktadır. **Google** bulut sistemi içerisinde bulunan verilere erişim ise sadece ABD'de bulunan genel merkez vasıtasıyla gerçekleştirilebilmektedir<sup>365</sup>.

---

<sup>362</sup> Schwartz, "Legal Access To The Global Cloud", s. 1695; In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 7. Ayrıca, Google veri merkezleri ve konumları hakkında bilgi için bkz. <https://www.google.com/about/datacenters/locations/>.

<sup>363</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 7; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1929-1930; Schwartz, "Legal Access To The Global Cloud", s. 1695.

<sup>364</sup> Google şirketler topluluğuna ait veri merkezleri hakkında bilgi için bkz. <https://www.google.com/about/datacenters/>.

<sup>365</sup> Paul Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", **Computer Law Review International**, S. 1, 2019, s. 6, (Çevrimiçi) <https://paulschwartz.net/wp-content/uploads/2020/08/Schwartz-Peifer-Data-Localization-CRi-2019-1.pdf>, 27.09.2020; Schwartz, "Legal Access To The Global Cloud", s. 1695.

### 3. Erişim Yetkisi Ayırıştırılmış Bulut Bilişim Sistemi

Erişim yetkisi ayırıştırılmış bulut bilişim sistemleri modelinde temel olarak bulut bilişim sisteminin işletilmesi ile bulut bilişim sistemi içerisindeki verilere erişim imkânı ayırıştırılarak farklı kişilere verilmektedir<sup>366</sup>. Böylelikle bulut bilişim sistemini işleten kişinin ya da (devletler dahil) diğer üçüncü kişilerin, bulut bilişim sistemi üzerindeki verilere erişmesi, verilere erişim imkanını yöneten kişinin kontrolüne bırakılmaktadır.

Erişim yetkisi ayırıştırılmış bulut bilişim sistemleri modeli, önde gelen bulut bilişim sağlayıcılarından, sadece **Microsoft** tarafından Almanya'ya özgü olarak uygulanmaktadır<sup>367</sup>. Almanya'da bulunan **Microsoft** veri merkezlerinin işletmesi **Microsoft** tarafından yapılmakta; verilere erişim imkanları ise **T-Systems** adlı bir Alman şirketi tarafından yönetilmektedir<sup>368</sup>. Söz konusu sistem, ABD istihbarat kurumlarının bulut sistemlerine erişimlerine ilişkin haberlerin basına yansımaları üzerine kurulmuştur<sup>369</sup>. Ancak bu sisteme yeni müşteri kabulü gerek yeni talep olmaması gerekse bu modelde çalışan veri merkezlerinin, diğer veri merkezleri ile birlikte çalışamamalarından dolayı yeterli teknolojik imkanları sağlayamaması nedenleriyle 2018 yılında durdurulmuştur<sup>370</sup>.

---

<sup>366</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 100; Schwartz, "Legal Access To The Global Cloud", s. 1697-1699.

<sup>367</sup> "Microsoft Cloud Germany", **Microsoft**, 2016, (Çevrimiçi) <https://go.microsoft.com/fwlink/?LinkId=839380&clcid=0x409>; Esat Dedeze, "Microsoft to Deliver Cloud Services From New Datacentres in Germany in 2019 to Meet Evolving Customer Needs", 31.08.2018, (Çevrimiçi) <https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/>, 06.06.2022.

<sup>368</sup> Sinha, Amber, Elonnai Hickok, Udbhav Tiwari, Arindrajit Basu, "Cross Border Data-Sharing and India A Study in Processes, Content and Capacity", **The Centre for Internet & Society**, s. 29, (Çevrimiçi) <https://cis-india.org/internet-governance/files/mlat-report>, 19.05.2020; "Microsoft Cloud Germany"; Schwartz, "Legal Access To The Global Cloud", s. 1698; Fred H. Cate, James X. Dempsey, **Systematic Government Access to Private-Sector Data Bulk Collection**, New York, NY, USA, Oxford University Press, 2017, s. 86-87; Theodore Christakis, **Lawful Access To Data: The Us V. Microsoft Case, Sovereignty In The Cyber-Space And European Data Protection**, CEIS and The Chertoff Group, 2017, s. 33; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 100; Schwartz, "Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies", s. 2.

<sup>369</sup> Glyn Moody, "Microsoft Building Data Centers in Germany That US Government Can't Touch", **Ars Technica**, 11.12.2015, (Çevrimiçi) <https://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>, 09.07.2021.

<sup>370</sup> Yahya Mohamed Mao, "Microsoft Announces the End of the Germany Cloud", 12.10.2018, (Çevrimiçi) <https://hackernoon.com/microsoft-announces-the-end-of-the-germany-cloud-431bbe407b94>, 06.07.2022.

Daha önce açıklanan lokal bulut bilişim sistemi modeli ile dağıtık bulut bilişim sistemi modeli kapsamında veriye adli makamların erişimi konusunda en kritik hususların veri merkezinin konumu ya da veriye erişilebilen yer olduğu görülmüştür. Erişim yetkisi ayrıştırılmış bulut bilişim sistemi modeli ise erişim imkanını, bulut sistemi sağlayıcılardan almak suretiyle bu soruna bir çözüm sunabilecek niteliktedir. Zira böyle bir durumda yurtdışında bulunan bir veri merkezinin erişim imkanlarını yöneten ve yurtiçinde yerleşik kişiye yönelik adli makamlardan gelecek bir bilgi talebi; o kişi tarafından adli istinabe prosedürlerine gerek kalmaksızın yurtiçindeki prosedürlere göre yanıtlanabilecektir<sup>371</sup>. Özellikle verinin fiziki bir varlık olmadığını ve sınırsız olarak kopyalanabildiğini düşündüğümüzde; kanaatimizce bu model hukuki veri lokalizasyonu yükümlülüklerine alternatif olabilecek niteliktedir. Modelin kullanımı ile veriye erişim imkânı lokal bir şirkete verilerek verinin konumuna müdahale edilmemesi, bulut bilişimi hizmetlerinin kullanımını tamamen engelleyen hukuki düzenlemelerin ortadan kalkmasını sağlayacaktır. Bu durum aynı zamanda bulut bilişim sisteminde bulunan verilere erişime yönelik zorlukları ortadan kaldıracaktır. Öte yandan bu modelin teknik açıdan getirebileceği kısıtlamaların da değerlendirilmesi gerekmektedir.

### III. ABD HUKUKU ÇERÇEVESİNDE DİJİTAL ORTAMDAKİ BİLGİLERE ERİŞİM İMKANLARI

#### A. Giriş

ABD, dünya üzerindeki teknoloji şirketlerinin büyük çoğunluğuna ev sahipliği yapmaktadır. Her ne kadar global anlamda yaygın kullanım oranlarına sahip olan **Facebook, Microsoft, Google** ya da **Amazon** gibi bulut bilişim sağlayıcıları dünyanın çeşitli yerlerinde veri saklamakta olsalar da hepsinin ana yönetim merkezleri ABD sınırları içerisinde yer almaktadır<sup>372</sup>. İşte bu nedenle ABD hukukunun ceza

---

<sup>371</sup> Önemle belirtmek gerekir ki böyle bir senaryoda dahi ülkeler arasında kanunlar ihtilafı sorunları doğabilecektir. Zira erişim imkanına sahip şirketin, kendisinin bulunduğu ülke adli makamlarının kararlarını yerine getirmesi, veri merkezinin bulunduğu ülke hukukunu ihlal edebilir.

<sup>372</sup> Krista Peace, “Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation”, **North**

yargılaması usulü mevzuatı çerçevesinde adli makamların dijital ortamda bulunan bilgilere erişim imkânlarının anlaşılması kritiktir. Zira bu imkanlar hem bahse konu şirketlerin tüm dünyadaki faaliyetlerini etkilemektedir hem de tüm devletler için kamu güvenliğinin tesisi noktasında da büyük önem arz etmektedir. Ülkemiz açısından konuya baktığımızda ise ana yönetim merkezleri ABD’de bulunan bulut bilişim sağlayıcılarının hizmetlerinden yararlanan Türk gerçek ve tüzel kişilerinin bilgilerine erişilmesinin hangi kurallara tabi olduğunun anlaşılması faydalı olacaktır. Son olarak belirtmek gerekir ki ABD hukuku, ülkemizde adli makamların dijital ortamdaki bilgilere erişim imkânlarına ilişkin yapılabilecek yeni düzenlemelere örnek teşkil edebilecek niteliktedir.

ABD hukukunda konuyla ilgili temel düzenleme Federal Anayasanın Dördüncü Değişikliğidir<sup>373</sup>. Dördüncü Değişiklik, temel olarak mahkeme kararı (**warrant**)<sup>374</sup> olmadan arama ya da el koyma (insanlar için alıkoyma) işlemlerinin yapılamayacağını düzenlemektedir. Dijital ortamda bulunan bilgilerin verilmesi ya da erişime açılmasına ilişkin talepler de Dördüncü Değişiklik kapsamında arama işlemi olarak kabul edilmektedir. Dördüncü Değişiklik, ABD Yüksek Mahkemesi kararları çerçevesinde tüm federe devletlerde uygulama alanı bulmaktadır<sup>375</sup>. Dördüncü Değişikliğin Türkçe tercümesi<sup>376</sup> aşağıda paylaşılmaktadır:

---

**Carolina Journal of International Law**, C. 47, 2022, s. 418; Philip J. Pullen, “Nail in the MLAT Coffin: Examining Alternatives Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing”, **North Carolina Journal of International Law**, C. 44, S. 1, 2018, s. 3-4; Gail Kent, “The Mutual Legal Assistance Problem Explained”, **Stanford Law School**, 23.02.2015, (Çevrimiçi) <https://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>, 06.05.2022.

<sup>373</sup> Özgün hali ile *Fourth Amendment* şeklindedir, bkz. “Bill of Rights - Fourth Amendment [Search and Seizure]”, (1791), (Çevrimiçi) [https://www.law.cornell.edu/constitution/fourth\\_amendment](https://www.law.cornell.edu/constitution/fourth_amendment).

<sup>374</sup> ABD hukukunda arama, el koyma ya da bilgi talepleri gibi işlemler genellikle mahkemelerin verdikleri kararlar ile gerçekleştirilmektedir. Ancak bu kararların aradıkları koşullar bakımından farklı isimlerle adlandırıldıkları görülmektedir. En sıkı koşulları arayan karar tipi “**warrant**” olarak adlandırılmaktadır. Biz de bu terimin karşılığını ABD hukukundan bahsedilen kısımlar boyunca “mahkeme kararı” olarak adlandıracamız.

<sup>375</sup> Neil Richards, “The Third Party Doctrine and the Future of the Cloud”, **Washington University Law Review**, C. 94, S. 6, 2017, s. 1452. ABD'deki her eyaletin kendine özgü anayasası olduğundan her eyalet/devlet kendi sınırları içerisindeki anayasal korumadan yararlanmaktadır. Şöyle ki, birleşik devletlerden herhangi birinde uygulanan anayasal haklar diğerinde uygulanmayabilir. Bu sebeple önemle belirtmek gerekir ki, Dördüncü Değişiklik tüm federe devletlerde uygulama alanı bulmaktadır.

<sup>376</sup> Orijinal hali için bkz.: “*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue,*

*“İnsanların kişiliklerine, evlerine, belgelerine ve eşyalarına karşı yapılacak makul olmayan arama ve el koymalara (insanlar için alıkoyma) karşı güvende olma hakkı ihlal edilemez ve yemin ya da doğruluk beyanı ile desteklenen makul şüpheye dayanmayan ve aranacak yeri ya da el konulacak şeyi ya da alıkonulacak kişiyi özel olarak tarif etmeyen mahkeme kararları verilemez.”<sup>377</sup>*

Dördüncü Değişiklik yanında ABD hukukuna ilişkin önemli kaynaklardan bir diğeri de Yüksek Mahkeme’nin Dördüncü Değişiklik kapsamında karara bağladığı davalarlardır. ABD Kongresi’nin<sup>378</sup> çıkarmış olduğu federal kanunlar ile diğer mahkemelerin verdikleri kararlar da dikkate alınması gereken kaynaklardır. Öte yandan belirtmek gerekir ki işbu çalışma kapsamında sadece federal hukuk kuralları çerçevesinde inceleme yapılacaktır ve federe devletlerin iç mevzuatı ile ilgili konulara değinilmeyecektir.

## **B. Dördüncü Değişiklik Kapsamında Bilgi Talepleri**

### **1. Dördüncü Değişiklik Hakkında Genel Bilgiler**

Dördüncü Değişiklik, kişilerin alıkonmasını ya da kişilerin üzerlerinin veya makul derecede gizlilik beklentisi içinde bulundukları yerlerin aranmasını sınırlamaktadır<sup>379</sup>. Dördüncü Değişikliğin, Haklar Bildirgesi<sup>380</sup> (**Bill of Rights**) içerisinde yer almasının sebebi Amerikan Devrimi sırasında Britanya İmparatorluğu’nun genel arama kararları vasıtasıyla kişi ya da yer ayrımı gözetmeksizin dilediğince arama ve el koyma

---

*but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”*

<sup>377</sup> Çeviri yazara ait olup çeviri metninde kullanılan terimler, Türk Hukukundaki olası anlamları ile kullanılmamıştır. Bu terimlerin anlamları, ABD Hukukundaki karşılıklarının dikkate alınması yoluyla yorumlanmalıdır.

<sup>378</sup> Özgün adı ile *U.S. Congress* olan ABD Kongresi hakkında bilgi için bkz. The Editors of Encyclopaedia, “Congress of the United States”, **Encyclopedia Britannica**, 13.12.2022, (Çevrimiçi) <https://www.britannica.com/topic/Congress-of-the-United-States>, 17.07.2021.

<sup>379</sup> Bill of Rights - Fourth Amendment [Search and Seizure]. Ayrıca bkz. Secil Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, **Harvard Journal of Law & Technology**, C. 32, S. 1, 2018, s. 324-325; Diana Benton, “Seeking Warrants for Unknown Locations: The Mismatch between Digital Pegs and Territorial Holes”, **Emory Law Journal**, C. 68, S. 1, 2018, s. 190; Schwartz, “Legal Access To The Global Cloud”, s. 1709.

<sup>380</sup> Haklar Bildirisi, orijinal adı ile *Bill of Rights*, 15 Aralık 1791 tarihinde ABD Anayasası’na dahil edilen 10 ek maddeden oluşmaktadır. Dördüncü Değişiklik, Haklar Bildirisi’ne eklenen söz konusu maddelerden biridir. Detaylar için bkz. “United States Bill of Rights”, (1791), (Çevrimiçi) <https://www.law.cornell.edu/constitution/billofrights>, 10.10.2022.

işlemleri yapmasıdır<sup>381</sup>. Bu uygulamanın yarattığı tepki, Dördüncü Değişiklik vasıtasıyla kamu gücüne bir denge ve sınırlama getirilmesi düşüncesini doğurmuştur.

Dördüncü Değişikliğin uygulama alanı son derece geniştir. Dördüncü Değişiklik için uygulanma alanlarından birisi kişilerin alıkonması (gözaltına alınma gibi) halleridir. Diğer alanlar ise kişinin yaşam alanlarının, işyerinin, üzerinin veya motorlu taşıtlarının aranması ile buralarda bulunacak eşyalara el konulmasıdır. Yeni teknolojilerin yarattığı sorunlar başta olmak üzere toplumun geçirdiği değişimlere göre Dördüncü Değişikliğin uygulama alanı da sürekli olarak değişmekte ve genişlemektedir.

Dördüncü Değişiklik, ABD Federal Anayasasında açıkça düzenlenmeyen özel hayatın gizliliği hakkı ile de yakın bir ilişki içerisindedir. Çünkü yapılan her arama, alıkoyma veya el koyma işlemi aynı zamanda kişilerin özel hayatının gizliliği hakkının da ihlal edilmesi sonucunu doğurmaktadır. Teknolojik gelişmelere bağlı olarak dijital ortamın genişlemesinin en önemli sonuçlarından birisi de kişisel verilerin korunması da dahil olmak üzere özel hayatın gizliliği hakkının öneminin ciddi bir şekilde artmış olmasıdır. Adli makamlarının dijital ortamdaki bilgilere erişmesi, Dördüncü Değişiklik kapsamında arama işlemi olarak kabul edilmekte ve özel hayatın gizliliği hakkı ile çelişki yaratmakta olduğu için Dördüncü Değişiklik, çalışmamızın bu bölümünün merkezine oturmuş durumdadır.

Yukarıdaki açıklamalar ışığında, sonraki bölümlerde ilk önce Dördüncü Değişiklik ile özel hayatın gizliliği hakkının ilişkisi incelenecektir. Bundan sonra Dördüncü Değişiklik kapsamında arama yapılmasına ilişkin şartlar değerlendirilecektir. Son kısımda ise Yüksek Mahkeme uygulamaları ile Dördüncü Değişiklik uygulamasının tarih boyunca teknolojik gelişmelere göre nasıl uyarlandığı açıklanacaktır.

---

<sup>381</sup> Laura Temme, “The Fourth Amendment - Unreasonable Search and Seizure”, **FindLaw**, 2019, (Çevrimiçi) <https://constitution.findlaw.com/amendment4.html>, 04.08.2019.

## 2. Dördüncü Değişikliğin Özel Hayatın Gizliliği Hakkı (Right to Privacy) ile İlişkisi

Özel hayatın gizliliği hakkı, ABD Federal Anayasası'nda açıkça tanımlanmayan ancak gölge hak (**penumbra**) olarak varlığı kabul edilen bir anayasal haktır<sup>382</sup>. Yüksek Mahkeme **Griswold v. Connecticut** kararında<sup>383</sup>; Birinci Değişiklikte yer alan toplanma hakkının<sup>384</sup>, Üçüncü Değişiklikte yer alan askerlerin konutlara konuşlandırılması yasağının<sup>385</sup>, Dördüncü Değişikliğin getirdiği arama, alıkoyma veya el koymaya ilişkin sınırlandırmaların<sup>386</sup>, Beşinci Değişikliğin getirdiği suçu kabule zorlama yasağının<sup>387</sup> ve Dokuzuncu Değişiklikte yer alan Federal Anayasa içinde bazı hakların sayılmasının toplumun sahip olduğu diğer hakların bireylerden esirgendiği ya da bu hakların daha düşük seviyede olduğu şeklinde yorumlanamayacağı kuralının<sup>388</sup>; kişiler için çok sayıda mahremiyet alanları oluşturduğunu ifade ederek bunların özel hayatın gizliliği hakkını bir gölge hak olarak oluşturduğu sonucuna varmıştır<sup>389</sup>. Ayrıca bu kararda özel hayatın gizliliği hakkının Haklar Bildirgesinden daha eski olduğu da ifade edilmiştir<sup>390</sup>. **Griswold v. Connecticut** kararından beri özel hayatın gizliliği hakkı bir anayasal hak olarak kabul edilmektedir<sup>391</sup>.

Yüksek Mahkemenin **Katz v. United States** kararında ise özel hayatının gizliliği hakkının yaygın kullanılan tanımı yapılmıştır. Bu tanıma göre özel hayatın gizliliği hakkı, diğer kişiler tarafından yalnız bırakılmayı isteme hakkıdır<sup>392</sup>.

<sup>382</sup> Rolando V. del Carmen, Craig Hemmens, **Criminal Procedure Law and Practice**, 10. bs, Boston, Cengage Learning, 2017, s. 188; Mallory Ursul, "The States' Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause Notes", **Suffolk University Law Review**, C. 52, S. 4, 2019, s. 583-584.

<sup>383</sup> **Griswold v. Connecticut**, C. 381, C. 381 U.S. Reports 479, (U.S. Supreme Court 1965).

<sup>384</sup> "Bill of Rights - First Amendment [Religion, Speech, Press, Assembly, Petition]", (1791), (Çevrimiçi) [https://www.law.cornell.edu/constitution/first\\_amendment](https://www.law.cornell.edu/constitution/first_amendment).

<sup>385</sup> "Bill of Rights - Third Amendment [Quartering of Troops]", (1791), (Çevrimiçi) [https://www.law.cornell.edu/constitution/third\\_amendment](https://www.law.cornell.edu/constitution/third_amendment).

<sup>386</sup> Bill of Rights - Fourth Amendment [Search and Seizure].

<sup>387</sup> "Bill of Rights - Fifth Amendment [Grand Jury, Double Jeopardy, Self-Incrimination, Due Process]", (1791), (Çevrimiçi) [https://www.law.cornell.edu/constitution/fifth\\_amendment](https://www.law.cornell.edu/constitution/fifth_amendment).

<sup>388</sup> "Bill of Rights - Ninth Amendment [Non-Enumerated Rights]", (1791), (Çevrimiçi) [https://www.law.cornell.edu/constitution/ninth\\_amendment](https://www.law.cornell.edu/constitution/ninth_amendment).

<sup>389</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 188-189.

<sup>390</sup> **Griswold v. Connecticut**, 381 U.S. Reports de 484.

<sup>391</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 189.

<sup>392</sup> **Katz v. United States**, C. 389, C. 389 U.S. Reports 347, (U.S. Supreme Court 1967).



Özel hayatın gizliliği hakkının uygulanabileceği olaylar neredeyse sınırsızdır. Bu nedenle hangi durumlarda özel hayatın gizliliği hakkının Federal Anayasa çerçevesinde korunacağı sorusu önem kazanmaktadır. Yüksek Mahkeme bu soruyu, kişinin gizlilik beklentisinin makul olduğu durumlarda özel hayatın gizliliği hakkının anayasal korumaya sahip olacağı şeklinde yanıtlamıştır<sup>393</sup>.

Kişinin gizlilik beklentisinin makul olduğu durumların belirlenmesi için Yüksek Mahkeme iki koşul belirlemiştir<sup>394</sup>. Bunlardan ilki kişinin fiili olarak gizlilik beklentisi içerisinde olduğunu göstermesidir. İkinci koşul ise kişinin gizlilik beklentisinin toplum tarafından makul karşılanabilir olmasıdır. Örnekle açıklamak gerekirse kalabalık bir ortam içerisinde bağırarak telefonla konuşan bir kişinin hem fiili olarak bir gizlilik beklentisi içinde olduğunu söylemek mümkün değildir hem de toplumun bu gizlilik beklentisini makul karşılaması söz konusu olmayacaktır. Öte yandan evli bir çiftin yatak odalarında gizlilik beklentisi içerisinde olmaları hem makul bir beklentidir hem de bu beklenti toplum tarafından kabul edilebilirdir<sup>395</sup>. Dolayısıyla ilk örnekteki kişinin konuşmalarını duyan kişiler açısından özel hayatın gizliliği hakkının anayasal bir korumaya sahip olmayacağı sonucuna varılmaktadır. Ancak ikinci örnekteki evli çiftin özel hayatın gizliliği hakkı, anayasal bir korumaya sahip olacaktır.

Toplumun hangi durumları makul bulabileceği zaman içerisinde özellikle teknolojik gelişmeler ve bunların insan yaşayışı üzerindeki etkileri ve değişen ahlaki değerlere bağlı olarak değişim göstermektedir. Bu nedenle toplumun hangi durumlarda gizlilik beklentisini makul bulabileceği konusu her somut olaydaki koşullara göre değerlendirilmelidir<sup>396</sup>. Nitekim bu yaklaşım, hukukun toplum hayatının yeni gereklerine uyum sağlayabilmesine imkân vermektedir.

---

<sup>393</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 189; Katz v. United States, 389 U.S. Reports de 361.

<sup>394</sup> Katz v. United States, 389 U.S. Reports de 361.

<sup>395</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 189.

<sup>396</sup> Carmen, Hemmens, **a.y.**

Arama işlemi, kişilerin makul gizlilik beklentisine sahip olduğu yerlerde iddia makamı<sup>397</sup> tarafından bir suç soruşturması için delil aranması anlamına gelmektedir<sup>398</sup>. Bu tanımdan da anlaşılabileceği üzere arama sadece kişilerin evlerinde ya da işyerlerinde değil makul derecede gizlilik beklentisine sahip oldukları kamusal alanlar da dahil olmak üzere her yerde yapılabilmektedir<sup>399</sup>. Yeni teknolojik gelişmeler ışığında oluşan dijital ortamın, kişilerin makul gizlilik beklentisine sahip olduğu yerlerden biri olarak sayılıp sayılamayacağı sorunu ABD hukukunda gündeme gelmiştir. Nitekim aşağıda detayları ile açıklanan Dördüncü Değişikliğe ilişkin Yüksek Mahkeme kararları, ABD Kongresi’ni bu sorunun yanıtının olumsuz olduğunu düşünmeye itmiştir. Bu eğilim neticesinde de dijital ortamda da kişilerin özel hayatlarının gizliliğinin sağlanması amacıyla 1986 yılında SCA<sup>400</sup> çıkarılmıştır. SCA ile birlikte adli makamlarının dijital ortamdaki bilgilere erişmesi de arama işlemi olarak kabul edilmeye başlanmıştır. Günümüze kadar geçen zaman içerisinde verilen güncel Yüksek Mahkeme kararları söz konusu sorunun yanıtının olumlu olduğunu göstermektedir.

### 3. Dördüncü Değişiklik Kapsamında Arama İşlemi Yapılmasının Şartları

Dördüncü Değişiklik kapsamında arama işleminin gerçekleştirilebilmesinin temel şartı bu konuda bir mahkeme kararı alınmasıdır. Ancak istisnai durumlarda mahkeme kararı olmaksızın arama işlemi gerçekleştirilebilmektedir. Bu bölüm altında öncelikle arama işlemi yapılabilmesi için mahkeme kararı alınmasının şartları incelenecektir. Daha sonra da mahkeme kararı alınması kuralının istisnaları üzerinde durulacaktır.

<sup>397</sup> ABD hukuk kaynaklarında, ceza yargılaması kapsamında arama ya da el koyma işlemi için talepte bulunan taraf “**government**” terimi ile anılmaktadır. Söz konusu terim ile kastedilen esasen adli kolluk makamları (polis ya da FBI) ile mahkemelerde görev yapan savcılıklardır. Anlatımı gereksiz detaylardan arındırmak ve Türk hukukunda yer alan kavramlara yakınlaşmak adına “**government**” teriminin tercümesi olabilecek “devlet” ya da “hükümet” terimleri yerine “**government**” teriminin karşılığı olarak “iddia makamı” ifadesi kullanılacaktır.

<sup>398</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 190.

<sup>399</sup> Katz v. United States, 389 U.S. Reports de 351.

<sup>400</sup> Özgün adı ile *Stored Communications Act* denmektedir, bkz. <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>.

### a. Arama İşlemi İçin Mahkeme Kararı Verilmesinin Şartları

Yukarıda da belirtildiği üzere, arama işleminin yapılabilmesi için Dördüncü Değişiklik ile gelen ana kural bu konuda bir mahkeme kararı alınmasıdır. Yüksek Mahkeme'nin **Johnson v. United States**<sup>401</sup> kararında belirtildiği üzere Dördüncü Değişiklik ile arama işlemleri için mahkeme kararı gerektirmesinin gerekçesi, korumanın halihazırda soruşturmaya taraf olan bir memur tarafından değil, tarafsız ve bağımsız bir hâkim tarafından sağlanmasını temin etmektir<sup>402</sup>. Dolayısıyla mahkeme kararının tarafsız ve bağımsız bir hâkim tarafından verilmesi, ilgili arama işlemi neticesinde elde edilen delillerin hükme esas alınabilmesi açısından önem arz etmektedir. Nitekim çeşitli Yüksek Mahkeme kararlarında, verdiği arama kararı başına ek ücret alan bir hâkimin<sup>403</sup> ya da daha önceki soruşturma işlemlerinde görev almış bir hâkimin tarafsız olamayacağına<sup>404</sup> hükmedilmiştir<sup>405</sup>. Ayrıca savcılık makamınca verilen arama kararlarının<sup>406</sup> da tarafsızlık unsurunun bulunmaması nedeniyle geçerli olmayacağı Yüksek Mahkeme tarafından kararlaştırılmıştır<sup>407</sup>.

Tarafsız ve bağımsız hâkim kararı kuralı haricinde arama işlemini gerçekleştirmek için mevcut olması gereken diğer şartlar; makul şüphe bulunması, destekleyici yemin ya da doğruluk beyanı bulunması ile aramaya konu olacak unsurun açıkça belirlenmesidir. Her bir şart aşağıdaki başlıklar altında incelenecektir.

#### (1) Makul Şüphe Bulunması

Bir suç işlendiğine dair makul şüphe (**probable cause**) bulunması, arama işleminin gerçekleştirilebilmesi için gereken şartlardan birisidir. Makul şüphe, Yüksek Mahkeme tarafından ortalama güvenilirlik seviyesine sahip olan somut bilgiler ve koşullar çerçevesinde; talepte bulunan iddia makamının bilgisinde olan unsurların, ortalama dikkate sahip bir kişiyi bir suçun işlendiğine ya da işlenmekte olduğuna ikna

<sup>401</sup> Johnson v. United States, C. 333, C. 333 U.S. Reports 10, (U.S. Supreme Court 1947).

<sup>402</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 190; Jefferson L. Ingram, **Criminal Procedure: Theory and Practice**, 3. bs, Routledge, 2022, s. 350-354.

<sup>403</sup> Connally v. Georgia, 429 U.S. 245 (1977), (U.S. Supreme Court 10 Ocak 1977).

<sup>404</sup> Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979), (U.S. Supreme Court 11 Haziran 1979).

<sup>405</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 198-199.

<sup>406</sup> Coolidge v. New Hampshire, 403 U.S. 443 (1971), (U.S. Supreme Court 21 Haziran 1971).

<sup>407</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 198-199.

edecek seviyede şüphe yaratması olarak tanımlanmıştır<sup>408</sup>. Yüksek Mahkeme'nin yaptığı değerlendirme, tanımdan da anlaşılabilceği üzere son derece soyut ve görecelidir. Bu nedenle her somut olayda makul şüphenin varlığının yeniden değerlendirilmesi gerekmektedir.

Makul şüphenin tespitinde önemli bir kavram olan ortalama dikkate sahip bir kişi terimi, hukuk alanında eğitim görmüş bir kişiyi değil; esnaf, öğretmen ya da kasap gibi sıradan insanları kastetmektedir<sup>409</sup>. Öte yandan Yüksek Mahkeme, polis memurlarının sıradan insanlara göre suç işlenmesi konusunda makul şüpheyi daha iyi tespit edebileceğini ifade ederek objektif ve ortalama bir polis memurunun algısının makul şüphenin tespitinde bir kriter olarak kabul edilebileceğini de ifade etmiştir<sup>410</sup>.

Yüksek Mahkeme'nin verdiği karmaşık ve göreceli tanım yanında makul şüphenin uygulamaya yönelik bir tanımı daha bulunmaktadır. Buna göre, eğer bir suç işlendiği konusunda %50'den fazla oranla emin olunabiliyorsa olayda makul şüphenin varlığı sonucuna varılmalıdır<sup>411</sup>. Önemle belirtmek gerekir ki bu tanımlama, Yüksek Mahkeme'nin kullandığı bir oran ya da verdiği bir tanım değildir.

Mahkemelerce arama işlemleri için karar verildiği durumlarda, arama yapılacak yerde bir delil bulunmasının mümkün olup olmadığı da makul şüphenin varlığına ilişkin değerlendirilmeye dahil edilmektedir<sup>412</sup>.

## (2) Destekleyici Yemin ya da Doğruluk Beyanı Bulunması

Arama izni talebinde bulunmak için talepte bulunan iddia makamı tarafından (genellikle yerel polis ya da FBI) mahkemeye yazılı bir ifade (**affidavit**) sunulmaktadır<sup>413</sup>. Bu ifade yeminli bir ifadedir. Dini sebeplerle yemin etmek

---

<sup>408</sup> Carmen, Hemmens, **a.g.e.**, s. 68.

<sup>409</sup> Carmen, Hemmens, **a.y.**

<sup>410</sup> United States v. Ortiz, 422 U.S. 891 (1975), (U.S. Supreme Court 30 Haziran 1975); Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 69; Ingram, **Criminal Procedure: Theory and Practice**, s. 233-236.

<sup>411</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 69.

<sup>412</sup> Carmen, Hemmens, **a.g.e.**, s. 221.

<sup>413</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 233-236; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 195.

istemeyen kişiler de yemin ile aynı hukuki güce sahip olan doğruluk beyanında bulunmak zorundadır<sup>414</sup>.

Söz konusu yazılı ifade; olay, makul şüpheyi ispatlayan unsurlar ve aramaya konu unsur hakkında bilgiler içermektedir<sup>415</sup>. Söz konusu bilgilerin güncel olması da mutlak bir gerekliliktir<sup>416</sup>. Mahkeme, arama kararını bu belge üzerinden vermektedir. Ek olarak belirtmek gerekir ki yazılı ifade yerine sözlü ifadelere dayanarak da mahkemenin karar vermesi mümkündür<sup>417</sup>.

### (3) Aramaya Konu Unsurun Açıkça Belirtilmesi

Dördüncü Değişikliğin getirdiği bir diğer şart da aramaya konu olan unsurun, mahkeme kararı içerisinde açıkça tanımlanması zorunluluğudur. Örnek vermek gerekirse arama kararının uygulanabilmesi için söz konusu apartmanın adresinin verilmesi yeterli değildir. Apartmanda bulunan dairelerden hangisinin aranacağı da belirlenmelidir<sup>418</sup>.

Dijital ortamda bulunan bilgilere erişim taleplerinde ise bu husus, talep edilen bilgiye ilişkin tanımlayıcı unsurların da mahkeme kararına eklenmesini gerektirir. Örneğin bir e-posta içeriği talep ediliyorsa bu e-postanın tarihi veya atılmış olabileceği tarih aralıkları ile göndericisinin ve alıcısının belirtilmesi gerekmektedir<sup>419</sup>.

Aramaya konu unsurun belirlenmesi kriterinin istisnası ise yine bir Yüksek Mahkeme kararı içerisinde belirtilmiştir. **Maryland v. Garrison** kararına<sup>420</sup> konu olayda iddia makamı tarafından arama kararına konu olan adres, sadece ilgili apartmanın üçüncü

<sup>414</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 195.

<sup>415</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 234.

<sup>416</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 196.

<sup>417</sup> Carmen, Hemmens, **a.g.e.**, s. 195.

<sup>418</sup> Carmen, Hemmens, **a.g.e.**, s. 196.

<sup>419</sup> Orin S. Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't", **Northeastern University Law Review**, C. 97, S. 2, 2003, s. 610-615; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 219; Lin, "Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption", s. 1101.

<sup>420</sup> **Maryland v. Garrison**, C. 480, C. 480 U.S. Reports 79, (U.S. Supreme Court 1986).

katı olarak beyan edilmiştir<sup>421</sup>. Mahkeme kararına aramaya konu adres bu şekilde yansıtılmıştır. Ancak arama işlemini yapacak görevli polisler adrese geldiklerinde, apartmanın üçüncü katında iki ayrı dairenin var olduğunu görmüşlerdir<sup>422</sup>. Bunlardan birisine giren polis, aramaya ilişkin mahkeme kararına konu olan kişinin değil; **Garrison** adlı kişinin evine girdiğini fark etmiştir. Ancak polis hatasını anlamadan önce **Garrison**'un evinde uyuşturucu madde bulunmuştur. **Garrison**, söz konusu arama kapsamında elde edilen delillerin, aramaya ilişkin mahkeme kararı olmaması nedeniyle hükme esas alınamayacağını iddia etmiştir. Olay hakkında karar veren Yüksek Mahkeme, mahkeme kararının çıkarıldığı sırada iddia makamı tarafından doğru bilgilerin toplanması için makul derecede çaba gösterilmesine rağmen yine de bir hata meydana gelmişse bu mahkeme kararının geçerliliğini koruyacağına karar vermiştir. Dolayısıyla **Garrison**'un itirazları kabul edilmemiştir.

#### **b. Mahkeme Kararı Olmaksızın Arama İşlemi Yapılmasına İmkân Veren İstisnalar**

Dördüncü Değişiklik kapsamında ana kural, arama işlemlerinin mahkeme kararına dayanarak gerçekleştirilmesidir. Ancak bu kurala Yüksek Mahkeme kararları ile az sayıda ve sınırları net bir şekilde çizilmiş istisnalar getirilmiştir<sup>423</sup>. İstisnaların varlığı halinde dahi arama neticesinde elde edilen delillerin hükme esas alınabilmesi için arama talebinde bulunan iddia makamının, daha sonradan makul şüphenin varlığını ispatlaması gerekmektedir.

Mahkeme kararı olmadan arama yapılabilecek istisnai yedi adet durum bulunmaktadır<sup>424</sup>. Bunlardan suç şüphesi halinde durdurma, motorlu araçların aranması, idari arama veya denetimler, kişinin alıkonmasına bağlı arama ve özel durum aramalarına (devlet okullarında yapılan aramalar, öğrencilerin uyuşturucu testlerine sokulması, havalimanı aramaları ile şartlı tahliyede bulunan kişilerin aranması) ile rızaya ilişkin istisnalar konu olarak bu çalışma kapsamı dışındadır.

<sup>421</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 221.

<sup>422</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 197.

<sup>423</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 244; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 199-209.

<sup>424</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 206.

Acil durumlarda mahkeme kararı olmaksızın arama yapılmasına ilişkin istisna kural, başta bu çalışma kapsamı içerisine girebilecek gibi görünmekteyse de bu husustaki Yüksek Mahkeme kararları incelendiğinde aksi durumun mevcut olduğu anlaşılmaktadır. Zira bu kategorideki istisna kuralları; bir memura fiziki zarar verilmesi ya da delil yok edilmesine dair yakın ve gerçek tehdit olması,<sup>425</sup> şüphelilerin sıcak takibi sırasında yapılacak aramalar,<sup>426</sup> üçüncü kişilerin yardım çağrılarına yanıt verilmesi<sup>427</sup> ya da alkollü araç süren kişilerden kan örneği alınması<sup>428</sup> hususlarını düzenlemektedir.

Arama işlemi için mahkeme kararına ihtiyaç duyulmayan istisnai durumlar Yüksek Mahkeme kararları çerçevesinde şekillendiğinden gelecekte verilecek kararlarla istisnaların değişmesi mümkündür.

#### 4. Dördüncü Değişiklik Uygulamasına Teknolojik Gelişmelerin Etkisi

1791 tarihli Haklar Bildirgesi ile yürürlüğe giren Dördüncü Değişiklik posta, telgraf, telefon ve veri aktarım sistemleri (GPS, cep telefonu sinyalleri veya internet gibi) gibi insanlık tarihi üzerinde büyük etkileri olan iletişim sistemleri vasıtasıyla gerçekleştirilen iletişimlere, devlet müdahalesinin sınırlandırılması konusunda her dönemin şartlarına uygun koruma sağlayabilmiştir. Söz konusu korumanın sağlanabilmesi, Dördüncü Değişikliğin şartlarına uygun şekilde Yüksek Mahkeme tarafından yorumlanması neticesinde mümkün olmuştur. Bu çalışmanın konusunun daha iyi anlaşılabilmesi adına aşağıda çeşitli teknolojik gelişmelere karşı Dördüncü Değişikliği uyarlayan Yüksek Mahkeme kararları incelenecektir.

---

<sup>425</sup> Vale v. Louisiana, 727, (U.S. Supreme Court 22 Haziran 1970); Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 206-207.

<sup>426</sup> Warden v. Hayden, 480, (U.S. Supreme Court 29 Mayıs 1967). Detaylı bilgi için bkz. Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 207; Ingram, **Criminal Procedure: Theory and Practice**, s. 259.

<sup>427</sup> Brigham City v. Stuart, 05-502, (U.S. Supreme Court 22 Mayıs 2006). Detaylı bilgi için bkz. Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 208.

<sup>428</sup> Schmerber v. California, 658, (U.S. Supreme Court 20 Haziran 1966). Detaylı bilgi için bkz. Ingram, **Criminal Procedure: Theory and Practice**, s. 471-475; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 208.

### a. Posta ve Telgrafın Etkisi

ABD Federal Anayasası, ABD Kongresi'ne postane kurma ve posta yolları oluşturma yetkisi vermektedir<sup>429</sup>. Etkin bir posta sistemine sahip olmak, geniş topraklara yayılmış ve federal sisteme sahip olan ABD'nin kuruluş aşamasında büyük bir önem taşımıştır<sup>430</sup>. Ayrıca Amerikan Devrimi öncesi Britanya Posta Ofisi'nin yine Britanya istihbaratının bir parçası olması nedeniyle ABD'nin kurucuları nezdinde posta sisteminde gizliliğin sağlanması önemli görülmüştür<sup>431</sup>. Bu tecrübe neticesinde toplumda, ABD'nin kurulmasından sonra hızlı bir şekilde, postaların gizli olması ve devlet müdahalesinden korunması gerektiğine dair bir anlayış yerleşmiştir<sup>432</sup>. Nitekim ABD Kongresi tarafından çıkarılan 1792 ve 1825 tarihli kanunlarla<sup>433</sup> bu konuda düzenlemeler yapılmıştır.

1878 yılında ise Yüksek Mahkeme önüne gelen bir davada, Posta Ofisi'nin elinde bulundurduğu mektubu açması için Dördüncü Değişiklik gereğince mahkeme kararına ihtiyaç duyulup duyulmadığı tartışılmıştır. Yüksek Mahkeme **Ex parte Jackson** kararı ile Dördüncü Değişikliğin kişilere sahip oldukları belgeler için makul olmayan aramalara karşı koruma hakkı verdiğini ifade ederek mektupların açılması için de mahkeme kararına ihtiyaç olduğu sonucuna varmıştır<sup>434</sup>. Yüksek Mahkeme'ye göre mektupların bir kamu otoritesi olan Posta Ofisi elinde bulunması, söz konusu Dördüncü Değişiklik korumasının ortadan kalktığı anlamına gelmeyecektir<sup>435</sup>. Toplumda yerleşen postaların gizli olması ve devlet müdahalesinden korunması gerektiğine dair anlayış, söz konusu kararın verilmesinde etkili olmuştur. Öte yandan söz konusu kararın sadece mektupların içeriğini Dördüncü Değişiklik kapsamında

<sup>429</sup> ABD Federal Anayasası'nın 1. Maddesi 8. Bölümünde söz konusu yetki tanınmaktadır.

<sup>430</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1452.

<sup>431</sup> Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't", s. 610-619; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1452-1453.

<sup>432</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1453.

<sup>433</sup> Orijinal isimleri ile *Post Office Act of 1792* ve *Postal Act of 1825* denmektedir. Detayları için bkz. Richards, **a.y.**

<sup>434</sup> *Ex parte Jackson*, C. 96, C. 96 U.S. Reports 727, (ABD Yüksek Mahkemesi 1877).

<sup>435</sup> William Jeremy Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", **The Georgetown Law Journal**, C. 98, 2010, s. 1229; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1452.



korumaya değer bulduğunu, mektup zarfı üzerinde yazarların koruma kapsamında bulunmadığını ifade etmekte yarar vardır.

Telgraf 1844'te icat edilerek kullanılmaya başlanmıştır. Telgraf şebekeleri, posta sisteminden farklı olarak devlet tarafından değil özel şirketler tarafından işletilmektedir. Dolayısıyla her telgraf, özel hukuk tüzel kişisi olan telgraf şirketi tarafından göndericiden alınıp alıcıya ulaştırılmaktadır. Telgraf, pahalı bir hizmet olması nedeniyle toplumun dikkatini posta hizmetleri kadar çekememiştir<sup>436</sup>. Telgraf konusunda Yüksek Mahkeme önüne giden bir karar olmamıştır. Ancak telgraf içeriklerinin gizliliği de federe devletlerin çıkardığı kanunlarla sağlanmıştır<sup>437</sup>. İlerleyen tarihlerde de telefonun yaygınlaşmasıyla telgraf önemini kaybetmiştir.

#### **b. Telefonun Etkisi**

1870 yılında **Alexander Bell** tarafından icat edilen telefon kısa zaman içerisinde yaygın şekilde kullanılmaya başlanmıştır. Telefon da tıpkı telgraf gibi arayan, aranan ve telefon hatlarını işleten şirket arasında bilgi paylaşımını gerektirmektedir<sup>438</sup>. Erken dönemlerde, arayan kişi telefon şirketinin operatörüne bağlanarak aramak istediği kişinin bilgilerini vermek suretiyle telefon görüşmesi yapabilmektedir. Daha sonraki dönemlerde ise telefon operatörü kaldırılarak süreç otomatikleştirilmiştir. Ancak bu otomatikleştirme, telefon şirketlerinin arayan ve arananlar hakkında bilgi sahibi olmasını engellememiştir.

Telefon dinlemelerine ilişkin ilk Yüksek Mahkeme kararı 1928 yılında verilen **Olmstead v. United States** kararıdır<sup>439</sup>. Karara konu olayda bir suç örgütü lideri olan **Olmstead**'in telefonları polis tarafından mahkeme kararı olmaksızın dinlenmiştir<sup>440</sup>. **Olmstead**'in bu dinlemelerin Dördüncü Değişiklik kapsamında ihlal ettiğine ilişkin iddiaları, Yüksek Mahkeme tarafından Dördüncü Değişikliğin sadece fiziki ortamları

---

<sup>436</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1457-1458.

<sup>437</sup> Richards, **a.g.e.**, s. 1456-1457.

<sup>438</sup> Richards, **a.g.e.**, s. 1458.

<sup>439</sup> *Olmstead v. United States*, C. 277, C. 277 U.S. Reports 438, (U.S. Supreme Court 1928).

<sup>440</sup> Teresa Nesbitt Cosby, "The Expectation of Privacy: An Unreasonable Standard in an Era of Rapid Innovations in Technology", **Charleston Law Review**, C. 12, S. 3, 2017, s. 339.

koruduğu (kişinin kendisi, evi, belgeleri ya da eşyaları) kanaatine varılarak reddedilmiştir<sup>441</sup>. **Olmstead v. United States** kararı içerisinde yer alan muhalefet şerhi ise hukukun gelişen teknolojilere ayak uydurması gerektiğini ifade ederek bir gün devletin yeni teknolojiler sayesinde bireylerin evlerine girmeden dahi onlar hakkında bilgi toplayabileceği ve bunun özel hayatın gizliliği hakkının ihlali olacağını belirtmiştir. Söz konusu muhalefet şerhine göre Dördüncü Değişiklik, teknolojik gelişmelere sürekli olarak uyarlanarak Federal Anayasa'ya eklenme amacına uygun şekilde uygulanmaya devam edilmelidir<sup>442</sup>.

**Olmstead v. United States** kararında, telefon dinlemesi yapılabilmesi için mahkeme kararı alınması zorunluluğunun ABD Kongresi tarafından yerine getirilebileceği ifade edilmiştir. ABD Kongresi de 1934 yılında bu konuda bir federal kanun<sup>443</sup> çıkarmıştır. Ancak çıkarılan bu kanun, iddia makamlarının, mahkeme kararı olmaksızın telefon dinlemesi yapabilme imkânını kayda değer bir şekilde sınırlayamamış ve bunun sonucu olarak da FBI tarafından **Martin Luther King Jr.** gibi siyasi kişilerin telefonlarının dinlenmesi gibi birçok tartışmalı olay meydana gelmiştir<sup>444</sup>.

**Olmstead v. United States** kararından 39 yıl sonra Yüksek Mahkeme, **Katz v. United States** kararı<sup>445</sup> ile görüşünü değiştirerek telefon dinlemesi yapılabilmesi için Dördüncü Değişiklik gereğince mahkeme kararı alınması gerektiği sonucuna ulaşmıştır<sup>446</sup>. Bu kararda Yüksek Mahkeme, gizlilik beklentisinin makul olduğu durumlarda Dördüncü Değişikliğin uygulama alanı bulacağını belirterek telefon konuşmaları sırasında kişilerin gizlilik beklentisinin makul olduğu sonucuna ulaşmıştır<sup>447</sup>.

---

<sup>441</sup> Robinson, “Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act”, s. 1229-1230; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 465.

<sup>442</sup> Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1459-1460.

<sup>443</sup> ABD Kongresi 1934 yılında bu konuda bir federal kanun çıkarmıştır, bilgi için bkz. “Federal Communications Act”, 73-416, (1934), (Çevrimiçi) <https://transition.fcc.gov/Reports/1934new.pdf>, 17.11.2022.

<sup>444</sup> Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1460.

<sup>445</sup> Katz v. United States, 389 U.S. Reports.

<sup>446</sup> Lin, “Where Are Your Papers: The Fourth Amendmnet, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption”, s. 1098; Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1461.

<sup>447</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 466-467.

### c. Veri Aktarım Sistemlerinin Etkisi

Teknolojik gelişmeler neticesinde cep telefonları, GPS sistemleri ve internet gibi çeşitli teknolojiler kişilerin günlük kullanımına sunulmuştur. Teknolojik gelişmeler neticesinde kişilere ilişkin bilgiler dijital ortamda saklanmaya ve paylaşılmaya başlanmıştır. Bu teknolojilerin yaygın bir şekilde kullanımı, söz konusu teknolojiler kapsamında ortaya çıkan verilerin Dördüncü Değişiklik kapsamına girip girmediği konusunda ABD mahkemeleri önüne birçok dava gelmesine sebep olmuştur<sup>448</sup>. Bahse konu davaların büyük kısmı, henüz Yüksek Mahkeme'ye ulaşamamıştır. Daha alt seviyedeki federal ya da federe devlet mahkemelerinde ise birçok konuda değişik kararlar verilmiştir. Bu çalışma için önemli görülen kararlar aşağıda incelenecektir.

Söz konusu kararlardan ilki Federal İstinaf Mahkemesi'nin 6. Dairesi'nin<sup>449</sup> e-postaların içeriklerine erişmek için Dördüncü Değişiklik kapsamında mahkeme kararına ihtiyaç olduğuna dair<sup>450</sup> **United States v. Warshak** kararıdır<sup>451</sup>. Diğer bir önemli karar ise Federal İstinaf Mahkemesi'nin 4. Dairesi'nin<sup>452</sup> vermiş olduğu, cep telefonlarının geçmişteki konumlarını gösteren baz istasyonu kayıtlarının mahkeme kararı olmaksızın polis tarafından alınmasının Dördüncü Değişikliği ihlal etmeyeceğine ilişkin karardır<sup>453</sup>. Ayrıca bulut bilişim sağlayıcılarından veri taleplerine

<sup>448</sup> Cosby, "The Expectation of Privacy", s. 340; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1464.

<sup>449</sup> Özgün adı ile *United States Court of Appeals for the Sixth Circuit* şeklindedir. İnternet sitesi için bkz. <https://www.ca6.uscourts.gov/about-court>.

<sup>450</sup> Andrew B. Serwin, M. Leeann Habte, Jerry D. Brown, "Privacy in an Interconnected World", **GP Solo**, C. 28, 2011, s. 37, (Çevrimiçi) <https://www.foley.com/-/media/files/insights/publications/2011/06/privacy-in-an-interconnected-world/files/privacy-in-an-interconnected-world/fileattachment/privacy1106.pdf>, 09.03.2023; Wei Chen Lin, "Where Are Your Papers: The Fourth Amendmnet, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption Comments", s. 1101; Richard M. Thompson II, Jared P. Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)", **Congressional Research Service**, 2015, s. 5, (Çevrimiçi) <https://sgp.fas.org/crs/misc/R44036.pdf>, 03.8.2023; Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", s. 1233; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1933; Cosby, "The Expectation of Privacy", s. 345.

<sup>451</sup> *United States v. Warshak*, 08-3997, 08-4085, 08-4087, 08-4212, 08-4429, 09-3176, (United States Court of Appeals, Sixth Circuit 14 Aralık 2010).

<sup>452</sup> Özgün adı ile *The United States Court of Appeals for the Fourth Circuit* şeklindedir. Detaylı bilgi için bkz. <https://www.ca4.uscourts.gov/about-the-court>.

<sup>453</sup> *United States v. Graham*, No. 12-4825, No. 12-4659, (United States Courts of Appeals. United States Court of Appeals (4th Circuit) 31 Mayıs 2016).

ilişkin olarak çeşitli mahkeme kararları da bulunmakta olup bunlar sonraki bölümlerde detaylıca incelenecektir.

Veri aktarım sistemlerine ilişkin Yüksek Mahkeme tarafından verilen iki karar bulunmaktadır. Bunlardan ilki **United States v. Jones** kararıdır<sup>454</sup>. Anılan karara konu olayda, polis tarafından şüpheliye ait araca mahkeme kararı olmaksızın GPS cihazı takılarak takip yapılmıştır<sup>455</sup>. Yüksek Mahkeme bu işlemi kişinin özel mülküne girilip bilgi toplanması olarak yorumlamış ve bunun bir arama işlemi olduğunu tespit etmiştir. Bu tespite dayanarak Dördüncü Değişiklik kapsamında söz konusu GPS takibi işleminin yapılabilmesi için mahkeme kararına gerek olduğunu ifade etmiştir<sup>456</sup>.

Diğer bir Yüksek Mahkeme kararı olan **Riley v. California**<sup>457</sup> davasında ise bir mahkeme kararına dayanılarak alıkonan kişinin üzerinden çıkan cep telefonunun hafızasının aranması için Dördüncü Değişiklik kapsamında ayrı bir mahkeme kararına ihtiyaç duyulduğuna hükmedilmiştir<sup>458</sup>. Yüksek Mahkeme, kararının gerekçesinde ayrıca bireylerin cep telefonlarında bulunan verilerin çoğu zaman cihaz hafızasında mı bulut bilişim sistemlerinde mi bulunduğunu dahi bilmediğini ifade ederek bulut bilişim sistemlerinde saklanan verilerin de mahkeme kararı olmaksızın aranamayacağını açıklamıştır<sup>459</sup>.

#### d. Değerlendirmeler

Yukarıda verilen kararlar incelendiğinde posta, telgraf ve telefon konuşmalarının içeriklerinin devlet müdahalesinden korunması konusundaki gelişmelerin aynı

---

<sup>454</sup> United States v. Jones, C. 565, U.S. Reports 400, (U.S. Supreme Court 2012).

<sup>455</sup> Cosby, “The Expectation of Privacy”, s. 341.

<sup>456</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 254-255; Ingram, **Criminal Procedure: Theory and Practice**, s. 351-353.

<sup>457</sup> Riley v. California, 1 U.S. Reports.

<sup>458</sup> Jennifer Daskal, “The Un-Territoriality of Data”, **Yale Law Journal**, C. 125, S. 2, 2015, s. 374; Benton, “Seeking Warrants for Unknown Locations: The Mismatch between Digital Pegs and Territorial Holes”, s. 190; Ingram, **Criminal Procedure: Theory and Practice**, s. 326-330; Lin, “Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption Comments”, s. 1095; Cosby, “The Expectation of Privacy”, s. 342.

<sup>459</sup> Lin, “Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption”, s. 1113-1115; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 218-219.

döngüyü takip ettiği görülecektir. Bu döngüye göre bir teknolojik gelişme, kullanıma alındıktan sonra uyumsuzlukların gündeme gelmesi ile çeşitli davalar Yüksek Mahkeme önüne gelmektedir. Yüksek Mahkeme de önüne gelen konuları nihai olarak Dördüncü Değişiklik kapsamına almakla beraber bu kararlarını verirken toplumdaki beklentilere ve anlayışlara da uygun hareket etmektedir. Ayrıca ABD Kongresi'nin de gerek Yüksek Mahkeme'nin bağlayıcı olmayan görüşleriyle gerekse kendi inisiyatifi ile kanuni düzenlemeler çıkardığı görülmektedir.

İlerideki bölümlerde görüleceği üzere ABD hukukunda yer alan CLOUD Act'in kanunlaşması sürecinde de benzer olgular kendini tekrarlamıştır. Aynı döngü çerçevesinde dijital ortamdaki verilerin de giderek genişleyen kapsamda Dördüncü Değişiklik kapsamına alınacağını beklemek kanaatimizce yanlış olmayacaktır. Nitekim son yıllarda yayınlanan Yüksek Mahkeme kararları da bu eğilimi işaret etmektedir.

Gözlemlenen ikinci bir husus, hukuk kurallarının teknolojik gelişmelerin getirdiği yeni durumlara uyum sağlama süresinin kısalma eğiliminde olduğudur. Nitekim her yeni iletişim sisteminin ortaya çıkmasından sonra, Yüksek Mahkeme'nin konuyla ilgili karar verebilmesi için birkaç on yıl geçmesi gerekmiştir. Ancak günümüzdeki teknolojilerin kullanılma ve yayılma hızı ile nüfusun çok daha fazla olması, geçmişteki gibi Yüksek Mahkeme kararının uzun süre beklenmesine izin vermeyecektir. Nitekim Yüksek Mahkeme'nin GPS ya da cep telefonu hafızaları için verdiği kararlar, ilgili teknolojik gelişmelerin ortaya çıkmasından sadece birkaç yıl sonra verilmiştir.

Son olarak geçmişte verilen kararların, daha sonraki teknolojilere de etki ettiği görülmektedir. Örneğin mektuplar konusunda verilen içerik ile zarf üzerinde yazarların farklı değerlendirilmesi gerektiği şeklindeki karar<sup>460</sup> günümüzde bir e-postanın içeriğinin farklı, e-postaya ilişkin üst verinin (**metadata**)<sup>461</sup> farklı

---

<sup>460</sup> Ex parte Jackson, 96 U.S. Reports.

<sup>461</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1484; Alan Rusbridger, "The Snowden Leaks and the Public", **The New York Review**, 2013, (Çevrimiçi) <https://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/>, 20.01.2021.

değerlendirilmesi gerektiği şeklinde kanuni düzenlemelere ve kararlara sebebiyet verebilmiştir<sup>462</sup>. İşte tam olarak bu nedenle geçmişte ortaya çıkan teknolojiler ile bunların yarattıkları hukuki sorunlara bulunan çözümlerin incelenmesi, gelecekte ortaya çıkabilecek yeni hukuki sorunlara çözüm bulunmasını kolaylaştırabilecek niteliktedir.

## 5. Üçüncü Kişi Doktrini

### a. Üçüncü Kişi Doktrini Hakkında Genel Bilgiler

Dördüncü Değişikliğin kişilere arama ve el koyma işlemlerine karşı sağladığı korumanın temelinde, kişinin gizlilik beklentisinin makul kabul edilebileceği durumlarda özel hayatın gizliliği hakkının korunması gerektiği prensibi yatmaktadır. Üçüncü kişi doktrini (**third party doctrine**) ise bu korumanın sınırlandırılmasına ilişkin iki Yüksek Mahkeme kararından doğmuştur<sup>463</sup>.

Üçüncü kişi doktrini, kişilerin gönüllü olarak üçüncü kişilerle paylaştıkları bilgiler üzerinde gizlilik beklentisinde bulunmalarının makul kabul edilemeyeceğini ve bu nedenle de Dördüncü Değişiklik korumasının paylaşılan bilgiler açısından uygulama alanı bulamayacağını ifade eder<sup>464</sup>. Üçüncü kişi doktrinin sonucu, adli makamların üçüncü kişilerle gönüllü olarak herhangi bir mahkeme kararına ihtiyaç duymadan paylaşılan bilgilere erişim sağlayabilmesidir<sup>465</sup>.

Günümüz teknolojileri göz önüne alındığında, üçüncü kişilerle gönüllü olarak paylaşılan bilgilerin Dördüncü Değişiklik koruması kapsamına çıkarılmasının son derece olumsuz etkileri olacaktır. Zira bulut bilişim sağlayıcıların sunduğu hizmetlerden yararlanılması, aslında üçüncü kişilere gönüllü olarak bilgi açıklanması

---

<sup>462</sup> Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1483-1485.

<sup>463</sup> Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 325.

<sup>464</sup> Adam Gillaspie, “Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law Comments”, **University of Kansas Law Review**, C. 66, S. 2, 2017, s. 465; Lin, “Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption Comments”, s. 1097.

<sup>465</sup> Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 77.

şeklinde gerçekleşmektedir. Örnek vermek gerekirse; cep telefonunda yüklü olan bir sosyal medya uygulamasının, daha iyi arkadaş önerileri verebilmesi için konum takibi yapmasına izin verilmesi halinde; bu sosyal medya uygulamasının sahibi olan şirkete kullanıcının konum bilgileri gönüllü olarak açıklanmış olacaktır. Hal böyle olunca adli makamlar, Dördüncü Değişikliğin gerektirdiği şekilde bir mahkeme kararı almaksızın sınırsız bir şekilde bu konum bilgilerine erişebilecektir. Akıllı elektronik cihazların veri toplamadaki üstün yetenekleri göz önüne alındığında, üçüncü kişi doktrini sebebiyle dijital ortamda kişilerin özel hayatın gizliliği hakkının orantısız şekilde zedelenmesi söz konusu olabilecektir<sup>466</sup>. Zira kişilere Dördüncü Değişiklik ile getirilen makul olmayan arama işlemlerine tabi tutulmama koruması ortadan kalkacaktır. Nitekim henüz Yüksek Mahkeme'nin üçüncü kişi doktrini ve dijital ortama ilişkin herhangi bir kararı olmadığı 1986 yılında ABD Kongresi bu sakıncalı durumu gidermek için harekete geçerek SCA'yı yürürlüğe koymuştur<sup>467</sup>.

Üçüncü kişi doktrini açısından yeni teknolojilerin birçok soru işareti doğurduğu şüphesizdir. Ancak bu soruların yanıtlanabilmesi için öncelikle doktrinin ortaya çıkışı ve kapsamının anlaşılması gerekmektedir. Bu kapsamda aşağıdaki bölümlerde sırasıyla üçüncü kişi doktrinin ortaya çıkışı ve dijital ortamda bulunan bilgilere uygulanması üzerinde durulacaktır.

### **b. Üçüncü Kişi Doktrininin Ortaya Çıkışı**

Üçüncü kişi doktrini, ilk olarak kişiler arasındaki özel konuşmaların gizliliği ve Dördüncü Değişiklik kapsamında bunların elde edilmelerine ilişkin mahkeme kararı gereksinimi olup olmadığına dair tartışmalar ile ortaya çıkmıştır<sup>468</sup>. Daha sonra üçüncü kişi doktrini kayıt sistemlerine sahip olan ve güven duyularak bilgi paylaşılan ticari işletmelere veya araçlara açıklanan bilgileri kapsayacak şekilde genişlemiştir<sup>469</sup>.

---

<sup>466</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1482.

<sup>467</sup> Bkz. Aş. s. 148 vd.

<sup>468</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1467.

<sup>469</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 77; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1468.

### i. Üçüncü Kişi Doktrininin Kişiler Arası Konuşmalara Uygulanması

Üçüncü kişi doktrininin kişiler arası özel konuşmaları kapsayan dönemini oluşturan kararlardan ilki **Hoffa v. United States** kararıdır<sup>470</sup>. Bu karara konu olayda sanık, kaldığı otel odasında kolluk kuvvetlerine muhbirlik yapan bir kişiye, sanığı olduğu diğer bir davada jüri üyelerine rüşvet vermeyi planladığını anlatmıştır. Sanığın iddiası, bu konuşmaya dayanarak tanıklık yapan muhbirin ifadelerinin verilen hükme esas alınmasının kendisinin Dördüncü Değişiklik kapsamındaki anayasal haklarını ihlal ettiği şeklindedir.

Yüksek Mahkeme, gerekçeli kararında öncelikle Dördüncü Değişikliğin sağladığı korumanın ev, işyeri ya da araç içi gibi özel alanlarda etkili olduğunu ve otel odalarının da bu kapsamda değerlendirileceğini ifade etmiştir<sup>471</sup>. Ancak Yüksek Mahkeme muhbirin gizli bir şekilde otel odasına girmediğini, herhangi bir şekilde konuşmaları gizlice dinlemediğini ifade ederek, muhbirin otel odasına sanığın daveti üzerine girdiğini vurgulamıştır. Yüksek Mahkeme'ye böyle bir davet, sanığın muhbirin kendisini ihbar etmeyeceğine dair güven duyduğu anlamına gelmektedir<sup>472</sup>. Dolayısıyla sanık bu konuşmaları yaparken Dördüncü Değişikliğin kendisine sağladığı korumalara değil, muhbire duyduğu güvene dayanmaktadır. Yüksek Mahkeme, Dördüncü Değişikliğin kişilerin kime güveneceklerine dair yaptığı hatalara karşı koruma sağlamayacağını ifade ederek Dördüncü Değişikliğin sağladığı korumaların herhangi bir şekilde ihlal edilmediği sonucuna varmıştır<sup>473</sup>.

Kişiler arasındaki özel konuşmalara dair ikinci karar ise **United States v. White** kararıdır<sup>474</sup>. Bu karara konu olayda üzerinde dinleme cihazı olan muhbire anlattıklarından dolayı mahkûm olan kişinin, söz konusu konuşmaların delil olarak hükme esas alınamayacağı iddiası mevcuttur<sup>475</sup>. Söz konusu iddia, Yüksek Mahkeme tarafından üçüncü kişilere verilen bilgiler için kişinin gizlilik beklentisinin makul

<sup>470</sup> Hoffa v. United States, C. 385, C. 385 U.S. Reports 293, (U.S. Supreme Court 1966).

<sup>471</sup> **a.g.e.**, C. 385, s. 301.

<sup>472</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1468; Hoffa v. United States, 385 U.S. Reports de 302.

<sup>473</sup> Hoffa v. United States, 385 U.S. Reports de 302.

<sup>474</sup> United States v. White, C. 401, C. 401 U.S. Reports 745, (U.S. Supreme Court 1971).

<sup>475</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 219-220.



olmadığı, bireyin yanlış kişilere güvenmesinin sonuçlarından Dördüncü Değişiklik kapsamında korunmasının mümkün olmayacağı gerekçeleriyle reddedilmiştir<sup>476</sup>. Yüksek Mahkeme, dinleme cihazını da muhbirin aktarabileceği bilgileri daha iyi bir şekilde aktarabilecek bir araç olarak nitelemiştir.

## (2) Üçüncü Kişi Doktrininin Büyük Kayıt Sistemlerine Sahip Kişilere Uygulanması

Üçüncü kişi doktrinin kişiler arasındaki özel konuşmalara uygulanmasına kıyasla çok daha önemli olan kısmı, bu doktrinin güven duyulan ticari işletmelerin ve aracılardan sahip olduğu büyük kayıt sistemlerine uygulanmasıdır. Nitekim üçüncü kişi doktrinin bu şekilde büyük kayıt sistemlerine sahip kişilere uygulanacak şekilde genişletilmesi, doktrinin meşruluk açısından tartışmalı bir konuma gelmesine sebep olmuştur<sup>477</sup>. Söz konusu genişleme, üçüncü kişi doktrininin banka ve telefon şirketlerine de uygulanabileceğine dair iki Yüksek Mahkeme kararı vasıtasıyla gerçekleşmiştir<sup>478</sup>.

**United States v. Miller** davasına konu olayda, polis tarafından mahkeme kararı olmaksızın elde edilen çek ve hesap hareketleri gibi finansal kayıtların delil olarak hükme esas alınması neticesinde Miller mahkûm edilmiştir<sup>479</sup>. Yüksek Mahkeme, **Miller**'ın finansal kayıtların elde edilmesi için Dördüncü Değişiklik gereğince mahkeme kararı alınması gerektiği iddiasını iki sebebe dayanarak reddetmiştir. Bunlardan ilki söz konusu finansal kayıtların **Miller**'a ait belgeler olmaması<sup>480</sup>, diğeri ise **Miller**'ın finansal kayıtlar üzerindeki gizlilik beklentisinin makul olmamasıdır<sup>481</sup>. Zira bu finansal kayıtlar hem gizli olarak kabul edilebilecek iletişim niteliğinde değildir hem de esasen ticari faaliyetlerin parçası oldukları için gizli olmaları söz

<sup>476</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 469; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1468.

<sup>477</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1468.

<sup>478</sup> Robert J. Peters, Alicia D. Loy, Matthew Osteen, Joseph Remy, Justin Fitzsimmons, "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", **Mitchell Hamline Law Review**, C. 47, S. 3, 2021, s. 1075; Cosby, "The Expectation of Privacy", s. 344.

<sup>479</sup> *United States v. Miller*, C. 425, C. 425 U.S. Reports 435, (U.S. Supreme Court 1976).

<sup>480</sup> Schwartz, "Legal Access To The Global Cloud", s. 1711; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1469; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 77.

<sup>481</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1469.

konusu değildir<sup>482</sup>. Ayrıca Yüksek Mahkeme üçüncü kişilerle bilgi paylaşımı olması halinde paylaşımda bulunan kişinin makul derecede gizlilik beklentisi olamayacağını ifade ederek bankaya gönderilen bilgiler açısından da bu kuralın geçerli olduğuna hükmetmiştir<sup>483</sup>. Bankaların tüm finansal işlemlere ilişkin kayıtları saklamakla yükümlü olduğunu düzenleyen bir kanunun<sup>484</sup> da kararın verildiği tarihte yürürlükte bulunması, kararın bu şekilde verilmesinde etkili olmuştur<sup>485</sup>. **United States v. Miller** kararının özel hayatın gizliliği hakkı açısından kabul edilemez olduğunu savunan görüşler olduğu gibi kararının esasen son derece limitli bir alanı düzenlediğini ifade eden görüşler de bulunmaktadır<sup>486</sup>.

Üçüncü kişi doktrininin uygulama alanının genişlemesine ilişkin ikinci karar olan **Smith v. Maryland**<sup>487</sup> davasına konu olayda, bir kadının çantasını çalan kişinin; kadını sürekli olarak telefonla araması söz konusudur. Telefon görüşmelerinden birisinde, **Smith** kadına camdan bakmasını söylemiştir. Bunun üzerine camdan bakan kadın, çantasının çalınması sırasında gördüğü aracın evinin önünden geçtiğini fark etmiş ve aracın plakasını polise bildirmiştir. Polis de plaka vasıtasıyla **Smith**'i tespit etmiş ve telefon şirketinin sistemlerine herhangi bir mahkeme kararı olmadan sadece **Smith**'in aradığı numaraları kaydeden bir cihaz yerleştirmiştir. Söz konusu cihaz vasıtasıyla da **Smith**'in mağdur kadını aradığı tespit edilmiş ve **Smith** bu delillere dayanarak ceza almıştır.

Yüksek Mahkeme'ye gelen dosya da **Smith**, kayıt cihazının mahkeme kararı olmadan takılmasının Dördüncü Değişiklik ihlali olduğunu iddia etmektedir. Yüksek Mahkeme, **Smith**'in arama yaptığı telefon numaraları açısından gizlilik beklentisinin

---

<sup>482</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 76; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1469.

<sup>483</sup> Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", s. 1226; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1470.

<sup>484</sup> Özgün adı ile *Federal Bank Secrecy Act* hakkında bilgi için bkz. [www.law.cornell.edu/uscode/text/12/1829b](http://www.law.cornell.edu/uscode/text/12/1829b).

<sup>485</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1469.

<sup>486</sup> Richards, **a.g.e.**, s. 1470. Örnek görüşler için bkz. Cosby, "The Expectation of Privacy", s. 344.

<sup>487</sup> *Smith v. Maryland*, C. 442, C. 442 U.S. Reports 735, (U.S. Supreme Court 1979).

makul olmadığına karar vererek **Smith**'in iddialarını reddetmiştir<sup>488</sup>. Kararın gerekçesinde ise telefon numaralarının aracı niteliğindeki telefon şirketine mutlaka verilmesi gerektiğini (hem iletişimin sağlanması hem de faturalama gibi işlemler için) ve bunun eski dönemde operatörler yeni dönemde ise otomatik sistemlerle gerçekleştirilmesinin herhangi bir fark yaratmadığını belirten Yüksek Mahkeme, üçüncü kişilerle bilgi paylaşımı yapılması halinde paylaşılan bilgiler üzerinde gizlilik beklentisinin makul olmayacağını ifade etmiştir. Yüksek Mahkeme ayrıca yukarıda açıklanan mektup içeriği ile mektup zarfı üzerinde yazan bilgiler üzerinde yaptığı ayrımı<sup>489</sup> koruyarak burada sadece üst veri niteliğindeki aranılan telefon numaralarının takip edildiğini ve aramaların içeriklerinin dinlenmediğini de vurgulamıştır<sup>490</sup>.

### c. Üçüncü Kişi Doktrininin Dijital Ortamda Bulunan Bilgilere Uygulanması

Üçüncü kişi doktrinin getirdiği kurallar, yeni teknolojiler açısından son derece olumsuz sonuçlara yol açabilecek niteliktedir. Zira GPS ya da internet vasıtasıyla çalışan hizmetler veya cep telefonu sinyalleri, esasen üçüncü kişilere gönüllü bir şekilde bilgi aktarımı yapılması anlamına gelmektedir. Eğer bu tür durumlarda üçüncü kişi doktrinine uygulama alanı tanınırsa dijital ortam için kişilerin Dördüncü Değişiklik korumasından yararlanma imkânı büyük oranda ortadan kalkacaktır. Bu endişelerin ele alındığı ve Yüksek Mahkeme'nin üçüncü kişi doktrinin geleceğine dair görüşlerini ifade ettiği iki karar bu bölümde incelenecektir.

**United States v. Jones** kararına<sup>491</sup> konu olayda polis tarafından şüpheliye ait araca mahkeme kararı olmaksızın GPS cihazı takılarak takip yapılmıştır. Yüksek Mahkeme bu işlemi kişinin özel mülküne girilip bilgi toplanması olarak yorumlamış ve bunun

---

<sup>488</sup> Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1075; Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 474; Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1471; Robinson, “Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act”, s. 1226; Schwartz, “Legal Access To The Global Cloud”, s. 1711.

<sup>489</sup> Bkz. Yuk. s. 138.

<sup>490</sup> **Transcript of Oral Argument at 27:02**, Smith v. Maryland, 442 U.S. 735 (1979), 1979, (Çevrimiçi) [https://apps.oyez.org/player/#/burger6/oral\\_argument\\_audio/16917](https://apps.oyez.org/player/#/burger6/oral_argument_audio/16917), 15.11.2022; Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1472.

<sup>491</sup> United States v. Jones, 565 U.S. Reports.

bir arama işlemi olduğunu tespit etmiştir<sup>492</sup>. Her ne kadar bu karar oybirliği ile alınmış olsa da karara üç farklı gerekçe yazılmıştır.

İlk gerekçeye göre mahkeme kararı olmaksızın araca müdahale edilmiş olması, Dördüncü Değişikliğin açıkça ihlalini gösterdiği için herhangi bir ek değerlendirmeye ihtiyaç duyulmamaktadır<sup>493</sup>. İkinci gerekçeye göre ise sadece ilk gerekçenin kabulü, konum takip sistemlerine ilişkin gizlilik konusunda alt dereceli mahkemelere yeterli yönlendirmenin verilmemesi anlamına gelecektir<sup>494</sup>. Olayla ilgili olarak ise GPS vasıtasıyla kişinin uzun süreli olarak takip edilmesinin, Dördüncü Değişiklik koruması kapsamı dışına çıkarılmasının mümkün olmayacağı sonucuna varılmıştır. Bu sonucun gerekçesi, kişinin uzun bir zaman boyunca sürekli olarak takip edilmesinin mümkün olamayacağına dair düşüncesinin, makul gizlilik beklentisi oluşturmastır. Ayrıca ikinci gerekçe içerisinde teknolojik gelişimlerin hızı karşısında konunun Yüksek Mahkemece değil, ABD Kongresi tarafından kanun çıkarılması yoluyla düzenlenmesinin daha uygun olabileceği de ifade edilmiştir. Son gerekçede ise GPS takibinin konum yanında kişinin aile yapısı, dini inançları, mesleği veya cinsel yönelimleri gibi birçok konuda da bilgi toplanmasına imkân vereceği ifade edilmiştir. Bu düzeyde bilgi toplama imkânının kontrolsüz şekilde devlete tanınması halinde demokratik toplum yapısının bozulacağı endişesi dile getirilmiştir<sup>495</sup>. Üçüncü gerekçe içerisinde ayrıca kişilerin kendileri ile ilgili çoğu bilgiyi paylaştığı dijital dünyaya uyumlu olmayan üçüncü kişi doktrininin de yenilenmesi gerektiği ifade edilmiştir<sup>496</sup>.

Diğer bir Yüksek Mahkeme kararı olan **Carpenter v. United States** kararına<sup>497</sup> konu olayda FBI, **Carpenter**'ın aleyhine delil elde etmek için baz istasyonlarından toplanan cep telefonu konum bilgilerini (**cell-site location information**) Dördüncü Değişiklik kapsamında bir mahkeme kararı yerine federal kanunlar çerçevesinde aldığı bir hâkim

---

<sup>492</sup> Carmen, Hemmens, **Criminal Procedure Law and Practice**, s. 477; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1475.

<sup>493</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1475-1476.

<sup>494</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 350-354; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1476.

<sup>495</sup> Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1477.

<sup>496</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 350-354; Richards, "The Third Party Doctrine and the Future of the Cloud", s. 1477-1478.

<sup>497</sup> *Carpenter v. United States*, C. 585, C. 585 U.S. Reports, (ABD Yüksek Mahkemesi 2018).

emrine (**subpoena**)<sup>498</sup> istinaden toplamıştır<sup>499</sup>. Hâkim emrinin alınması ise Dördüncü Değişiklik kapsamında alınacak bir mahkeme kararına kıyasla çok daha basit koşullara tabidir. **Carpenter**, ilgili konum bilgileri üzerindeki gizlilik beklentisinin makul olduğunu ve bu nedenle söz konusu işlemin Dördüncü Değişiklik kapsamında mahkeme kararı olmaksızın yapılamayacağını; dolayısıyla da toplanan delillerin hükme esas alınamayacağını iddia etmiştir.

Yüksek Mahkeme, **Carpenter**'ın iddiaları hakkında yaptığı değerlendirmede öncelikle Dördüncü Değişikliğin kişilerin makul gizlilik beklentisini de koruduğunu belirterek FBI tarafından yapılan işlemin Dördüncü Değişiklik kapsamında bir arama işlemi olduğunu tespit etmiştir. Daha sonra Yüksek Mahkeme, üçüncü kişiler ile yapılan bilgi paylaşımları açısından iki türlü içtihat grubu olduğunu ifade etmiştir. İlk grupta kişilerin fiziki konum ve hareketleri üzerindeki makul gizlilik beklentisini değerlendiren **United States v. Jones** kararı bulunmaktadır<sup>500</sup>. İkinci grupta ise kişinin bilgilerini gönüllü olarak üçüncü kişilerle paylaştığı **United States v. Miller**<sup>501</sup> ve **Smith v. Maryland**<sup>502</sup> kararları bulunmaktadır.

Yüksek Mahkeme tarafından **Carpenter**'ın iddiası, konum bilgileri üzerindeki makul gizlilik beklentisinin getirdiği koruma ile kişinin gönüllü olarak üçüncü kişilerle bilgi paylaşmasının bu korumaya getirdiği kısıtlamaların (yani üçüncü kişi doktrinin uygulanmasının) çatışması olarak görülmüştür. Yüksek Mahkeme yaptığı değerlendirme neticesinde cep telefonu konum bilgilerinin kişi hakkında geçmişe dönük ve çok detaylı konum bilgileri ile bunlara bağlı olarak kişinin yaşam tarzına ilişkin bilgileri tespit etmeye elverişli olacağı sonucuna vararak, söz konusu bilgilerin **United States v. Miller** ve **Smith v. Maryland** kararlarına konu olan kısıtlı bilgi

---

<sup>498</sup> Subpeonalara ilişkin detaylı bilgi için bkz. Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act", **Journal of National Security Law and Policy**, C. Forthcoming 2020, 2019, s. 13-14, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3469808](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469808), 16.03.2021.

<sup>499</sup> Schwartz, "Legal Access To The Global Cloud", s. 1711; Ingram, **Criminal Procedure: Theory and Practice**, s. 322-323; Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act", s. 325.

<sup>500</sup> Bkz. Yuk. s. 136.

<sup>501</sup> Bkz. Yuk. s. 142.

<sup>502</sup> Bkz. Yuk. s. 142 vd.

setine göre çok daha farklı olduğunu ifade etmiştir<sup>503</sup>. Yüksek Mahkeme ayrıca cep telefonlarının çalışma prensipleri gereği anlık olarak konum bilgilerini baz istasyonlarına aktarmalarının, söz konusu içtihatlar kapsamında gönüllü bir bilgi paylaşımı olarak kabul edilemeyeceği sonucuna varmıştır<sup>504</sup>. Bu iki tespit kapsamında Yüksek Mahkeme, üçüncü kişi doktrini cep telefonu konum bilgilerine uygulanacak şekilde genişletmeyi reddetmiştir<sup>505</sup>. Zira böyle bir genişleme, devletin kontrolsüz ve orantısız bir şekilde vatandaşlar hakkında geniş kapsamlı bilgilere erişmesine sebebiyet verecektir. Son olarak Yüksek Mahkeme, teknolojik gelişmelerin sonuçlarından çekinerek bu kararın sadece huzurdaki olay ile sınırlı olduğunu, daha önceki içtihatların uygulanmasını ortadan kaldırmayacağını da ifade etmiştir. Yüksek Mahkeme, daha önceki içtihatlarına konu olan acil durumlarda Dördüncü Değişiklik kapsamında mahkeme kararı olmaksızın arama işlemi yapılabilmesi imkanının da hala mevcut olduğunu belirtmiştir<sup>506</sup>.

#### d. Üçüncü Kişi Doktrini Üzerine Değerlendirmeler

Üçüncü kişi doktrini, ortaya çıkışı itibarıyla Dördüncü Değişiklik korumalarının bir istisnası olarak değerlendirilebilmektedir. Üçüncü kişi doktrinin temeli, bir kişinin gizlilik beklentisinden; üçüncü kişilere yaptığı ifşalar yoluyla gönüllü olarak vazgeçmesine dayanmaktadır. Ancak üçüncü kişi doktrininin dijital dünyaya uyumlu olmadığı ve bunun uygulanması halinde Dördüncü Değişiklik korumasının fiilen ortadan kalkacağı görüşü doktrinde de ifade edilmiştir<sup>507</sup>. Zira dijital dünyanın yapısı, bireylerin kendileri hakkındaki bilgileri üçüncü kişilere yani genellikle bulut bilişim hizmet sağlayıcılarına gönüllü olarak ifşa etmeleri üzerine kurulmuş durumdadır. Dolayısıyla üçüncü kişi doktrini geçmişteki gibi aynen günümüze uygulamak,

<sup>503</sup> Daskal, “The Un-Territoriality of Data”, s. 377-378; Cosby, “The Expectation of Privacy”, s. 344; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1075.

<sup>504</sup> Carpenter v. United States, 585 U.S. Reports de 3; Ingram, **Criminal Procedure: Theory and Practice**, s. 322-323.

<sup>505</sup> Sabrina McCubbin, “Summary: The Supreme Court Rules in Carpenter v. United States”, **Lawfare**, 22.06.2018, (Çevrimiçi) <https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states>, 25.06.2020.

<sup>506</sup> Ingram, **Criminal Procedure: Theory and Practice**, s. 322-323; McCubbin, “Summary: The Supreme Court Rules in Carpenter v. United States”.

<sup>507</sup> Richards, “The Third Party Doctrine and the Future of the Cloud”, s. 1482.

bireylerin dijital ortamdaki mahremiyetlerinin ortadan kalkmasına sebebiyet verebilecektir.

Günümüzde dijital ortamın hayatın her alanını etkilediği düşünüldüğünde, üçüncü kişi doktrinin yeni teknolojilere uyarlanmamasının, bireylerin özel hayatlarının gizliliği hakkının ortadan kalkmasına sebebiyet vereceği açıktır. Nitekim **Carpenter v. United States** kararı ve daha önceki kararlar birlikte değerlendirildiğinde, kanaatimizce Yüksek Mahkemenin üçüncü kişi doktrininin dijital ortamdaki verilere uygulanmaması yönünde bir yaklaşıma sahip olduğunu söylemek mümkündür. Ancak Yüksek Mahkeme kararları, henüz açıkça bulut sistemlerindeki verilere erişim ya da e-postalara erişim gibi konuları ele almış değildir. Aşağıda incelenecek olan federal kanunlar ile bu konuların da çözüme kavuşturulmaya çalışıldığı görülmektedir.

Son olarak ifade etmek gerekir ki üçüncü kişi doktrini ve Dördüncü Değişiklik uygulamalarının en önemli sonuçlardan birisi de bulut bilişim sağlayıcıların bireylerin temel hak ve özgürlüklerini savunma konusunda önemli bir rol üstlenmelerini sağlamasıdır. Aşağıda da görülebileceği üzere **Microsoft** ve **Google** gibi bulut bilişim sağlayıcıların açmış olduğu davalar, bu konudaki hukuki düzenlemelerin şekillenmesinde önemli bir rol oynamıştır.

## **C. SCA Kapsamında Bilgi Talepleri**

### **1. SCA Hakkında Genel Bilgiler**

21 Ekim 1986 tarihinde yürürlüğe giren SCA, dijital ortamda gerçekleşen ve internet hizmet sağlayıcıları tarafından saklanan iletişim içerikleri ile iletişimin taraflarına ilişkin işlem kayıtlarına üçüncü kişilerin erişim taleplerini düzenlemektedir. 23 Mart 2018 tarihinden önce SCA kapsamında ABD mahkemelerinin verdiği iletişim içeriğinin kolluk kuvvetlerine verilmesine yönelik kararların, ABD sınırları dışında bulunan fakat ABD şirketleri kontrolü altında bulunan verileri kapsayıp kapsamayacağına dair görülen davalar, SCA'nın tadil edilmesi ihtiyacını

doğurmuştur<sup>508</sup>. Bu ihtiyacın neticesinde de SCA'yı tadil eden CLOUD Act<sup>509</sup> 23 Mart 2018 tarihinde yürürlüğe girmiştir<sup>510</sup>.

Kronolojik bütünlüğü sağlamak adına öncelikle SCA'nın yürürlüğe konmasına ilişkin sebepler ile kapsam ve amacına ilişkin bilgiler paylaşılacaktır. Akabinde ise SCA'nın tadil edilmesine neden olan mahkeme kararları incelenerek CLOUD Act'in hazırlanmasına sebep olan tartışmalar üzerinde durulacaktır. Son kısımda ise CLOUD Act ile tadil edilmiş olan güncel SCA'nın getirdiği kurallar irdelenecektir.

## 2. SCA'nın Yürürlüğe Konmasının Sebepleri

SCA gibi bir kanuni düzenlemeye ihtiyaç duyulmasının altında yatan temel neden Dördüncü Değişikliğin, internetin ortaya çıkışı ile doğan özel hayatın gizliliğinin sağlanmasına yönelik yeni ihtiyaçları karşılamada yetersiz kalacağına yönelik endişeler olarak ifade edilmektedir<sup>511</sup>. İnternetin çalışma yapısı çok basit olarak kişilerin bilgilerini başka kişilere ait bilgisayarlara aktarmaları şeklindedir. Örneğin

<sup>508</sup> Chris Cook, "Cross-Border Data Access and Active CyberDefense: Assessing Legislative Options for a New International Cybersecurity Rulebook", *Stanford Law & Policy Review*, C. 29, S. 2, 2018, s. 222-223.

<sup>509</sup> Bkz. "Clarifying Lawful Overseas Use of Data Act", H.R. 4943, (2018).

<sup>510</sup> Detaylı bilgi için bkz. Jonathan I. Blackman, Jared Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", *Clearly Gottlieb*, 2018, (Çevrimiçi) <https://www.clearlygottlieb.com/-/media/files/alert-memos-2018/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications.pdf>, 18.08.2019, s. 1-6; Stephen P. Mulligan, "Cross-Border Data Sharing Under the CLOUD Act", *Congressional Research Service*, No: 7-5700, 2018, s. 21-22, (Çevrimiçi) <http://www.crossborderdataforum.org/wp-content/uploads/2018/07/CRS-Cross-Border-Data-Sharing-Under-the-CLOUD-Act.pdf>, 05.07.2019; Mark D. Cole, Quintel Teresa, "Transborder Access to e-Evidence by Law Enforcement Agencies", University of Luxembourg Law Working Paper No. 2018-010, 2018, s. 10-11, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3278780](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278780), 05.07.2019; Jean-Baptiste Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", *Springer*, 2018, s. 386, (Çevrimiçi) <https://link.springer.com/content/pdf/10.1007%2Fs12027-018-0527-2.pdf>, 05.07.2019; Els De Busser, "The Digital Unfitness of Mutual Legal Assistance", *Security and Human Rights*, C. 28, S. 1-4, 2017, s. 177; Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?", SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 27.05.2019, s. 1, (Çevrimiçi) <https://papers.ssrn.com/abstract=3397047>, 27.09.2020; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1937-1938.

<sup>511</sup> Önemle belirtmek gerekir ki bu değerlendirme, SCA'nın yürürlüğe konduğu 1986 yılından önceki mahkeme içtihatları dikkate alınarak yapılmıştır. Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 77-78; Blackman, Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", s. 2; Lin, "Where Are Your Papers: The Fourth Amendmnet, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption", s. 1097; Graber, "Where in the World Is Your Data: Who Can Access It?", s. 161-162.



**Facebook**'a yüklenen bir fotoğraf aslında kullanıcı olan gerçek kişinin bilgisayarından, bahse konu internet sitesini işleten tüzel kişinin bilgisayarına aktarılmaktadır. Burada açıklanan çok daha büyük ve karmaşık boyutlu iletişimlere içeren internet üzerinde kişilerin özel hayatlarının gizliliğinin Dördüncü Değişiklik kapsamında korunamayacağı düşüncesini doğuran temel olarak üç sebep bulunmaktadır.

İlk sebep, Dördüncü Değişiklik kapsamında Yüksek Mahkeme tarafından geliştirilen ve yukarıda detayları ile açıklanan üçüncü kişi doktrini'dir. Kısaca tekrar etmek gerekirse, üçüncü kişi doktrini; bir kişinin üçüncü kişilerle paylaştığı bilgiler üzerinde makul gizlilik beklentisi olmadığını ve bu nedenle de söz konusu bilgilerin Dördüncü Değişiklik kapsamında korunmayacağını kabul etmektedir<sup>512</sup>. Her ne kadar 2018 yılında Yüksek Mahkeme tarafından verilen **Carpenter v. United States** kararı ile önemli bir aşama kaydedilmiş olsa da bugün dahi üçüncü kişi doktrininin dijital ortamda uygulanmasına ilişkin önemli soru işaretleri bulunmaktadır<sup>513</sup>. SCA'nın yürürlüğe konduğu 1986 yılında ise konunun çok daha belirsiz olduğu açıktır. Nitekim o yıllarda mevcut olan üçüncü kişi doktrininin dijital ortamda uygulanması halinde özel hayatın gizliliği hakkının ciddi şekilde zedeleneyecek olmasına yönelik endişeler, SCA'nın yürürlüğe konmasını konusunda etkili olmuştur.

İkinci sebep, iddia makamlarının emir gönderme vasıtasıyla üçüncü kişilerden bilgi ya da delil talep etmesinin, Dördüncü Değişiklik açısından herhangi bir hukuka aykırılık teşkil etmemesidir. Zira Dördüncü Değişikliğin gerektirdiği mahkeme kararı alınması şartı, sadece arama ya da el koyma işlemine doğrudan konu olan kişiler için geçerlidir. Oysaki bulut bilişim sağlayıcılarının bilgi sistemlerine adli makamlarca doğrudan erişilmesi (örneğin veri merkezine polis baskını yapılarak cihazlara el konması ya da olay yerinde cihazlar içerisinden bilgi alınması gibi) söz konusu olmamaktadır. Dolayısıyla Dördüncü Değişikliğin gerektirdiği şekilde bir mahkeme kararı alınmasına da ihtiyaç bulunmamaktadır. Bunun yerine adli makamlar bulut bilişim sağlayıcılarına

---

<sup>512</sup> Bkz. Yuk. s. 138 vd. Bilgi için bkz. Hemmings, Srinivasan, Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act", s. 13-14.

<sup>513</sup> Bkz. Yuk. s.145 vd.

emir göndererek sağlayıcıları ellerindeki bilgileri vermeye hukuken mecbur bırakmaktadırlar. İddia makamlarının bu şekilde emir gönderme imkânına sahip olması, Dördüncü Değişikliğin etrafından dolaşılmasını sağlamaktadır. SCA ile bu sorun da çözümlenmeye çalışılmıştır.

Üçüncü sebep ise bulut bilişim sağlayıcıların esasen özel hukuk kişileri olmaları nedeniyle ellerindeki bilgileri, hukuki sınırlar çerçevesinde diledikleri gibi kullanma ve paylaşma imkânına sahip olmalarıdır. Dolayısıyla her ne kadar adli makamlardan hukuka uygun bir talep olmasa dahi bulut bilişim sağlayıcıların gönüllü olarak bilgi paylaşımları önünde herhangi bir engel bulunmamaktadır. Söz konusu durumun sakıncalarını gidermek de SCA ile ulaşılmak istenilen amaçlardan birisidir.

### 3. SCA'yı Tadil Eden CLOUD Act'in Doğuşuna Sebep Olan Mahkeme Kararları

SCA'nın CLOUD Act vasıtasıyla tadil edilmesine giden süreç, iddia makamlarınca kendilerine iletilen bilgi taleplerine karşı **Microsoft** ve **Google**'ın mahkemelerde itiraz etmeleriyle başlamıştır. Mahkemeler, **Microsoft**'un taraf olduğu davalar ile **Google**'ın taraf olduğu davalar hakkında farklı kararlar vermişlerdir<sup>514</sup>. Söz konusu farklılıklar özellikle ABD mahkemelerinin verdiği arama ve el koymaya ilişkin kararların ABD sınırları dışında uygulanıp uygulanamayacağı noktasındadır. **Microsoft**'un taraf olduğu bir dava neticesinde verilen kararı Yüksek Mahkeme'ye taşındığı sırada, ABD Kongresi tarafından CLOUD Act çıkarılmıştır<sup>515</sup>. Yüksek Mahkeme de uyuşmazlığın

<sup>514</sup> Toy, Gunasekara, "Is There a Better Option than the Data Transfer Model to Protect Data Privacy", s. 738; Cole, Quintel Teresa, "Transborder Access to e-Evidence by Law Enforcement Agencies", s. 10; Schwartz, "Legal Access To The Global Cloud", s. 1691-1694.

<sup>515</sup> Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0", **Stanford Law Review**, C. 71, 2018, s. 9; Eleni Kyriakides, "The CLOUD Act, E-Evidence, and Individual Rights", **European Data Protection Law Review (EDPL)**, C. 5, S. 1, 2019, s. 99; Kayahan Cantekin, "Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?", **1st Edition of the Seminars of the PhD School in Public, International and European Union law of "Università degli Studi di Milano"**, 2018, s. 80; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 85; De Hert, Thumfart, "The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies", s. 3; Hemmings, Srinivasan, Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act", s. 21; Benton, "Seeking Warrants for Unknown Locations: The Mismatch between Digital Pegs and Territorial Holes", s. 191; Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", s. 386-387; Jennifer Daskal, "Privacy and Security Across Borders", **Yale Law Journal Forum**, 2019, s. 1030.

CLOUD Act'in yürürlüğe girmiş olması dolayısıyla kanun değişikliği ile çözüldüğünü öne sürerek herhangi bir karar verilmesine yer olmadığına hükmetmiştir<sup>516</sup>.

Mahkeme kararları arasında farklılıklar bulunmasının en büyük sebeplerinden birisi de ilgili kararlara konu, **Microsoft** ve **Google** tarafından işletilmekte olan bulut sistemlerinin farklı modeller kullanmasıdır. Yukarıda açıklandığı üzere<sup>517</sup> **Microsoft**, lokal bulut bilişim sistemi modelini kullanmaktadır. Yani **Microsoft** tarafından veriler bir bütün olarak, tek bir ülkede ya da bölgede bulunan veri merkezinde saklanmaktadır. Dolayısıyla bu ülke mahkemelerinin vereceği bir karar ya da söz konusu ülkeye yapılacak bir adli istinabe talebi, talebe konu bilgilerin alınması için yeterli olacaktır. Öte yandan **Google**, dağıtık bulut bilişim sistemi modelini kullanmaktadır. Söz konusu model içerisinde veriler parçalanarak değişik veri merkezlerinde saklanmakta ve bu parçaların yerleri de sürekli olarak değiştirilmektedir. Saklama modeli nedeniyle verilere erişmek için adli süreçlerin kullanılması imkânsız hale gelmektedir. Çünkü adli istinabe talebinin hangi ülkeye yapılacağı belirsiz olduğu gibi veri konumunun sürekli değişiyor olması da talepte bulunulmasını anlamsızlaştırmaktadır.

Kullanılan bulut bilişim sistemi modellerindeki farklılık, iddia makamlarının bilgi taleplerine ilişkin yargılamaların da farklı sonuçlanmasına sebep olmuştur. **Microsoft**'a ilişkin yargılama süreci sonucunda, SCA kapsamında verilen mahkeme kararlarının sadece ABD sınırları içerisinde hüküm ifade edeceği kararlaştırılmıştır. **Google**'a ilişkin yargılama süreci sonucunda ise SCA kapsamında verilen mahkeme kararlarının ABD sınırları dışında da hüküm doğuracağı sonucuna varılmıştır. Her iki karar da aşağıdaki başlıklar altında detaylıca incelenecektir.

---

<sup>516</sup> Microsoft Corp v. United States; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 85; Paul De Hert, Cihan Parlar, Johannes Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland", **New Journal of European Criminal Law**, C. 9, S. 3, 2018, s. 347-348.

<sup>517</sup> Bkz. Yuk. s.115 vd.

#### a. Microsoft Corp v. United States Kararı

ABD Federal 2. Bölge İstinaf Mahkemesi<sup>518</sup> tarafından görülen **Microsoft Corp v. United States**<sup>519</sup> davasına konu olay, 4 Aralık 2013 tarihinde, adli makamların talebi üzerine yetkili yerel mahkemece **Microsoft**'un elindeki bazı bilgileri<sup>520</sup> teslim etmesini gerektiren bir mahkeme emri verilmesi ile başlamıştır<sup>521</sup>. Söz konusu karara göre **Microsoft**, kendi e-posta hizmetlerini barındıran veri merkezlerini araştırarak sahip olduğu bilgilerden mahkeme emrine konu olanları teslim etmelidir. **Microsoft** tarafından ilgili karara uyulması için yapılan çalışmalar neticesinde e-posta içeriklerinin İrlanda'da bulunan veri merkezinde saklandığı<sup>522</sup>; ancak diğer bilgilerin ABD içerisinde bulunan veri merkezlerinde de bulunduğu tespit edilmiştir. Bunun üzere **Microsoft**, ABD'de bulunan verileri teslim etmiş ve İrlanda'da bulunan e-posta

<sup>518</sup> Özgün adı ile *United States Court of Appeals for the Second Circuit* şeklindedir. İnternet sitesi için bkz. (Çevrimiçi) <http://www.ca2.uscourts.gov>, 04 Ocak 2020.

<sup>519</sup> *Microsoft Corp v. United States*, 14-2985, (United States Court of Appeals for the Second Circuit 14 Temmuz 2016).

<sup>520</sup> Başvuru kapsamında talep edilen bilgiler şunlardır: (i) Gönderilen e-postalar da dahil olmak üzere talebe konu e-posta hesabında saklanmakta olan tüm e-postaların içerikleri; (ii) E-posta hesabının belirlenmesine ilişkin her türlü bilgi (özellikle isim, fiziki adres, telefon numaraları, oturum açma kapama tarihleri ile süreleri, giriş yapılan IP adresleri ve hesaba ilişkin yapılan ödemelerde kullanılan ödeme araçları); (iii) Hesabı kullanan kişi tarafından hesapta saklanmakta olan her türlü kayıt ve diğer bilgiler (özellikle kaydedilen kişi bilgileri, yakın arkadaş listesi, resimler ve diğer dosyalar); (iv) Talebe konu e-posta adresi ile hesabın yönetimi ve bakımı hakkında, ilgili kişilerle gerçekleşen tüm iletişimler ile önerilen çözüm yöntemleri.

<sup>521</sup> Omer Tene, "Microsoft v. USA: Location of Data and the Law of the Horse", **IEEE Security Privacy**, C. 14, S. 6, 2016, s. 81; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 80-81; Richard Kemp, "Cloud Computing and Data Sovereignty", 2016, s. 10, (Çevrimiçi) <https://kempitlaw.com/insights/cloud-computing-and-data-sovereignty/>, 12.06.2019; Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act", s. 1; Paul De Hert, Johannes Thumfart, "The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies", **Brussels Privacy Hub, Working Paper**, C. 4, S. 11, 2018, s. 3, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3228388](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228388), 15.12.2020; Jacqueline De Souza Abreu, "Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience", **Revista de Informação Legislativa: RIL**, C. 55, S. 220, 2018, s. 235; Graber, "Where in the World Is Your Data: Who Can Access It?", s. 163; Andrew J. Pecoraro, "Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act", **Creighton Law Review**, C. 51, S. 1, 2017, s. 87; Busser, "The Digital Unfitness of Mutual Legal Assistance", s. 176-177; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1940-1941; De Hert, Parlar, Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders", s. 345-348.

<sup>522</sup> Eric Clemons, "The Federal Government's Attempt to Force Microsoft to Violate Irish Territoriality", 2017, s. 4997, (Çevrimiçi), <http://scholarspace.manoa.hawaii.edu/handle/10125/41768>, 12.06.2019.

içerikleri hakkında yetkili yerel mahkemeye itirazda bulunmuştur<sup>523</sup>. Söz konusu itiraz, SCA kapsamında alınan mahkeme kararlarının sınır ötesi uygulama kapsamı ya da bir başka deyişle ABD toprakları dışında etkisi olmadığı iddiasına dayanmaktadır<sup>524</sup>.

İtirazı görmekte olan yerel mahkeme, **Microsoft**'un davasını reddetmiştir. Söz konusu karara göre SCA kapsamında verilen bilgi taleplerine ilişkin mahkeme emirleri; fiziki bir ortama dair verilen arama ve el koymaya ilişkin mahkeme kararları gibi kolluk kuvvetlerinin bir mekâna girerek araştırma yapmasını ya da çeşitli eşyalara el koymasını gerektirmemektedir<sup>525</sup>. Bunun yerine SCA kapsamındaki söz konusu mahkeme emirleri; mahkeme, jüri ya da idari makam emirleri gibi muhatabının elindeki, gözetimindeki veya kontrolündeki ilgili bilgileri teslim etmesi şeklinde uygulanmaktadır<sup>526</sup>. Açıklanan farklılığı göz önüne alan yerel mahkeme, SCA kapsamında verilen bilgi taleplerine ilişkin mahkeme emirlerinin; bilgi taleplerine ilişkin mahkeme, jüri ya da idari makam emirleri ile fiziki ortamda arama ve el koymaya ilişkin mahkeme kararlarının karışımı olarak anlaşılması gerektiği sonucuna varmıştır<sup>527</sup>.

---

<sup>523</sup> Microsoft Corp v. United States de 5; Eichensehr, "Data Extraterritoriality", s. 149; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 81; Schwartz, "Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies", s. 1; De Souza Abreu, "Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience", s. 235; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1092-1093; Cole, Quintel Teresa, "Transborder Access to e-Evidence by Law Enforcement Agencies", s. 9-10.

<sup>524</sup> Kemp, "Cloud Computing and Data Sovereignty", s. 10; Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 2; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 425; Graber, "Where in the World Is Your Data: Who Can Access It?", s. 163; Thompson II, Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)", s. 14; Pecoraro, "Drawing Lines in the Cloud", s. 87-88.

<sup>525</sup> De Souza Abreu, "Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience", s. 235; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 81.

<sup>526</sup> Mahkeme, jüri ya da idari makam emirlerine uygun hareket edilmesi hukuki bir zorunluluktur. Bu zorunluluğa aykırı hareketler, muhatabın çeşitli yaptırımlara tabi tutulmasını gerektirmektedir. Ayrıca bkz. Kemp, "Cloud Computing and Data Sovereignty", s. 25-26.

<sup>527</sup> Ned Schultheis, "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry", **Brooklyn Journal of Corporate, Financial & Commercial Law**, C. 9, S. 2, 2015, s. 669-670; Kemp, "Cloud Computing and Data Sovereignty", s. 10; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1942.

Yerel mahkeme, bilgi taleplerine ilişkin emirlerin uygulanmasına paralel olarak, dava konusu olayda da **Microsoft**'un kendi veri merkezlerini araştırarak talebe konu bilgileri toplaması ve teslim etmesi gerektiğine hükmetmiştir. Yerel mahkemeye göre ilgili bilgilerin bulunduğu konum herhangi bir önem arz etmemektedir<sup>528</sup>. Ayrıca iddia makamlarının (yani kolluk kuvvetlerinin) ilgili bilgilere erişmek için ABD dışında herhangi bir faaliyeti bulunmaması nedeniyle davaya konu mahkeme kararının, ABD sınırları dışında egemenlik gücü kullanılarak uygulanması söz konusu değildir. Talebe konu bilgilerin incelenmesi de ABD topraklarında gerçekleşeceği için, itiraza konu mahkeme emrinin etkisinin, ABD sınırları dışına çıkması sonucuna da ulaşamayacaktır.

**Microsoft**, yapılan ilk itirazı gören yerel mahkemenin kararına da itiraz etmiştir. İtiraz süreçleri neticesinde dosya 2. Bölge İstinaf Mahkemesi önüne kadar gelmiştir. Söz konusu süreç boyunca itirazların ve yerel mahkeme kararlarının dayandıkları sebeplerde önemli bir farklılaşma meydana gelmemiştir.

2. Bölge İstinaf Mahkemesi tarafından yapılan değerlendirmede öncelikle kanunların sınır ötesi uygulama kapsamı olup olmadığına ilişkin kurallar incelenmiştir. Yüksek Mahkeme'nin **Morrison v. National Australia Bank**<sup>529</sup> kararında da belirtildiği üzere kural olarak ABD Kongresi tarafından çıkarılan her kanun sadece ABD toprakları içerisinde uygulanabilmektedir<sup>530</sup>. Bu kurala iki istisna bulunmaktadır. İlki ilgili kanun metninde sınır ötesi uygulama kapsamından açıkça bahsedilmesidir. İkincisi ise ilgili

---

<sup>528</sup> Daskal, "The Un-Territoriality of Data", s. 378; Eichensehr, "Data Extraterritoriality", s. 149-150; Pecoraro, "Drawing Lines in the Cloud", s. 88.

<sup>529</sup> Morrison v. National Australia Bank Ltd. ( No. 08-1191 ), (U.S. Supreme Court 24 Haziran 2010).

<sup>530</sup> Alexander Dugas Jr. Battey, "A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act Notes & Comments", **Rutgers Computer and Technology Law Journal**, C. 42, S. 2, 2016, s. 279; Dan Svantesson, Felicity Gerry, "Access to extraterritorial evidence: The Microsoft cloud case and beyond", **Computer Law & Security Review**, C. 31, S. 4, 2015, s. 481; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 82; Toy, Gunasekara, "Is There a Better Option than the Data Transfer Model to Protect Data Privacy", s. 734; Clemons, "The Federal Government's Attempt to Force Microsoft to Violate Irish Territoriality", s. 4999; Daskal, "The Un-Territoriality of Data", s. 334-335; Graber, "Where in the World Is Your Data: Who Can Access It?", s. 164; Pecoraro, "Drawing Lines in the Cloud", s. 85-86; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1940; Schultheis, "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry", s. 674-675.

kanunun odak noktasının ve amacının, kanunun sınır ötesi uygulama kapsamına sahip olmasına elverişli olmasıdır. Söz konusu iki durumdan en az birinin varlığı halinde ilgili kanunun sınır ötesi uygulama kapsamına sahip olduğu kabul edilmektedir.

Kanunların sınır ötesi uygulanmasına ilişkin kuralları önündeki somut olaya uygulayan İstinaf Mahkemesi, ilk olarak SCA metninde sınır ötesi uygulama kapsamına ilişkin herhangi bir ifade bulunmadığını tespit etmiştir. Bunun üzerine İstinaf Mahkemesi SCA'nın odak noktasını ve amacını incelemiştir. İstinaf mahkemesine göre 1986 yılında çıkarılan SCA'nın amacının gelişen teknolojiler karşısında özel hayatın gizliliği hakkının korunmasını sağlamaktır. Özel hayatın gizliliği hakkı sınır ötesi uygulama kapsamı gerektirmediği için, SCA kapsamında alınan arama ve el koymaya ilişkin mahkeme kararlarının ABD toprakları dışında uygulanmasının mümkün olmayacağı sonucuna ulaşılmıştır<sup>531</sup>.

İstinaf Mahkemesi ayrıca kendisinden önce davaya bakan mahkemelerin gerekçelerine dair de değerlendirmeler yapmıştır. Bu kapsamda değerlendirilen konulardan birisi, yurtdışında bulunan verilerin; SCA kapsamında alınan arama ve el koymaya ilişkin mahkeme kararları kapsamında teslim edilmesi halinde ABD toprakları dışında egemenlik gücünün kullanılmamış olacağı gerekçesidir. İstinaf Mahkemesi bu gerekçeye katılmamaktadır<sup>532</sup>. İstinaf Mahkemesine göre burada ABD adli makamlarının egemenlik hakkına dayanarak güç kullanmaları söz konusudur. Çünkü yurtdışında bulunan verilere, adli makamlara teslim etmek amacıyla erişen taraf (somut olayda **Microsoft**), esasen adli makamların bir yardımcısı gibi hareket etmektedir. Bu tür yardımcıları da adli makamlar ile aynı kurallara tabidir. Dolayısıyla

---

<sup>531</sup> Bilgi için bkz. Microsoft Corp v. United States de 44; Graber, “Where in the World Is Your Data: Who Can Access It?”, s. 160-166; Eichensehr, “Data Extraterritoriality”, s. 150; Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 2; De Hert, Thumfart, “The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies”, s. 7; De Souza Abreu, “Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience”, s. 236; Pecoraro, “Drawing Lines in the Cloud”, s. 88-90; Svantesson, Gerry, “Access to extraterritorial evidence: The Microsoft cloud case and beyond”, s. 481; Kirschenbaum, “Beyond Microsoft: A Legislative Solution to the SCA’s Extraterritoriality Problem”, s. 1941.

<sup>532</sup> Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 331-333; Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 2; Graber, “Where in the World Is Your Data: Who Can Access It?”, s. 163-164.

yardımcı konumunda bulunan **Microsoft**'un İrlanda'daki veri merkezinden gerekli bilgilere erişmesi, el koyma işleminin yurtdışında gerçekleştiği anlamına gelecektir.

İstinaf Mahkemesinin değindiği gerekçelerden birisi de SCA kapsamında verilen bilgi taleplerine ilişkin mahkeme emirlerinin, esasen arama ve el koymaya ilişkin mahkeme kararları ile eldeki bilgilerin teslimini gerektiren mahkeme, jüri ya da idari makam emirlerinin karışımı gibi algılanması gerektiğidir<sup>533</sup>. İstinaf Mahkemesine göre SCA'da mahkeme emri terimini tesadüfen kullanması gibi bir durum olamayacağı gibi SCA metninde, mahkeme emri teriminin mahkeme, jüri ya da idari makam emri olarak anlaşılmasını sağlayacak herhangi bir ifade de bulunmamaktadır. Yüksek Mahkeme kararlarına göre de mevcut bulunan bir hukuki terim, herhangi bir kanun metninde kullanılmışsa bu terimin mevcut hukuki anlamında kullanıldığı kabul edilmelidir. Bunun istisnası, ilgili kanunda bahse konu terimin farklı bir şekilde tanımlanmış olmasıdır. Dolayısıyla yerel mahkemenin SCA kapsamındaki bilgi taleplerine ilişkin mahkeme emirlerinin, fiziki ortamda arama ve el koymaya ilişkin mahkeme kararları ile aynı niteliği taşımadığına ilişkin yorumu İstinaf Mahkemesince uygun bulunmamıştır.

İstinaf Mahkemesi verdiği karar neticesinde iddia makamlarının delil toplamada karşılaşılabileceği zorluklara ilişkin itirazlarının bulunduğunu, ancak mevzuatın mevcut durumu karşısında söz konusu zorluklara çare bulmanın mümkün olmadığını ifade etmiştir. İstinaf Mahkemesi bahse konu delil toplama süreçlerin adli istinabe sözleşmeleri kapsamında yönetildiğini belirterek, verdiği kararın milletlerarası nezaket kurallarını güçlendirdiğini de söylemiştir. Zira yabancı ülkede bulunan bilgilere ABD mahkemelerinin kararları ile erişebilmesinin ilgili yabancı ülkenin yerel hukukunu ve menfaatlerini ihlal etmesi son derece olasıdır. Bu da muhtemel kanunlar ihtilafı sorunlarının doğması anlamına gelecektir. Kanaatimizce burada kanunlar ihtilafı ifadesi ile kastedilen bir olaya uygulanacak hukukun tespitini düzenleyen kurallar değil; çalışmamızın ilk bölümünde ifade edilen hukukların çatışması kavramıdır.

---

<sup>533</sup> Microsoft Corp v. United States de 18-19.



**b. In re Search Warrant No. 16-960-M-01 and No. 16-1061-M to Google Kararı**

Davaya konu olayda iddia makamları, **Google**'ın veri merkezlerinde bulunan ilgili bilgilerin teslimi için Ağustos 2016 tarihinde yerel mahkemelerden arama ve el koymaya ilişkin mahkeme kararı almışlar ve bunu **Google**'a göndermişlerdir. **Google** ise karara konu bilgilerden ABD toprakları içerisinde saklananları tespit ederek teslim etmiştir. Öte yandan ABD sınırları dışında saklanan bilgiler açısından itirazı görmeye görevli olan yerel mahkemeye itirazda bulunmuştur. Yerel mahkeme tarafından verilen **In re Search Warrant No. 16-960-M-01 and No. 16-1061-M to Google** kararı<sup>534</sup>, **Google**'a yönelik olarak iddia makamlarınca alınmış olan iki adet arama ve el koymaya ilişkin mahkeme kararına karşın **Google**'ın itirazlarının birleştirilerek tek dosyada karara bağlanması neticesinde doğmuştur.

**Google**, arama ve el koymaya ilişkin mahkeme kararlarına karşı itirazlarını, önceki başlıkta detayları paylaşılan **Microsoft Corp v. United States** kararına dayandırmıştır. **Google**'a göre söz konusu kararda; SCA kapsamında alınan arama ve el koymaya ilişkin mahkeme kararlarının ABD sınırları dışında bulunan veri merkezlerinde saklanan bilgiler açısından geçerli olmayacağı ifade edildiğinden<sup>535</sup>, huzurdaki davaya konu olaydaki mahkeme kararlarının da kaldırılması gerekmektedir.

Yerel mahkeme, **Google** tarafından verilen beyanlara dayanarak öncelikle **Google**'ın dağıtık bulut bilişim sistemi modelini kullandığı tespit etmiştir<sup>536</sup>. Söz konusu modelde kullanıcıların bulut bilişim sistemine aktardığı veriler çok sayıda parçaya bölünmekte ve bu parçalar bulut bilişim sistemine dahil olan veri merkezleri arasında

---

<sup>534</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google.

<sup>535</sup> Mitchol Dunham, "Arbitrary and Outdated: Reforming the Stored Communications Act", 2018, s. 11-14, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3258774](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258774), 19.03.2020; Shelli Gimelstein, "A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy", **University of Illinois Journal of Law, Technology & Policy**, C. 2018, S. 1, 2018, s. 13; Pecoraro, "Drawing Lines in the Cloud", s. 93.

<sup>536</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 7; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1946; De Hert, Parlar, Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders", s. 348; Gimelstein, "A Location-Based Test for Jurisdiction over Data", s. 11.

dağıtılarak saklanmaktadır. Veri parçaları tekrar bütünleştirilmeden, anlamlı bir bilgiye erişmek mümkün olmamaktadır.

İkinci olarak yerel mahkeme Dördüncü Değişikliğin getirdiği arama ve el koyma kurallarının korudukları değerleri Yüksek Mahkeme kararlarına da değinerek açıklamıştır<sup>537</sup>. Bu kapsamda arama kuralları, kişinin makul gizlilik beklentisini yani özel hayatının gizliliği hakkını korurken; el koyma kuralları kişinin eşyaları üzerindeki zilyetliğini korumaktadır. Her ne kadar bu iki işlem de genellikle art arda uygulanıyor olsa da her zaman bu durum söz konusu olmamaktadır. Örneğin kilitli bir dolaba el konması, el koyma işlemi yapılmasına rağmen arama işlemi yapılmadığını göstermektedir.

Yukarıdaki tespitlerden sonra yerel mahkeme önündeki somut olayda el koyma işlemi bulunmadığına karar vermiştir<sup>538</sup>. Zira talebe konu bilgilerin **Google** tarafından adli makamlara teslim edilmesi bir kopyalama işlemi olacaktır. Söz konusu kopyalama işleminin de bilgilerin sahibi olan kişinin, bilgiler üzerindeki menfaatlerini etkilemesi ya da **Google** hizmetlerinden yararlanmasını engellemesi gibi bir durum söz konusu değildir. Yerel mahkeme, ayrıca eşyanın sahibi kişi üzerinde herhangi bir etki doğurmayan işlemlerin de el koyma sayılmayacağına ilişkin Yüksek Mahkeme kararları ile görüşünü desteklemiştir<sup>539</sup>.

Yerel mahkeme, arama işleminin ise ancak **Google** tarafından talep edilen bilgilerin adli makamlara tesliminden sonra yapılabileceğini ifade etmiştir. Buna gerekçe olarak ise bilgilerin sahibi olan kişinin özel hayatının gizliliği hakkının adli makamların ilgili bilgileri gördüğü anda ihlal edilmiş olacağını göstermiştir. Adli makamlar da talebe konu bilgileri ABD topraklarında inceleyecekleri için arama işlemi de esasen ABD

---

<sup>537</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 18-19; Dunham, “Arbitrary and Outdated: Reforming the Stored Communications Act”, s. 11-14; Winston Maxwell, Mark W. Brennan, Arpan A. Sura, “Demystifying the U.S. CLOUD Act: Assessing the law’s compatibility with international norms and the GDPR”, **Hogan Lovells**, 2019, s. 19, (Çevrimiçi) [https://www.hoganlovells.com/~media/hoganlovells/pdf/2019/2019\\_01\\_15\\_whitepaper\\_demystifying\\_the\\_us\\_cloud\\_act.pdf](https://www.hoganlovells.com/~media/hoganlovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf), 14.03.2020.

<sup>538</sup> In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 18.

<sup>539</sup> a.g.e., s. 21.

toprakları içerisinde gerçekleşmiş olacaktır. Yerel mahkemeye göre açıklanan durum nedeniyle SCA kapsamında alınan arama ve el koymaya yönelik mahkeme kararlarının yurtdışında uygulanması durumu söz konusu değildir.

Yerel mahkeme, **Microsoft Corp v. United States** kararında bahsi geçen milletlerarası nezaket kurallarının güçlendirildiği görüşünü de eleştirmiştir<sup>540</sup>. Yerel mahkemeye göre **Google**'ın kullandığı dağınık bulut bilişim sistemi modelinde verilerin hangi ülkede bulunduğunu tespit etmek mümkün olmamaktadır<sup>541</sup>. Bu nedenle soyut hukuki tartışmalar ya da varsayımlar yerine somut gerçekliklere odaklanmak yerinde olacaktır.

Yerel mahkeme ayrıca mahkemelerin kanunları makul olmayan ya da anlamsız sonuçlar doğuracak şekilde yorumlamaması kuralına değinerek **Microsoft Corp v. United States** kararına uygun şekilde SCA'yı yorumlamanın söz konusu kurala aykırılık teşkil edeceği sonucuna iki gerekçeye dayanarak varmıştır<sup>542</sup>. İlk gerekçe, yabancı ülkelerde bulunan verilerin talebinin adli istinabe sözleşmeleri çerçevesinde çözümlenmesinin hem uzun süre alması ve maliyetli olması hem de her ülkeyle bu anlaşmaların bulunmamasıdır. İkincisi ise **Google**'ın kullandığı dağınık bulut bilişim sisteminin verinin konumunu tespit edilemez veya sürekli değişken şekilde bırakması nedeniyle adli istinabe sözleşmelerinin uygulanmasının imkânsız olacağı görüşüdür. Kanaatimizce her ne kadar ikinci gerekçe yerinde olsa da ilk gerekçeye dayanılması; adli istinabe süreçlerinin SCA'nın CLOUD Act ile güncelleştirilmiş versiyonunda dahi yabancı ülkeler için kullanılması gereken bir yol olarak konumlandırılmış olması karşısında önemli bir tutarsızlık teşkil etmektedir. ABD'nin kendi mahkemelerine adli istinabe süreçlerine dayanmaksızın bilgi alma imkânı tanırken yabancı devletleri adli istinabe süreçlerine başvurmaya zorlaması, ABD'nin bu konudaki politikalarını yansıtan önemli örneklerden birisini teşkil etmektedir.

---

<sup>540</sup> **a.g.e.**, s. 25-26.

<sup>541</sup> De Hert, Parlar, Thumfart, "Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders", s. 348.

<sup>542</sup> "In the United States District Court for the Eastern District of Pennsylvania Memorandum of Decision", 2017, (Çevrimiçi) <https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf>, 10.11.2021.

#### 4. CLOUD Act ile Tadil Edilen SCA'nın Getirdiği Kurallar

##### a. SCA'ya Genel Bakış

SCA'nın temel amacı, Dördüncü Değişiklik çerçevesinde dijital ortamda yeterince korunamayacağı düşünülen kişilerin özel hayatın gizliliği hakkının, korunmasını sağlamaktadır<sup>543</sup>. SCA, söz konusu amacı gerçekleştirmek için bilgi paylaşımına ilişkin çeşitli esasa ve usule ilişkin konuları düzenlemektedir. Bu başlık altında tüm maddelere genel olarak değinilecektir.

SCA'nın 2701 numaralı bölümü altında, TCK'nın onuncu bölümünde düzenlenen bilişim suçlarına benzer hükümlere yer verilmiştir. Bu şekilde bahse konu bilgilerin gizliliğinin sağlanması açısından ceza hukuku çerçevesinde de koruma öngörülmektedir.

2702 numaralı bölümde hizmet sağlayıcıların iddia makamları da dahil olmak üzere üçüncü kişilerle gönüllü olarak bilgi paylaşımları düzenlenmektedir. 2703 numaralı bölüm iddia makamlarının bilgi taleplerinin koşullarını belirlemektedir. 2705 numaralı bölümde de taleplere konu bilgilerin esas sahibi olan kişilere yapılacak bildirimlerin geciktirilmesine ilişkin kurallar getirilmektedir. 2709 numaralı bölümde de karşı istihbarat faaliyetleri kapsamında iletişime ilişkin işlem kayıtlarına erişilmesine ilişkin şartlar düzenlenmektedir. CLOUD Act ile yeni eklenen 2713 numaralı bölümde de SCA kapsamındaki bilgi taleplerinin, ilgili bilgilerin ABD dışında bulunup bulunmasına bakılmaksızın bağlayıcı olacağı hüküm altına alınmıştır.

2704 numaralı bölüm, iddia makamlarınca talep edilen bilgilerin teslim edilmesine kadar geçecek süre içerisinde yedeklerinin alınıp saklanmasına ilişkin kuralları belirlemektedir. Böylelikle hukuki süreçler boyunca söz konusu bilgilerin yok edilmesi ihtimali önlenmektedir. 2706 numaralı bölüm altında ise iddia makamlarınca talep edilen bilgilere karşı talep edilecek ücretler hakkında düzenlemeler yapılmıştır.

---

<sup>543</sup> Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", *The George Washington Law Review*, C. 72, 2003, s. 1209-1213; Daskal, "The Un-Territoriality of Data", s. 355.

2707 ve 2712 numaralı bölümlerde de sırasıyla hizmet sağlayıcılar ile ABD devletine karşı açılacak özel hukuk sorumluluğu davaları hakkında kurallar belirlenmiştir.

SCA'nın sistematığıne göre ayrılmış sonraki başlıklar altında, SCA'nın hükümleri incelenecektir. Ancak işbu çalışma konusu kapsamı dışında kalan SCA bölümlerine (örneğin ceza hukukuna ilişkin hükümler ya da bilgi taleplerinin ücretlendirilmesi gibi) değinilmeyecektir.

### b. SCA'da Yer Alan Önemli Tanımlar

SCA'nın kapsamı içerisinde temel olarak iki hizmet tipi bulunmaktadır. Bunlardan ilki elektronik iletişim hizmeti (**electronic communication service**); ikincisi uzaktan bilgi işleme hizmetidir (**remote computing service**)<sup>544</sup>. Elektronik iletişim hizmeti sağlayıcıları, dijital ortamda e-posta ya da anlık mesajlaşma hizmetlerini sunan kişilerdir<sup>545</sup>. Elektronik iletişim hizmeti sağlayıcıların temel özelliği, iletişimin sağlanması amacıyla bilgileri geçici olarak saklamaları ya da başkalarına aktarmalarıdır.<sup>546</sup> Uzaktan bilgi işleme hizmeti sağlayıcıları ise kişilere veri işleme hizmeti sunan kişilerdir<sup>547</sup>. Uzaktan bilgi işleme hizmeti sağlayıcılarının temel özelliği ise kendilerine aktarılan bilgileri kalıcı olarak saklamaları veya işlemeleridir<sup>548</sup>. Her iki kavram da 1986 yılının teknolojik durumuna göre tanımlanmıştır<sup>549</sup>.

<sup>544</sup> Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", s. 386; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 78; Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act", s. 327; Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", s. 1205; Lin, "Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption", s. 1104; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1214.

<sup>545</sup> "Report No.99-541", U.S. Code Congressional and Administrative News (U.S.C.C.A.N.), 1986, (Çevrimiçi) <https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf>, 11.11.2022.

<sup>546</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1214.

<sup>547</sup> Rojszczak, "CLOUD act agreements from an EU perspective", s. 4; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1214. Ayrıca bkz. SCA m. 2711(2).

<sup>548</sup> Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", s. 1206-1207.

<sup>549</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1214.

Sunulacak hizmet tipine göre bir hizmet sağlayıcının hem elektronik iletişim hizmeti sağlayıcısı hem de uzaktan bilgi işleme hizmeti sağlayıcısı olması mümkündür<sup>550</sup>. Örneğin günümüzde tüketicilerin kullanımına sunulan e-posta hizmetlerini (**Gmail** ya da **Hotmail** gibi) sunan şirketler e-postaların iletimi açısından elektronik iletişim hizmeti; e-postaların saklanması açısından ise uzaktan bilgi işleme hizmeti sağlayıcısı olarak konumlanmaktadır. Bulut bilişim sağlayıcıların genellikle her iki tanıma teker teker ya da birlikte uyan çeşitli hizmetler sunduğunu belirtmekte fayda vardır.

Hizmet sağlayıcıların kategorize edildiği bir diğer alan da kamuya hizmet sunup sunmamalarıdır<sup>551</sup>. SCA kapsamında bir elektronik iletişim sağlayıcının tabi olduğu hükümler, hizmetlerini kamuya açık olarak sunup sunmamasına göre değişiklik göstermektedir. Aynı durum uzaktan bilgi işleme hizmeti sağlayıcıları için de geçerlidir. Söz konusu ayrımı somutlaştırmak gerekirse, **Hotmail** ya da **Gmail** gibi e-posta hizmetleri, tüm kamuya sunulmaktadır. Herhangi bir kişi bu hizmetlerden yararlanabilmektedir. Ancak bir üniversitenin sunduğu edu.tr uzantılı e-posta hizmetleri sadece o üniversite ile ilişkili kişilere sunulduğu için kamuya açık değildir. Söz konusu ayrımın gerekçesi, kamuya hizmet sunan hizmet sağlayıcılardaki kullanıcı hesaplarının temel faydalanıcısının kullanıcılar olmasına rağmen kamuya açık olmayan hizmet sağlayıcılardaki kullanıcı hesaplarının temel faydalanıcısının esasen hizmet sağlayıcı olmasıdır<sup>552</sup>. Örneğin bir şirket tarafından çalışanlara tahsis edilen e-posta hesaplarında, şirketin menfaati ön plandadır. Zira söz konusu e-posta hesabı ticari faaliyetlerin sürdürülebilmesi için tahsis edilmiştir. Buna karşılık **Google** nezdinde açılmış bir bireysel kullanıcı hesabında **Google**'ın herhangi bir menfaati bulunmamaktadır. Bu ayrımın etkileri sonraki başlıklarda görülecektir.

SCA ile konular incelenirken bulut bilişim sağlayıcı terimi yerine kanuni terimler olan elektronik iletişim sağlayıcısı ve uzaktan bilgi işleme hizmeti sağlayıcısı terimleri

---

<sup>550</sup> Robinson, "Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act", s. 1209-1214; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1215.

<sup>551</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1226-1227.

<sup>552</sup> Kerr, a.y.

kullanılacaktır. Ayrıca hizmet sağlayıcı terimi de her iki tür sağlayıcıyı birlikte ifade etmek amacıyla kullanılacaktır. Dijital ortam açısından her iki hizmet tipi de bugün bulut bilişim sağlayıcıları tarafından sağlanmakta olduğu için çalışmamız kapsamında olmayan farklı kişilerden bahsedilmesi söz konusu olmamaktadır.

### **c. SCA Kapsamında Hizmet Sağlayıcıların Gönüllü Olarak Bilgi Paylaşması**

SCA'nın 2702 numaralı bölümü altında düzenlenen hizmet sağlayıcıların gönüllü olarak üçüncü kişilerle bilgi paylaşması kuralları, ilgili bilgileri iki kategoriye ayırmaktadır<sup>553</sup>. Bu kategorilerden ilki içeriktir. İçerik, ilgili iletişimin taşıdığı mesajın içeriğine ve anlamına ilişkin her türlü bilgi olarak tanımlanmıştır<sup>554</sup>. İletişime ilişkin olarak içerik harici bilgiler de ikinci kategoriye oluşturmaktadır. Ayrıca belirtmek gerekir ki bahse konu üçüncü kişiler içine iddia makamları da dahildir.

SCA'ya göre kamuya hizmet sunan hizmet sağlayıcıların gönüllü olarak üçüncü kişilerle içerik bilgisi paylaşması yasaktır<sup>555</sup>. Ancak hizmet sağlayıcının kamuya hizmet sunmaması halinde, gönüllü olarak üçüncü kişilerle içerik bilgisi paylaşmaları önünde herhangi bir engel bulunmamaktadır<sup>556</sup>. Bir diğer kural da kamuya hizmet sunan hizmet sağlayıcıların, içerik harici bilgileri sadece kamu kurum ve kuruluşları (iddia makamları dahil) ile paylaşmalarını engellemektedir<sup>557</sup>. Ancak kamuya hizmet sunan sağlayıcılar, içerik harici bilgileri kamu kurum ve kuruluşları olmayan kişilerle gönüllü olarak paylaşabilmektedirler<sup>558</sup>. Kamuya hizmet sunmayan hizmet

---

<sup>553</sup> Blackman, Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", s. 2; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1227-1228.

<sup>554</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1228.

<sup>555</sup> Thompson II, Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)", s. 3-4; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1220; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 78-79.

<sup>556</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 79; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1220.

<sup>557</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1220.

<sup>558</sup> Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", s. 387; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 79. Ayrıca bkz. SCA m. 2702.

sağlayıcıların ise içerik haricindeki iletişime ilişkin bilgileri herkesle paylaşabilmeleri mümkündür<sup>559</sup>.

İletişimlerin içeriğine ilişkin bilgiler ile içerik haricindeki bilgilerin paylaşımına ilişkin yukarıda belirtilen yasakların istisnaları bulunmaktadır<sup>560</sup>. Söz konusu istisna kuralları içerik ile içerik haricindeki bilgiler açısından farklılaşmaktadır. İçeriğin iletişimin muhatabı olan kişiye aktarılması, kanunlarda paylaşımın öngörülmesi (örneğin gerekli mahkeme kararlarının alınmasından sonra paylaşım), iletişimin hedefine ulaştırılması konusunda görevli olan kişilere aktarılması, hizmet sağlayıcının hizmetlerinin, haklarının veya mallarının korunması amacıyla paylaşılması halleri hayatın olağan akışına uygun ve ilgili hizmetlerin sunulabilmesi için gerekli olan istisnalardandır<sup>561</sup>. Çocuk pornosu ile mücadele ya da hizmet sağlayıcı tarafından yanlışlıkla elde edilmiş ve bir suça ilişkin gözüken içeriğin kolluk kuvvetlerine aktarılması şeklinde istisnalar da bulunmaktadır<sup>562</sup>. Yine iletişimin taraflarından birisinin ya da uzaktan bilgi işleme hizmetinin abonesinin içeriğin paylaşımı konusunda rıza göstermesi de istisna kabul edilmiştir<sup>563</sup>. Son istisna kuralı ise bir kişinin ölüm ihtimali olması ya da ciddi şekilde yaralanma ihtimali bulunması halinde ilgili içeriklerin paylaşılması şeklindedir<sup>564</sup>. CLOUD Act ile getirilen yeni istisna kuralı, CLOUD Act kapsamında imzalanacak bilgi paylaşımına ilişkin uluslararası sözleşme çerçevesinde yabancı devletlerin bilgi taleplerinin karşılanmasıdır.

İletişime dair içerik harici diğer bilgilerin üçüncü kişilerle gönüllü olarak paylaşılmasına ilişkin istisna kuralları ile çok büyük oranda aynı oldukları için burada tekrar sayılmayacaklardır.

---

<sup>559</sup> Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1220.

<sup>560</sup> Kerr, **a.g.e.**, s. 1221.

<sup>561</sup> Kerr, **a.y.**

<sup>562</sup> Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 79; Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1221-1222.

<sup>563</sup> Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1221.

<sup>564</sup> Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 79; Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1221.



Kanaatimizce anılan istisna kurallarının ülkemizden ABD şirketlerine yapılan bilgi talepleri açısından önem taşıdığı açıktır. Zira uygulamada **Facebook**, **Twitter** ya da **Google** gibi şirketlerin Türk adli makamlarından gelen bilgi taleplerinden yalnızca ölüm ya da ciddi yaralanma tehlikesi içinde kaybolma ile çocuk pornosuna ilişkin olanları yanıtladıkları görülmektedir. SCA metni de göz önüne alındığında bahse konu uygulamanın SCA'nın imkân verdiği istisnai paylaşım kuralları ile eşleştiği gözlemlenmektedir. Söz konusu uygulama, aynı zamanda ABD'nin iç hukuk kurallarının Türk kolluk kuvvetlerinin görev yapmasını engelleyecek şekilde uygulama alanı bulabildiğini göstermektedir. Mevcut durumun, 2022 yılında 5651 sayılı kanunda yapılan değişiklikler neticesinde değişip değişmeyeceği, ilgili kanun değişikliğinin uygulamasının gözlemlenmesi ile verilebilecektir.

#### **d. SCA Kapsamında İddia Makamlarının Bilgi Talepleri**

SCA çerçevesinde hizmet sağlayıcılardan talep edilebilecek bilgiler temel olarak üç kategoriye ayrılmıştır. Bunlar içerik, içerik harici bilgiler ve temel abone bilgileridir<sup>565</sup>. Önceki bölümlerde de açıklandığı üzere içerik ilgili iletişimin taşıdığı mesajın içeriğine ve anlamına ilişkin her türlü bilgidir. Geçmişten günümüze kullanılmış olan her iletişim aracında en sıkı şekilde korunan bilginin içerik olduğu görülmektedir. Nitekim internet çağında da bu durum değişmemiştir.

Temel abone bilgileri SCA içerisinde isim, adres, arama tarihleri ve süreleri ile uzun ya da kısa mesafeye ilişkin telefon kayıtları, telefon numarası, cihaz numarası, geçici olarak atanmış ağ adresleri de dahil olmak üzere abone numarası ya da kimliği, verilen hizmetlerin süreleri (başlangıç tarihi de dahil), hizmete ilişkin ödeme aracı ve bu araca

---

<sup>565</sup> Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1077.

ilişkin bilgiler olarak sıralanmıştır<sup>566</sup>. İçerik ya da temel abone bilgileri dışında kalan her türlü bilgi de içerik harici bilgi olarak kabul edilmektedir<sup>567</sup>.

SCA'ya göre bir elektronik iletişim sağlayıcının, elektronik saklama ortamında 180 günden daha az süre boyunca saklanmakta olan içerik bilgilerine erişmek sadece bir mahkeme kararı ile mümkündür<sup>568</sup>. Buna karşılık elektronik iletişim sağlayıcının elektronik saklama ortamında 180 günden fazla süre boyunca saklanmakta olan içerik bilgileri ile uzaktan bilgi işleme hizmeti sağlayıcıların sistemlerinde saklanan bilgilerin talebi için iddia makamlarının üç farklı seçeneği bulunmaktadır<sup>569</sup>. Bunlardan ilki mahkeme kararı almaktır. Daha önce de açıklandığı üzere bahse konu mahkeme kararlarının Dördüncü Değişiklik kapsamında gerçekleştirilecek bilgi talepleri için alınacak mahkeme kararları ile aynı şartları taşıması gerekmektedir.

İçerik bilgisinin talebi için iddia makamlarının elindeki diğer iki seçenek, bilginin sahibi olan kişilere; bilginin talebinden önce içerik bilgilerine erişileceğine ilişkin bildirim yapılmasını gerektirmektedir<sup>570</sup>. Bu bildirim yanında iddia makamlarının ya mahkeme, jüri ya da idari makam emri alması gerekmekte ya da 2703 (d) emri adı verilen farklı bir tür hâkim emri alması ihtiyacı bulunmaktadır<sup>571</sup>. Kısaca d emri olarak

---

<sup>566</sup> Bkz. SCA m. 2703(c)(2). Ayrıca bkz. Maillart, “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, s. 387; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 79; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1077; Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1219-1220; Graber, “Where in the World Is Your Data: Who Can Access It?”, s. 160.

<sup>567</sup> Bir görüşe göre söz konusu bilgilerin tamamını *metadata* içermektedir. Detaylı bilgi için bkz. Ustaran, **European Data Protection Law and Practice**, s. 308-310.

<sup>568</sup> Bkz. SCA m. 2703(a). Ayrıca bkz. Battey, “A Step in the Wrong Direction”, s. 268; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 80; Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1218; Lin, “Where Are Your Papers: The Fourth Amendmnet, the Stored Comunciations Act, the Third Party Doctrine, the Cloud and Encryption”, s. 1094.

<sup>569</sup> Graber, “Where in the World Is Your Data: Who Can Access It?”, s. 162; Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 327; Thompson II, Cole, “Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)”, s. 5; Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1218-1219; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 79.

<sup>570</sup> Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, s. 1219.

<sup>571</sup> Bkz. SCA m. 2703(d). Ayrıca bkz. Thompson II, Cole, “Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)”, s. 5; Peters vd., “Not an Ocean Away, Only a

da anılan bu hâkim emrinin çıkarılabilmesi için adli makamların yürütölmekte olan bir suç soruşturmaları ile talep edilen içerik bilgisinin ilgili olabileceğine dair makul sebepleri bulunduğuna inanmasını gerektiren belirli ve net durumlar bulunması gerekmektedir<sup>572</sup>. Söz konusu gereksinim, d emirlerini, iddia makamlarının yerine getirmesi gereken şartların zorluğu bakımından mahkeme kararları ile mahkeme, jüri ya da idari makam emirleri arasına yerleştirmektedir<sup>573</sup>. Bu işlemler yerine bilgilerin sahibi olan kişiden rıza alınması halinde de iddia makamlarının içerik harici bilgileri talep edebilmesi mümkün olmaktadır<sup>574</sup>.

Temel abone bilgilerinin iddia makamlarınca talep edilebilmesi ise sadece mahkeme, jüri ya da idari makam emri alınmasına bağılı kılınmıştır. Bu durumun gerekçesi söz konusu bilgilerin gizlilik seviyesi en yüksek olarak kabul edilen içerik bilgileri ile daha düşük olarak kabul edilen içerik harici bilgilere kıyasla daha düşük görülmesidir<sup>575</sup>.

Son olarak değinilmesi gereken husus SCA'nın, öngördüğü bilgi talebi yöntemleri açısından "çoğu yapmaya yetkili olan azı da yapmaya yetkilidir" prensibini kabul etmiş olmasıdır. Örnek vermek gerekirse içerik bilgisine erişmek için alınmış bir mahkeme kararı, aynı zamanda iddia makamlarına içerik harici bilgiler ile temel abone bilgileri de talep etme hakkını sağlar. Bu yaklaşımın temel nedeni, süreçlerin verimliliğini ya da bir başka deyişle usul ekonomisini sağlamaktır.<sup>576</sup>

---

Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1078; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 79; Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act", s. 327; Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't", s. 620; Thompson II, Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)", s. 5.

<sup>572</sup> Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1078; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1219.

<sup>573</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 79; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1219.

<sup>574</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1219.

<sup>575</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 79-80; Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1219.

<sup>576</sup> Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", s. 1220.

**e. SCA'nın Doğurduğu Hukukların Çatışması Sorunları ve Bunların Çözümüne İlişkin Kuralları**

**(1) SCA'nın Sınır Ötesi Uygulama Kapsamına İlişkin Kuralları ve Doğurabileceği Hukukların Çatışması Sorunu**

CLOUD Act öncesinde SCA'nın yurtdışındaki veri merkezlerinde bulunan bilgilere uygulanıp uygulanmayacağı tartışmalıdır. Yukarıda da açıklandığı üzere bu konuda değişik sonuçları olan mahkeme kararları verilmiş olup konu en son olarak ABD Yüksek Mahkemesi önüne kadar gelmiştir. Ancak ABD Yüksek Mahkemesi konu ile ilgili bir karar vermeden ABD Kongresi CLOUD Act'i çıkararak SCA üzerinde birtakım değişikliklere gitmiş ve bu konuyu kanuni düzenleme yoluyla netleştirmiştir. SCA'nın 2713 numaralı bölümü olarak CLOUD Act ile eklenen yeni bir maddeye göre SCA'nın iletişime ilişkin her türlü bilgi talebine dair hükümleri, söz konusu bilgilerin ABD sınırları içerisinde bulunup bulunmadığına bakılmaksızın uygulama alanı bulacaktır<sup>577</sup>. SCA'nın bu hükümlerinin uygulanabilmesi için gerekli olan ilgili elektronik iletişim hizmeti sağlayıcı ya da uzaktan bilgi işleme hizmeti sağlayıcının bahse konu bilgileri elinde ya da muhafazasında bulundurması ya da kontrolü altında tutmasıdır. Bir başka anlatımla, ABD sınırları içerisinde bulunan bir hizmet sağlayıcı, dünyanın herhangi bir yerinde elinde, muhafazasında ya da kontrolü altında bulundurduğu bilgileri; SCA'ya uygun bir talep alması halinde ABD iddia makamlarına teslim etmek zorundadır. Söz konusu paragraf ile SCA'nın sınır ötesi uygulama kapsamına sahip olduğu kesin bir şekilde ifade edilmiştir<sup>578</sup>.

Yukarıda açıklanan davalara<sup>579</sup> konu olan **Google** ve **Microsoft** gibi şirketler her ülkede farklı tüzel kişilikler kurarak faaliyet göstermektedir. Bu ülkelerde bulunan

<sup>577</sup> Tim Cochrane, "Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers", **Duke Journal of Comparative & International Law**, C. 32:153, 2021, s. 160-161; Blackman, Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", s. 3; Maillart, "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime", s. 386.

<sup>578</sup> Cook, "Cross-Border Data Access and Active CyberDefense: Assessing Legislative Options for a New International Cybersecurity Rulebook", s. 227; Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 9; Bilgic, "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act", s. 334.

<sup>579</sup> Bkz. Yuk. s. 150 vd.

şirketlerin hisseleri doğrudan ya da dolaylı olarak ABD’de bulunan ana şirkete ait olmaktadır. Örneğin daha önceki bölümde bahsedilen **Microsoft**’un taraf olduğu davalara konu olan bilgiler, mahkeme kararlarından anlaşıldığı üzere İrlanda’da bulunmaktadır. İrlanda’daki **Microsoft** veri merkezinin sahibi olan **Microsoft** şirketi, ABD’de bulunan ana **Microsoft** şirketinden farklı bir tüzel kişiliktir. SCA’ya eklenen yeni madde çerçevesinde, ABD’de bulunan ana **Microsoft** şirketinin İrlanda’da bulunan bağlı **Microsoft** şirketi üzerinde kontrole sahip olduğu kabul edilmektedir. Bu kontrol kapsamında, yetkili bir ABD makamından, ABD’de yerleşik ana **Microsoft** şirketine bilgi talebi gittiği zaman; ABD’de bulunan bu şirket ilgili bilgileri kontrolü altında bulunan İrlanda’daki bağlı **Microsoft** şirketinden alıp mahkemeye teslim etmek zorundadır. Dolayısıyla genel olarak ABD merkezli tüm hizmet sağlayıcılarının sakladığı bilgilerin, bulundukları yerler fark etmeksizin ABD makamlarınca erişilebilir olduğu sonucuna varılmaktadır.

SCA’ya getirilen sınır ötesi uygulama kapsamının diğer ülke kanunları ile çelişkili hükümler getirebileceğine şüphe yoktur. Örnek vermek gerekirse 5411 sayılı Bankacılık Kanunu<sup>580</sup> m. 73, Türk bankalarını yurtdışına veri aktarımının sınırlarını çizmektedir. SCA’nın Türkiye’de bulunan ve Türk bankalarının verilerini barındıran bir veri merkezi için uygulanması halinde, SCA’nın hükümleri ile Bankacılık Kanunu hükümleri arasında çelişki ortaya çıkacaktır. Bilgi talebi muhatabının herhangi bir hukuka uygun davranması, diğer hukuku ihlal etmesi sonucunu doğuracaktır.

SCA ile Bankacılık Kanunu çelişmesi örneği aslında çalışmamızın ilk bölümünde açıklanan hukukların çatışması kavramına tipik bir örnek teşkil etmektedir. Zira burada belirli veriler üzerinde hangi ülke hukuk kurallarının uygulanacağı sorunu bulunmaktadır. Ancak bahse konu sorun, kanunlar ihtilafı kavramı altında açıklanan hangi özel hukuk kurallarının değil, hangi kamu hukuku kuralların uygulama alanı bulacağı sorunudur. Kanaatimizce işte bu nedenle bu sorunu MÖHUK ya da muadilleri içerisinde bulunan gösterici nitelikteki milletlerarası özel hukuk kuralları

---

<sup>580</sup> “5411 Sayılı Bankacılık Kanunu”, (2005), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5>, 17.10.2021.

ile çözmek mümkün değildir. Ayrıca ABD dışındaki ülkelerde, bahse konu bilgi taleplerinin herhangi bir mahkemeye veya idari makama intikal etmesi genellikle söz konusu olmadığı için ev sahibi devletin idari ya da yargı organlarının da duruma müdahil olma şansı bulunmamaktadır. Bu şekilde adeta ev sahibi devletin haberi dahi olmadan, yabancı bir devletin hukuku; ilgili ev sahibi devlet ülkesinde uygulanmaktadır.

Önemle belirtmek gerekir ki verilerin konumuna ve yurtdışına aktarımına ilişkin dünya çapında birçok düzenleme bulunmakta olup söz konusu düzenlemeler sadece ülkemize özgü değildir. Dolayısıyla SCA hükümlerinin yaratacağı hukukların çatışması sorunu, sadece ülkemize has bir problem değildir. Nitekim ABD kanun koyucusu tarafından da yukarıda tanımlanan hukukların çatışması<sup>581</sup> sorunu öngörülmüştür. Bu nedenle SCA içerisinde hukukların çatışması sorunlarının çözümüne ilişkin hükümlere yer verilmiştir.

## **(2) Hukukların Çatışması Sorununun Çözümlerine Yönelik SCA Kuralları**

SCA'nın hukukların çatışması sorunu yaratacağı öngörülmüş olduğu için bunların çözümüne yönelik düzenlemeler de SCA içerisine eklenmiş durumdadır. Bu kapsamda getirilen en büyük düzenleme ABD Hükümeti'ne, dijital ortamda bulunan bilgilere erişim konusunda uluslararası adli istinabe sözleşmesi imzalama yetkisi verilmesidir. Bu sözleşmeler bir anlamda yeni nesil adli istinabe sözleşmeleri olup taraf ülkeler arasında bilgi paylaşımını hızlandırmayı amaçlamaktadırlar<sup>582</sup>. Söz konusu sözleşmelere taraf olma veya olmama durumu, hukukların çatışması sorunlarının nasıl çözümlenmesinde uygulanacak kuralları da etkilemektedir.

---

<sup>581</sup> Önemle belirtmek gerekir ki bu kavramın karşılığı, SCA içerisinde “**conflict of laws**” olarak kullanılmıştır. Dolayısıyla ABD ve İngiliz hukukları terminolojilerinde “kanunlar ihtilafı” teriminin karşılığı olarak kullanılan bu terim; SCA içerisinde kamu hukuku kurallarının çatışmasını ifade etmek için de kullanılmıştır. Ancak çalışmamız kapsamında kamu hukuku kurallarının çatışması “hukukların çatışması” olarak adlandırıldığı için; SCA'daki “**conflict of laws**” kavramı, “hukukların çatışması” olarak tercüme edilmiştir.

<sup>582</sup> Söz konusu adli istinabe sözleşmeleri hakkında Bkz. 18 U.S. Code m. 2523. Ayrıca bkz. Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 4.

SCA içerisinde, SCA'nın yaratabileceği hukukların çatışması sorununun çözümüne ilişkin olarak iki temel kural seti öngörülmüştür<sup>583</sup>. Bunlardan ilki CLOUD Act'in 103(c) paragrafı ile yürürlüğe konan açıklayıcı maddedir. Söz konusu maddeye göre SCA içerisinde yer alan hiçbir hüküm, müşterek hukukun (**common law**) milletlerarası nezaket kurallarının uygulanmasına engel olmayacaktır. İkinci kural seti ise SCA kapsamında dijital ortamda yer alan bilgilere erişime ilişkin adli istinabe sözleşmesi imzalayan devletlerin hukukları ile meydana gelebilecek hukukların çatışması sorunlarının nasıl çözümleneceğini açıklamaktadır. Netice itibarıyla SCA içerisinde, adli istinabe sözleşmesi imzalayan ve imzalamayan devletler arasında ayrıma gidilerek her iki durumda da meydana gelebilecek hukukların çatışması sorunlarının çözümüne ilişkin kurallar belirlenmiştir<sup>584</sup>.

#### **i. SCA Kapsamında Uluslararası Adli İstinabe Sözleşmesi İmzalayan Devletlere İlişkin Hukukların Çatışması Sorunlarının Çözümü**

SCA içerisinde ABD ile uluslararası adli istinabe sözleşmesi imzalayan devletler, yeterli yabancı devlet<sup>585</sup> olarak tanımlanmaktadır<sup>586</sup>. Yeterli yabancı devlet olarak kabul edilmenin bir diğer şartı da elektronik iletişim hizmeti ve uzaktan bilgi işleme hizmeti sağlayıcılarına, SCA'nın 2703 (h) kısmında yer alanlarla benzer itiraz haklarını ve usullerini tanımaktır. SCA itiraz imkânını, bilgi talebinin muhatabı olan elektronik iletişim hizmeti veya uzaktan bilgi işleme hizmeti sağlayıcısına tanınmıştır<sup>587</sup>. Burada talebe konu bilginin sahibi olan gerçek ya da tüzel kişiliğe itiraz hakkı tanınmadığını vurgulamak gerekmektedir. Örnek vermek gerekirse **Google**'ın bulut bilişim hizmetlerini kullanan bir şirket, kendi verilerinin talebine ilişkin mahkeme kararına SCA çerçevesinde itiraz edemeyecektir.

---

<sup>583</sup> Schwartz, "Legal Access To The Global Cloud", s. 1715; Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 3-4; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1092.

<sup>584</sup> Detaylı bilgi için bkz. SCA m. 2703.

<sup>585</sup> Yeterli yabancı devlet olarak tanımlanan devletlere orijinal hali ile qualifying foreign government denmektedir.

<sup>586</sup> Bkz. SCA m. 2703(h)/1-A. Ayrıca bkz. Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 3; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 92; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 426; Schwartz, "Legal Access To The Global Cloud", s. 1715.

<sup>587</sup> Bkz. SCA m. 2703(h).

Hizmet sağlayıcıların itiraz süresi, ilgili bilgi talebine ilişkin belgenin tebliğinden itibaren 14 gün olarak belirlenmiştir<sup>588</sup>. Bu sürenin mahkeme kararıyla ya da iddia makamıyla anlaşılması vasıtasıyla uzatılması mümkündür. İtiraz talebini alan mahkemenin, konuya ilişkin olarak bilgi talebini mahkemeye ileten iddia makamının da görüşünü alması gerekmektedir.

SCA 2703(h)/2-A, hizmet sağlayıcıların sadece içeriklere ilişkin bilgi taleplerine itiraz hakları olduğunu düzenlemiştir. İçerik harici bilgiler ve temel abone bilgileri hakkında herhangi bir itiraz mekanizması öngörülmemiştir. Hizmet sağlayıcıların itiraz edebilmesi için ise iki adet itiraz sebebinin birlikte varlığı aranmaktadır<sup>589</sup>. Bunlardan ilki bilgileri talep edilen kişinin bir ABD kişisi olmaması ya da ABD’de yerleşik olmaması iddiasıdır. Diğeri ise talep edilen bilgilerin ifşası halinde yeterli yabancı devletin hukukunun ihlal edileceği iddiasıdır.

ABD kişisi kavramı, CLOUD Act ile SCA’ya eklenen yeni bir terim olup uluslararası adli istinabe sözleşmelerine ilişkin 2523 numaralı bölüm altında tanımlanmıştır. Söz konusu tanıma göre ABD vatandaşları, ABD’de kalıcı ikamet iznine sahip kişiler, çoğunluk üyesi ABD vatandaşlarından ya da ABD’de kalıcı ikamet iznine sahip kişilerden oluşan dernek, vakıf ya da kulüp ve benzeri kuruluşlar ile ABD’de kurulmuş şirketler ABD kişisidir<sup>590</sup>.

İtiraz talebini alan mahkeme, SCA 2703(h)/2-B içerisinde belirlenen üç sebebin birlikte var olduğu kanaatine varırsa, bilgi talebi içeren ve itiraz konusu olan işlemin kaldırılmasına ya da değiştirilmesine karar verebilecektir<sup>591</sup>. Bunlardan ilk ikisi; bilgileri talep edilen kişinin bir ABD kişisi olmaması ya da ABD’de yerleşik olmaması ve talep edilen bilgilerin ifşası halinde yeterli yabancı devletin hukukunun ihlal

---

<sup>588</sup> Bkz. SCA m. 2703(h)/2-A.

<sup>589</sup> Bkz. SCA m. 2703(h)/2-A(i) ve 2703(h)/2-A(ii). Ayrıca bkz. Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 103; Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 338.

<sup>590</sup> Bkz. SCA m. 2523(a)/2. Ayrıca bkz. Daskal, “Privacy and Security Across Borders”, s. 1039; Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 8-9.

<sup>591</sup> Blackman, Gerber, “CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications”, s. 4-5; Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 9.



edileceğinin tespit edilmesidir. Üçüncü sebep ise konuya ilişkin tüm koşullar birlikte değerlendirildiğinde, mahkemenin ilgili bilgi talebi işleminin kaldırılmasının adaletin tecellisi için gerekli olduğuna kanaat getirmesidir.

Bilgi talebine itirazı değerlendiren mahkemenin, adaletin tecellisi için gerekli olan durumu değerlendirmesi için SCA 2703(h)/3'te belirtilen kriterleri dikkate alarak bir milletlerarası nezaket (**comity**) analizi yapması gerekmektedir<sup>592</sup>. Anılan maddede bu konuda, durumun şartlarına uygun düştüğü ölçüde dikkate alınması gereken kriterler listelenmiştir. Bu kriterler (bilgi talebinde bulunan devlet biriminin soruşturma yapmadaki menfaati de dahil olmak üzere) ABD'nin menfaati<sup>593</sup>, yeterli yabancı devletin bilgi paylaşımını engellemekteki menfaati<sup>594</sup>, hizmet sağlayıcının ya da onun çalışanlarının tabi oldukları çatışan hukuki yükümlülükler nedeniyle yaptırıma uğrama olasılıkları ile bu yaptırımların içeriği ve kapsamı<sup>595</sup>, bilgi talebine konu olan kişinin bulunduğu yer ve vatandaşlığı, eğer biliniyorsa bu kişinin ABD ile bağı, eğer ilgili bilgi talebi yabancı bir devlet adına yapılıyorsa bilgi talebine konu kişinin bu yabancı devlet ile bağı<sup>596</sup>, hizmet sağlayıcının ABD ile bağı ve ABD'deki varlığı<sup>597</sup>, bilgi talebine sebep olan soruşturmanın önemi<sup>598</sup>, talep edilen bilgilere daha erken ve verimli erişmeyi sağlayabilecek ve daha az olumsuz sonuç doğuran imkânların varlığı<sup>599</sup> ile eğer ilgili bilgi talebi yabancı bir devlet adına yapılıyorsa bu devletin soruşturma yapmadaki menfaatidir<sup>600</sup>.

---

<sup>592</sup> Schwartz, "Legal Access To The Global Cloud", s. 1716; Miranda Rutherford, "The CLOUD Act: Creating Executive Branch Monopoly Over Cross-Border Data Access", 2019, s. 72-73, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3508942](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3508942), 15.03.2020; Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 7; Mulligan, "Cross-Border Data Sharing Under the CLOUD Act", s. 9-10; Blackman, Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", s. 5; Cantekin, "Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?", s. 81-82.

<sup>593</sup> Bkz. SCA m. 2703(h)/3-A.

<sup>594</sup> Bkz. SCA m. 2703(h)/3-B.

<sup>595</sup> Bkz. SCA m. 2703(h)/3-C. Ayrıca bkz. Cantekin, "Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?", s. 88.

<sup>596</sup> Bkz. SCA m. 2703(h)/3-D.

<sup>597</sup> Bkz. SCA m. 2703(h)/3-E.

<sup>598</sup> Bkz. SCA m. 2703(h)/3-F.

<sup>599</sup> Bkz. SCA m. 2703(h)/3-G.

<sup>600</sup> Bkz. SCA m. 2703(h)/3-H.

Anılan kriterler incelendiğinde ilk olarak bilgiyi talep eden devlet ile bilginin bulunduğu yerdeki devletin menfaatlerinin göz önünde bulundurulduğu görülmektedir. Ayrıca hizmet sağlayıcıların karşılaşılabileceği yaptırımlar da değerlendirmeye alınmaktadır. Son olarak bilgileri talep edilen kişinin ABD ile bağlantısı da göz önünde bulundurulmaktadır. Kanaatimizce tüm bu kriterler, bilgi talebinin karşılanması sırasında hem kamu menfaatlerinin hem de gerçek ve tüzel kişilerinin menfaatlerinin korunmasına imkân vermektedir. Özellikle ABD merkezli teknoloji şirketlerinin tüm dünyada çok yüksek gelirler elde ettiği düşünüldüğünde bu şekilde bir yaklaşımın yerinde olduğu düşünülmektedir.

SCA 2703(h)/2-B içerisinde belirtilen üç sebebin birlikte varlığının aranması kanaatimizce dikkate değer bir yaklaşımdır. Örneğin bilgi talebinin yerine getirilmesinin, bilginin bulunduğu yeterli yabancı devlet hukukunu ihlal etmesi; tek başına bilgi talebi işleminin kaldırılması için yeterli değildir. Tersinden bakıldığında ise eğer bilginin bulunduğu yeterli yabancı devlet hukuku, bilginin talebinin yerine getirilmesini engellemiyorsa bu durumda ilgili bilgi paylaşım talebinin yerine getirilmesi bir zorunluluk olmaktadır. Eğer bilgi talebine konu kişi bir ABD kişisi değilse ve buna rağmen yeterli yabancı devlet hukuku bilgi talebinin yerine getirilmesini engellemiyorsa yine bilgi talebine uyulması zorunlu olmaktadır. Yeterli yabancı devlet hukuku bu kişinin bilgilerinin paylaşımını engellese dahi bu sefer de yukarıda belirtilen kriterlere göre bir analiz yapılacak ve bunun sonucuna göre bilgi talebi işleminin akıbeti belirlenecektir. Kanaatimizce bir bilgi talebi işleminin kaldırılması ya da değiştirilmesi, aranan koşullar nedeniyle son derece zor olacaktır.

SCA'nın belirlediği itiraz mekanizmasının sadece içerikler için olduğu, itiraz hakkının sadece hizmet sağlayıcılara tanındığı ve itirazın kabulü için gerekli koşulların yerine getirilmesinin son derece zor olduğu göz önüne alındığında, kanaatimizce SCA'nın meydana gelen hukukların çatışması sorununu ortadan kaldırma konusunda etkin bir yol olduğunu kabul etmek mümkün değildir. Bunun ötesinde SCA'nın sınır ötesi uygulama kapsamının da son derece geniş olduğunu da kabul etmek gerekmektedir. Zira içeriğe ilişkin bilgi talebine konu kişinin bir ABD kişisi olmaması, bilgi talebi işleminin kaldırılması için tek başına yeterli bir sebep değildir. Bilgi talebi eğer içeriğe

ilişkin değilse de bilgi talebi işlemi için hukukların çatışması sorununa dair bir itiraz imkânı olmaksızın uygulanmaktadır. Bu tür taleplerde ilgili talebine konu kişinin bir ABD kişisi olmaması ya da ilgili bilgi talebinin bilginin bulunduğu yeterli yabancı devlet hukukunu ihlal etmesi dikkate alınmamaktadır.

## **ii. SCA Kapsamında Uluslararası Adli İstinabe Sözleşmesi İmzalamayan Devletlere İlişkin Hukukların Çatışması Sorunlarının Çözümü**

Yeterli yabancı devlet statüsüne sahip olmayan devletler için SCA 2703(h) içerisindeki hukukların çatışması sorunlarının çözümüne yönelik itiraz imkânı kullanılamamaktadır. Aynı şekilde söz konusu itiraz imkânı sadece içerik bilgilerine ilişkin olduğu için içerik dışındaki bilgi kategorileri hakkında da uygulanamamaktadır. Her iki halde de doğabilecek hukukların çatışması sorunlarının nasıl çözümleneceği konusunu netleştirmek amacıyla CLOUD Act ile SCA içerisine bir açıklayıcı madde eklenmiştir. Bu maddeye göre CLOUD Act'in getirdiği hiçbir hüküm, müşterek hukukun hukukların çatışması sorunlarının çözümlenmesine yönelik milletlerarası nezaket analizi veya diğer kurallarının uygulanmasını etkilemeyecektir. Dolayısıyla SCA'nın sınır ötesi uygulama kapsamı nedeniyle yeterli yabancı devlet statüsüne sahip olmayan ülke hukukları ile doğan hukukların çatışması sorunları, müşterek hukukun belirlediği milletlerarası nezaket esasları çerçevesinde çözümlenecektir.

Milletlerarası nezaket kuralları, 1648 yılında Vestfalya Anlaşması'nın imzalanması ile<sup>601</sup> devletlerin kendi sınırları içerisinde mutlak egemenliğe sahip olduklarının kabulünden sonra ortaya çıkmıştır<sup>602</sup>. Hollandalı hukukçu **Ulrich Huber**, bir devlet sınırları içerisindeki hakların diğer devlette nasıl korunacağı sorununun çözümünü milletlerarası nezaket kuralları ile sağlamaya çalışmıştır<sup>603</sup>. Huber'in görüşleri İngiltere'nin müşterek hukuk sistemine girmiş ve buradan da ABD'nin müşterek

---

<sup>601</sup> De Souza Abreu, "Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience", s. 241; The Editors of Encyclopaedia, "Peace of Westphalia", **Encyclopedia Britannica**, 17.10.2022, (Çevrimiçi) <https://www.britannica.com/event/Peace-of-Westphalia>, 15.11.2022.

<sup>602</sup> Thomas Schultz, Niccolo Ridi, "Comity in US Courts", **Northeastern University Law Review**, C. 10, No: 1, 2018, s. 290-291.

<sup>603</sup> Detaylı bilgi için bkz. Thomas Schultz, Niccolo Ridi, "Comity in US Courts", **Northeastern University Law Review**, C. 10, S. 1, 2018, s. 293-296; Childress III, "Comity as Conflict: Resituating International Comity as Conflict of Laws", s. 21.

hukukuna geçmiştir<sup>604</sup>. ABD’li hâkim **Joseph Story**, milletlerarası nezaket kurallarını sistematik olarak ifade etmiş ve sınırlarını çizmiştir<sup>605</sup>. Story’nin bu çalışması, sonraki dönemlerde ABD hukukunun milletlerarası nezaket kuralları uygulamasına ışık tutmuştur<sup>606</sup>. Günümüze kadar gelen dönemde ABD mahkemelerinin milletlerarası nezakete ilişkin birçok kararı olduğu görülmektedir.

Milletlerarası nezaket kuralları, ABD hukuku çerçevesinde uygulanacak hukukun tespiti, kanunların bölgesel uygulama sınırlarının belirlenmesi, yabancı mahkeme kararlarının tanınması ve tenfizi, yabancı devletlerin yargı bağımsızlığı ve adli istinabe gibi birçok konunun hukuki kaynağını oluşturmaktadır. Buna karşın milletlerarası nezaketin net bir tanımı bulunmamaktadır. Net bir tanım bulunmaması uygulamada bir taraftan belirsizlik yaratmakta diğer taraftan da gerekli esnekliği sağlamaktadır<sup>607</sup>. ABD Yüksek Mahkemesi tarafından verilen tanım fikir vermesi açısından aşağıda paylaşılmaktadır<sup>608</sup>.

*“Hukuki anlamda milletlerarası nezaket, üçüncü bir tarafa karşı ne bir mutlak yükümlülüktür ne de sadece kibarlık ya da iyi niyet göstergesidir. Bunlar yerine milletlerarası nezaket, diğer bir devletin yürütme, yasama ya da yargı organlarının işlemlerinin diğer devlet ülkesi içerisinde tanınmasıdır. Söz konusu tanıma, tanıyan devletin milletlerarası görevleri ve çıkarları ile kendi vatandaşlarının ve koruması altında bulunan kişilerin haklarını gözetmelidir.”*

Milletlerarası nezaket kurallarının bir diğer niteliği ise bunların iç hukuka ilişkin olmalarıdır. Yani milletlerarası nezaket kuralları, uluslararası hukuktan doğan yükümlülükler değildir. Öte yandan hem milletlerarası nezaket kuralları hem de milletlerarası hukuk kuralları, ABD’nin yabancı devletlerle olan ilişkilerini düzenlemektedir. Ancak milletlerarası hukuk kuralları bağlayıcılığa sahipken milletlerarası nezaket kurallarının bağlayıcılığı bulunmamaktadır.

<sup>604</sup> Childress III, “Comity as Conflict: Resituating International Comity as Conflict of Laws”, s. 22.

<sup>605</sup> Childress III, **a.g.e.**, s. 23-24.

<sup>606</sup> Childress III, **a.g.e.**, s. 23-30; Schultz, Ridi, “Comity in US Courts”, s. 284.

<sup>607</sup> Milletlerarası nezaket kurallarının net bir tanımı olmamasından ve doğasından kaynaklanan çeşitli görüşler hakkında bilgi için bkz. Childress III, “Comity as Conflict: Resituating International Comity as Conflict of Laws”, s. 13-17.

<sup>608</sup> Hilton v. Guyot, 159 U.S. 113 (1895), C. 159, C. 159 U.S. Reports 113, (U.S. Supreme Court 1895); Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 5-6; Schultz, Ridi, “Comity in US Courts”, s. 286; Woods, “Litigating Data Sovereignty”, s. 373.

Yukarıda detaylı olarak açıklandığı üzere SCA'nın sınır ötesi uygulama kapsamı bulunmaktadır. Dolayısıyla SCA kapsamında yabancı ülkede bulunan bir bilginin talep edilmesi halinde, söz konusu talebin yerine getirilmesi, ilgili yabancı ülke hukukunu ihlal ediyorsa bu durumda hangi ülke hukukunun uygulanacağı sorunu yani bir hukukların çatışması sorunu doğmaktadır. Bu sorunun çözümü için müşterek hukuk, milletlerarası nezaket kapsamında menfaat analizi yapılmasını öngörmektedir<sup>609</sup>. Söz konusu analizin neticesine göre hangi ülke hukukunun uygulanması makul kabul edilebiliyorsa, o ülkenin hukukunun uygulanmasına karar verilecektir.

Menfaat analizi çerçevesinde değerlendirilmesi gereken ilk konu, ilgili fiilin hukuki yükümlülüğü getiren devletin ülkesi ile olan bağıdır<sup>610</sup>. Bu bağın varlığı, fiilin ülke topraklarında gerçekleşmesi ya da ülke topraklarında esaslı, doğrudan ve öngörülebilir bir etki doğurması hususlarına göre değerlendirilmektedir. İkinci konu hukuki yükümlülüğü getiren devlet ile fiille ilişkili kişi arasında vatandaşlık, yerleşim yeri ya da ekonomik faaliyet gibi bağlantılardır<sup>611</sup>. Bu kapsamda hukuki yükümlülüğü getiren devlet ile hukuki yükümlülüğün korumayı amaçladığı kişiler arasındaki bağ da değerlendirmeye alınmaktadır. Üçüncü konu, hukuki yükümlülüğe konu fiilin niteliği, hukuki yükümlülüğü getiren devletin yükümlülüğe verdiği önem, diğer devletlerin aynı konuda getirdiği hukuki yükümlülüğün kapsamı ile söz konusu yükümlülüğün getirilmesinin genel olarak kabul edilebilir olup olmamasıdır<sup>612</sup>. Dördüncü konu ilgili hukuki yükümlülüğün korunması ya da zarar görmesi beklenen makul beklentiler olup olmadığıdır<sup>613</sup>. Beşinci konu, ilgili hukuki yükümlülüğün uluslararası siyasi, hukuki ya da ekonomik sistemlerdeki önemidir<sup>614</sup>. Altıncı konu, ilgili hukuki yükümlülüğün

---

<sup>609</sup> Hixson, "Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States", s. 135; Schwartz, Peifer, "Data Localization Under the CLOUD Act and the GDPR", s. 6; Michael M. Baylson, Sandra A. Jeskie, "Overseas Obligations: An Update on Cross-Border Discovery", *Judicature*, C. 103, S. 1, 2019, s. 57; Woods, "Litigating Data Sovereignty", s. 380; Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", s. 1936.

<sup>610</sup> *Restatement Third*, C. 1, s. 244.

<sup>611</sup> *a.g.e.*, C. 1, s. 244.

<sup>612</sup> *a.g.e.*, C. 1, s. 245.

<sup>613</sup> *a.g.e.*, C. 1, s. 244.

<sup>614</sup> *a.g.e.*, C. 1, s. 244.

uluslararası sistemin gelenekleri ile uyumlu olup olmadığıdır<sup>615</sup>. Yedinci konu başka bir devletin ilgili fiili hukuki düzenlemelere konu etmekteki menfaatidir<sup>616</sup>. Sekizinci konu ise başka bir devletin hukuki düzenlemelerinin de ilgili hukuki düzenleme ile çatışması olasılığıdır<sup>617</sup>.

SCA kapsamında yeterli yabancı devlet statüsünde olmayan bir devletin hukuku ile hukukların çatışması sorunu doğduğunda, yukarıda verilen kriterler çerçevesinde ilgili ABD mahkemesi tarafından bir değerlendirme yapılacak ve bunun sonucunda hangi ülke hukukuna öncelik verileceği tespit edilecektir. Önemle belirtmek gerekir ki müşterek hukukun milletlerarası nezaket çerçevesinde öngördüğü menfaat analizi çözümü, SCA'dan çok daha eskidir. Buna rağmen uygulamada hiçbir hizmet sağlayıcının bilgi talepleri konusunda hukukların çatışması doğduğuna dair bir itirazı olmamıştır. Böyle bir itirazın özellikle CLOUD Act'in yürürlüğe konmasına sebep olan **Microsoft** ve **Google**'a ilişkin yargılama süreçlerinde de bulunmadığını vurgulamakta fayda görülmektedir.

#### **f. SCA Kapsamında İmzalanabilecek Uluslararası Adli İstinabe Sözleşmeleri**

CLOUD Act'in yeniliklerinden birisi de ABD Hükümeti'ne yabancı devletlerle adli istinabe sözleşmesi imzalama yetkisi vermesidir<sup>618</sup>. Bu sözleşmelerin temel amacı, yabancı devletlerle karşılıklı olarak dijital ortamda bulunan delillere erişimi kolaylaştırmaktır<sup>619</sup>. Ancak getirilen kanuni düzenleme, ABD Hükümeti'ni sadece belirli şartları taşıyan yabancı devletlerle bu sözleşmeleri imzalamaya yetkili kılmaktadır. Aşağıda öncelikle bu şartlar üzerinde durulacaktır. Daha sonra ise ABD ve Birleşik Krallık arasında imzalanmış uluslararası adli istinabe sözleşmesi incelenecektir.

---

<sup>615</sup> a.g.e., C. 1, s. 244.

<sup>616</sup> a.g.e., C. 1, s. 244.

<sup>617</sup> a.g.e., C. 1, s. 244.

<sup>618</sup> Baylson, Jeskie, "Overseas Obligations: An Update on Cross-Border Discovery", s. 55-56.

<sup>619</sup> Rojszczak, "CLOUD act agreements from an EU perspective", s. 5; Mulligan, "Cross-Border Data Sharing Under the CLOUD Act", s. 11.

Üzerinde durulması gereken bir diğer husus da CLOUD Act çerçevesinde imzalanacak adli istinabe sözleşmelerinin mevcutta yürürlükte bulunan adli yardımlaşma sözleşmelerinin yerine geçmediği ya da onları değiştirmedir. Yani eğer bir adli yardım talebi gerekli şartları taşıyorsa CLOUD Act çerçevesinde imzalanan adli yardımlaşma sözleşmesi kapsamında, eğer bu şartları taşımıyorsa mevcut adli yardımlaşma sözleşmesi kapsamında yerine getirilecektir.

CLOUD Act çerçevesinde imzalanacak adli istinabe sözleşmelerin imzalanabilme şartları ile CLOUD Act kapsamında ABD ve Birleşik Krallık arasında imzalanan anlaşma sonraki başlıklar altında incelenmektedir.

### **(1) Uluslararası Adli İstinabe Sözleşmesi İmzalanabilmesine Dair CLOUD Act'in Getirdiği Şartlar**

CLOUD Act, yabancı devletlerle yapılacak dijital ortamdaki bilgilere yargı faaliyetleri çerçevesinde erişilmesine ilişkin adli istinabe sözleşmelerine dair maddeleri, U.S. Code'un<sup>620</sup> 2523 numaralı bölümü altına eklemiştir<sup>621</sup>. Söz konusu bölüm altında hem bu sözleşmelerin imzalanabileceği yabancı devletlerde bulunması gereken şartlar hem de sözleşmelerin yürürlüğe konması için gereken onay prosedürleri açıklanmıştır. İşbu çalışmanın kapsamı gereği sadece adli istinabe sözleşmeleri imzalayabilecek yabancı devletlerin taşıması gereken şartlar incelenecektir.

Yabancı devletlerin, ABD ile dijital ortamdaki bilgilere erişim amacıyla adli istinabe sözleşmesi imzalamaları için temel olarak dört adet koşulun varlığı gerekmektedir<sup>622</sup>. Aşağıdaki başlıklar altında bu dört koşul üzerinde durulacak ve bu koşullar altında düzenlenen ek şartlar incelenecektir.

---

<sup>620</sup> Birleşik Devletler Kanunu, orijinal adı ile *U.S. Code*, Birleşik Devletler'in genel ve daimî kanunlarının konularına göre birleştirilmesi ve kodlanmasından oluşmaktadır. Birleşik Devlet Kanunu hakkında detaylı bilgi için bkz. <https://uscode.house.gov>.

<sup>621</sup> Bkz. 18 U.S. Code m. 2523. Ayrıca bkz. Cole, Quintel Teresa, "Transborder Access to e-Evidence by Law Enforcement Agencies", s. 10; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 91-92; Mulligan, "Cross-Border Data Sharing Under the CLOUD Act", s. 14-16; Blackman, Gerber, "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", s. 3.

<sup>622</sup> Bkz. 18 U.S. Code m. 2523(b). Ayrıca bkz. Kyriakides, "The CLOUD Act, E-Evidence, and Individual Rights", s. 101-102; Mulligan, "Cross-Border Data Sharing Under the CLOUD Act", s. 16-17.

Bunlardan ilki, ilgili yabancı devletin iç hukukunun özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması konusunda usul ve esas açısından güçlü korumalar sağlamasıdır. İkincisi, adli istinabe sözleşmesine konu olan ABD kişilerine dair bilgilerin alınması, saklanması ve paylaşılmasının asgari düzeye indirilmesi için ilgili yabancı devletin gerekli prosedürleri oluşturmalarıdır. Üçüncü koşul, imzalanacak adli istinabe sözleşmesinin, hizmet sağlayıcıların verileri şifrelememesi ya da şifreli verilerin çözülmesini gerektirecek hukuki kurallar içermemesidir. Son koşul ise imzalanacak adli istinabe sözleşmesinin bazı düzenlemeleri ve kısıtlamaları içermesidir.

#### **i. Özel Hayatın Gizliliği ile Temel Hak ve Özgürlüklerin Korunması**

CLOUD Act'in getirdiği ilk şart ilgili yabancı devletin iç hukukunun özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması konusunda usul ve esas açısından güçlü korumalar sağlamasıdır<sup>623</sup>. Bahsi geçen güçlü korumaların nasıl sağlandığının tespiti konusunda da çeşitli kriterler belirlenmiş durumdadır. Bunlardan ilki değerlendirmeye dayanak alınan bilgilerin güvenilir kaynaklardan ve uzmanlardan gelmiş olmasıdır<sup>624</sup>. Birleşik Krallık'a ilişkin değerlendirme raporunda, temel alınan esas kaynağın ABD tarafından her yıl yayınlanan İnsan Hakları Uygulamalarına İlişkin Ülke Raporları olduğu görülmektedir<sup>625</sup>. Ayrıca açıkça belirtilmiş olmasa da değerlendirmeye konu ülkenin iç hukuk kuralları ile taraf olduğu uluslararası anlaşmalar da büyük önem arz etmektedir. Zira Birleşik Krallık'a ilişkin değerlendirme raporunda da bu husus açıkça görülebilmektedir<sup>626</sup>.

---

<sup>623</sup> Bkz. 18 U.S. Code m. 2523(b)-1. Ayrıca bkz. Kyriakides, "The CLOUD Act, E-Evidence, and Individual Rights", s. 104.

<sup>624</sup> Bkz. 18 U.S. Code m. 2523(b)-1/A.

<sup>625</sup> ABD tarafından yayınlanan rapor için bkz. "Country Reports on Human Rights Practices", 12.04.2022, (Çevrimiçi) <https://www.state.gov/reports-bureau-of-democracy-human-rights-and-labor/country-reports-on-human-rights-practices/>, 10.05.2022.

<sup>626</sup> "2021 Country Reports on Human Rights Practices: United Kingdom", U.S. Department of State, 12.04.2022, (Çevrimiçi) <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/united-kingdom/>, 05.10.2022.



Gerekli kořullardan birisi de siber suçlara ve elektronik delillere ilişkin esasa ve usule dair yeterli hukuk kurallarının bulunmasıdır<sup>627</sup>. Bu kořulun saęlanması, 23 Kasım 2001 tarihinde imzalanan ve 7 Ocak 2004 tarihinde yürürlüęe giren Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne<sup>628</sup> (dięer adıyla Budapeřte Konvansiyonu) taraf olunması ya da bu sözleşmedeki tanım ve gerekliliklere uygun iç hukuk kurallarına sahip olunmasına baęlıdır. Birleşik Krallık, Budapeřte Konvansiyonu'na taraf olduęu için raporda yeterli olarak kabul edilmiştir<sup>629</sup>.

Hukukun üstünlüęü ve ayrımcılık yasaęı prensiplerine uygun davranılması<sup>630</sup> aranan kořullardan bir dięerini teşkil etmektedir.<sup>631</sup> Bunun yanında başta özel hayatın gizlilięinin keyfi ve hukuka aykırı müdahalelerden korunması, adil yargılanma hakkı, ifade özgürlüęü, dernek kurma hakkı, toplantı ve gösteri yürüyüşü yapma hakkı, keyfi tutuklama ya da alıkoyma yasaęı, işkence ve eziyet yasaęı ile insan haysiyeti ile bağdaşmayan ceza ya da muamele yasaęı olmak üzere uluslararası insan hakları yükümlölükleri ve taahhütlerine baęlılık ya da evrensel insan haklarına saygının gösterilmesi aranmaktadır<sup>632</sup>.

Bir dięer kořul da ilgili yabancı devlet içerisinde bilgi talebinde bulunabilecek yetkili makamların bu talepleri hakkında net hukuki kurallar ve usuller belirlenmiş olmasıdır<sup>633</sup>. Söz konusu kuralların özellikle bilgilerin toplanması, saklanması, kullanılması ve paylaşılmasına ilişkin düzenlemeler içermesi ile söz konusu düzenlemelerin uygulandıęına dair etkin bir denetim mekanizması kurması gerekmektedir. Birleşik Krallık'a dair raporda bu hususların ceza yargılamasına ilişkin

---

<sup>627</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(i). Ayrıca bkz. Rojszczak, "CLOUD act agreements from an EU perspective", s. 6; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 430; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 92; Kyriakides, "The CLOUD Act, E-Evidence, and Individual Rights", s. 102.

<sup>628</sup> "Convention No. 185 of the Council of Europe on Cybercrime (Budapest Convention)".

<sup>629</sup> Budapeřte Konvansiyonu'na taraf olan devletler hakkında bilgi için bkz. [www.coe.int/en/web/cybercrime/the-budapest-convention](http://www.coe.int/en/web/cybercrime/the-budapest-convention).

<sup>630</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(ii).

<sup>631</sup> Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 431.

<sup>632</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(iii).

<sup>633</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(iv).

usul mevzuatı ve kişisel verilerin korunmasına dair mevzuatlar çerçevesinde değerlendirildiği görülmektedir<sup>634</sup>.

Aranmakta olan koşullardan bir diğeri de ilgili yabancı devlet tarafından toplanan ve kullanılan elektronik verilere dair hesap verilebilirliği ve şeffaflığı sağlayacak yeterli mekanizmaların bulunmasıdır<sup>635</sup>. Birleşik Krallık’a dair raporda bu hususların ceza yargılamasına ilişkin usul mevzuatı ve kişisel verilerin korunmasına dair mevzuatlar çerçevesinde değerlendirildiği görülmektedir<sup>636</sup>.

Son olarak aranan koşul ise ilgili yabancı devletin global bilgi akışının serbestçe sağlanmasının teşvik edilmesi ile korunması görüşüne bağlı olduğunu göstermesidir<sup>637</sup>. Ayrıca ilgili yabancı devlet internetin açık, merkezi olmayan ve birbirine bağlı mevcut yapısının korunması ve teşvik edilmesi görüşüne bağlı olmalıdır<sup>638</sup>. Birleşik Krallık’a dair raporda bu hususun gerçekleştirildiği, Birleşik Krallık’ın interneti etkileyen bir mevzuatının olmaması, veri lokalizasyonu gerektiren bir mevzuata sahip olmaması ve diğer ülkelerin de bu mevzuatlara sahip olmasına karşı çıkması hususları ile tespit edilmiştir<sup>639</sup>.

## **ii. Talebe Konu Verilerin Asgari Seviyede Kullanılması İçin Gerekli Prosedürlerin Oluşturulması**

CLOUD Act’in aradığı ikinci koşul, adli istinabe sözleşmesine konu olan ABD kişilerine dair bilgilerin alınması, saklanması ve paylaşılmasının asgari düzeye indirilmesi için ilgili yabancı devletin gerekli prosedürleri oluşturmasıdır<sup>640</sup>. Bu madde ile sözleşme çerçevesinde temin edilecek bilgilerin asgari seviyede kullanımı

---

<sup>634</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>635</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(v).

<sup>636</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>637</sup> Bkz. 18 U.S. Code m. 2523(b)-1/B-(vi).

<sup>638</sup> Cantekin, “Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?”, s. 88.

<sup>639</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>640</sup> Bkz. 18 U.S. Code m. 2523(b)-2. Ayrıca bkz. Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 92; Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 102; Peace, “Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation”, s. 431.

sağlanarak özel hayatın gizliliği hakkının zedelenmesi engellenmeye çalışılmıştır. Birleşik Krallık’a dair raporda bu hususlara dair ceza yargılamasına ilişkin mevzuat ve üzerinde mutabakata varılan adli istinabe sözleşmesi değerlendirilerek uyumluluk sağlandığı belirtilmiştir<sup>641</sup>.

### **iii. Şifrelemenin Kısıtlanmaması ya da Şifre Çözme Zorunluluğu Getirilememesi**

CLOUD Act’in aradığı üçüncü koşul, adli istinabe sözleşmesinin şifrelemeye ilişkin belirli hususlar hakkında hüküm içermemesidir<sup>642</sup>. Bu hükümlerden ilki, hizmet sağlayıcıların bilgi talebine konu verilerin şifresini çözme imkanına sahip olması zorunluluğunun getirilememesidir. İkincisi ise hizmet sağlayıcının talebe konu verilerin şifresini çözmesinin sınırlandırılmaması ya da yasaklanmamasıdır. Önemle belirtmek gerekir ki söz konusu sınırlamalar sadece imzalanacak adli istinabe sözleşmesinin içeriğine ilişkindir. İlgili yabancı devletin iç hukukunda söz konusu düzenlemeleri içeren herhangi bir hukuki düzenleme yapması önünde bir engel bulunmamaktadır. Birleşik Krallık’a dair raporda, üzerinde mutabakata varılan sözleşme metninin bu tür bir hüküm içermediği ifade edilmiştir<sup>643</sup>.

### **iv. Adli İstinabe Sözleşmesinin İçermesi Gereken Düzenleme ve Kısıtlamalar**

CLOUD Act’in aradığı son koşul ise imzalanacak adli istinabe sözleşmesinin bazı düzenlemeleri içermesidir. Bu düzenlemeler<sup>644</sup> imzalanacak adli istinabe sözleşmesinin amacına uygun şekilde kullanılması ile kapsam ve sınırlarının netleştirilmesine ilişkindir<sup>645</sup>.

---

<sup>641</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>642</sup> Bkz. 18 U.S. Code m. 2523(b)-3. Ayrıca bkz. Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 102; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 93.

<sup>643</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>644</sup> Bkz. SCA m.2523(b)-4.

<sup>645</sup> Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 102; Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 18; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 93; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1094; Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 337.

Sözleşme içeriğinde bulunması gereken ilk düzenleme, ilgili yabancı devletin ABD kişilerinin ya da ABD’de bulunan kişilerin bilgilerini, ilgili adli istinabe sözleşmesi çerçevesinde talep edemeyeceğidir<sup>646</sup>. Benzer şekilde ilgili yabancı devlet, bir ABD kişisine ya da ABD’de bulunan bir kişiye dair bilgi edinmek amacıyla ABD kişisi olmayan ve ABD’de bulunmayan bir kişinin bilgilerini bahse konu adli istinabe sözleşmesi çerçevesinde talep edemeyecektir<sup>647</sup>.

İlgili yabancı devlet, başka bir devlete ya da ABD Hükümetine bilgi vermek amacıyla adli yardım sözleşmesi çerçevesinde bilgi talebinde bulunmayacaktır<sup>648</sup>. Aynı şekilde ilgili yabancı devletin adli istinabe sözleşmesi çerçevesinde elde ettiği bilgileri ABD Hükümetine ya da başka bir devlete aktarması şartı da getirilemeyecektir<sup>649</sup>. Bu düzenlemeler, ilgili adli istinabe sözleşmesi vasıtasıyla ABD’nin iç hukukunun dolaşılmasını engellemek adına getirilmiştir.

İlgili yabancı devletin bir ABD kişinin iletişim içeriğine ulaşması halinde bu iletişimin ABD kurumlarıyla paylaşılmaması da bir ana kural olarak belirlenmiştir<sup>650</sup>. Bu kuralın istisnası ABD’ye ya da ABD kişilerine karşı ciddi bir zarara ya da tehdide ilişkin bilgilere ulaşılmış olmasıdır. Söz konusu durumlara örnek olarak<sup>651</sup> terörizm gibi ulusal güvenliğe ilişkin suçlar, önemli derecede şiddet içeren suçlar, çocuk istismarı, uluslararası organize suçlar ya büyük çaplı finansal dolandırıcılık verilmiştir<sup>652</sup>.

---

<sup>646</sup> Bkz. SCA m. 2523(b)-4/A.

<sup>647</sup> Bkz. 18 U.S. Code m. 2523(b)-4/B. Ayrıca bkz. Maillart, “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, s. 387.

<sup>648</sup> Bkz. 18 U.S. Code m. 2523(b)-4/C. Detaylı bilgi için bkz. Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 18.

<sup>649</sup> Bkz. 18 U.S. Code m. 2523(b)-4/C.

<sup>650</sup> Bkz. 18 U.S. Code m. 2523(b)-4/H. Ayrıca bkz. Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 338.

<sup>651</sup> Bkz. 18 U.S. Code m. 2523(b)-4/H.

<sup>652</sup> Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 93; Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 18; Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 102.

Yabancı devletler tarafından düzenlenen bilgi paylaşımı emirlerinin içeriği konusunda da CLOUD Act belirli şartlar aramaktadır<sup>653</sup>. Bunlardan ilki bilgi talebinin sadece terörizm dahil ciddi suçların soruşturulmasına ya da kovuşturulmasına ilişkin<sup>654</sup> olmasıdır<sup>655</sup>. Ek olarak bilgi talebi belirli bir kişiye, kullanıcı hesabına, adrese, kişisel cihaza ya da başka şekilde özel olarak ayrıştırılmış bir objeye ilişkin olmalıdır<sup>656</sup>.

İmzalanacak adli istinabe sözleşmesi çerçevesinde yapılan bilgi taleplerinin, aynı zamanda ilgili yabancı devletin iç hukukuna uygun olması gerekmektedir<sup>657</sup>. Bu kapsamda hizmet sağlayıcıların bu bilgi talebine yanıt verme konusundaki zorunlulukları, sadece ilgili yabancı devletin iç hukukuna göre belirlenecek bir husus olarak kabul edilmiştir<sup>658</sup>. Bir başka deyişle, adli istinabe sözleşmesi bilgi paylaşımı yükümlülüğü doğurmamakta, sadece yabancı devletin iç hukukuna göre verilen bilgi talebi kararının yerine getirilmesine imkân vermektedir.

Adli istinabe sözleşmesi kapsamında<sup>659</sup> işleme alınabilecek bilgi talebi kararının kolayca anlaşılabilir ve güvenilir olgulara dayalı, hukuki, soruşturulan konuyla ilgili ve bağlantılı bir gerekçeye dayanıyor olması gerekmektedir<sup>660</sup>. Ayrıca kararın ya mahkeme, hâkim veya bağımsız otorite gibi tarafsız bir makam tarafından, kararın infazından önce verilmesi ya da en geç kararın infazı sırasında incelenmesi<sup>661</sup> de aranmaktadır<sup>662</sup>.

---

<sup>653</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D.

<sup>654</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(i).

<sup>655</sup> Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 3; Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, s. 341.

<sup>656</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(ii)

<sup>657</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(iii). Ayrıca bkz. Maillart, “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, s. 387.

<sup>658</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(iii).

<sup>659</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(iv).

<sup>660</sup> Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 4.

<sup>661</sup> Bkz. 18 U.S. Code m. 2523(b)-4/D-(v).

<sup>662</sup> Cook, “Cross-Border Data Access and Active CyberDefense: Assessing Legislative Options for a New International Cybersecurity Rulebook”, s. 229-230; Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 105; Schwartz, Peifer, “Data Localization Under the CLOUD Act and the GDPR”, s. 4.

Yabancı devletin bilgi talebi kararının imzalanacak adli istinabe sözleşmesi çerçevesinde<sup>663</sup> işleme alınabilmesi için bu kararın ifade özgürlüğünü ihlal etmemesi gerekmektedir<sup>664</sup>.

Adli istinabe sözleşmesi çerçevesinde elde edilen bilgilerinin gecikmeksizin incelenmesi ve incelenmeyen bilgilerin de sadece güvenli bir sistemde, sadece yetkili kişilerce erişilebilecek şekilde saklanması gerekmektedir<sup>665</sup>. Bu bilgilerin incelenmesinden sonra da bilgilerin asgari ölçüde kullanılmasını sağlamak adına gerekli önlemler alınmalı ve özellikle ilgisiz kısımlar silinmelidir<sup>666</sup>.

Yabancı devletlere getirilen bir diğer yükümlülük<sup>667</sup> de kendi iç hukuklarında hizmet sağlayıcıların ABD makamlarına bilgi vermesini engelleyecek düzenlemeleri kaldırmaları ve bu yolla karşılıklılık ilkesine uygun davranmalarıdır<sup>668</sup>. Ek olarak yabancı devletler, ABD Hükümeti tarafından belirli dönemlerle ilgili adli istinabe sözleşmesine uygun davranıp davranmadıklarına dair denetlenmeyi de kabul etmelidirler<sup>669</sup>. ABD Hükümeti tarafından ilgili yabancı devletin adli istinabe sözleşmesine uygun hareket etmediği tespit edilirse bu sözleşmenin ABD hükümeti tarafından tek taraflı beyanla uygulanamaz hale getirilebileceği de ilgili yabancı devletçe uygun bulunmalıdır<sup>670</sup>.

---

<sup>663</sup> Bkz. 18 U.S. Code m. 2523(b)-4/E.

<sup>664</sup> Maillart, “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, s. 387; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 93; Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 18.

<sup>665</sup> Bkz. 18 U.S. Code m. 2523(b)-4/F. Ayrıca bkz. Daskal, “Privacy and Security Across Borders”, s. 1038.

<sup>666</sup> Bkz. 18 U.S. Code m. 2523(b)-4/G.

<sup>667</sup> Bkz. 18 U.S. Code m. 2523(b)-4/I.

<sup>668</sup> Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 93.

<sup>669</sup> Bkz. 18 U.S. Code m. 2523(b)-4/J. Ayrıca bkz. Kyriakides, “The CLOUD Act, E-Evidence, and Individual Rights”, s. 102; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 94; Daskal, “Privacy and Security Across Borders”, s. 1038.

<sup>670</sup> Bkz. 18 U.S. Code m. 2523(b)-4/K. Ayrıca bkz. Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 94.

Birleşik Krallık’a dair değerlendirme raporunda<sup>671</sup> yukarıda sayılan tüm koşulların gerek üzerinde mutabık kalınan sözleşme ile gerekse Birleşik Krallık iç hukukuna göre yerine getirildiği tespit edilmiştir<sup>672</sup>.

## (2) ABD ile Birleşik Krallık Arasında İmzalanan Uluslararası Adli İstinabe Sözleşmesinin İncelenmesi

### i. Sözleşmenin Amaç, Kapsam ve Uygulanma Hükümleri

ABD ile Birleşik Krallık arasında<sup>673</sup> 3 Ekim 2019 tarihinde CLOUD Act ile öngörülen şekilde bir adli istinabe sözleşmesi imzalanmıştır<sup>674</sup>. Bu sözleşme 3 Ekim 2022 tarihinde yürürlüğe girmiştir<sup>675</sup>. Söz konusu adli istinabe sözleşmesinin CLOUD

<sup>671</sup> “2021 Country Reports on Human Rights Practices: United Kingdom”.

<sup>672</sup> Adli istinabe sözleşmelerinin uygunluğuna ilişkin bilgi için bkz. Mulligan, “Cross-Border Data Sharing Under the CLOUD Act”, s. 20.

<sup>673</sup> Ayrıca ABD ile Avustralya arasında da benzeri bir sözleşme imzalanmıştır (bkz. <https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime>). ABD ile AB arasında da benzer bir adli istinabe sözleşmesinin müzakereleri yürütülmektedir (bkz. <https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations>). Kanada ile ABD arasında da aynı konuda müzakereler sürdürülmektedir (bkz. <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>). ABD ile yapılan adli istinabe sözleşmelerine ilişkin güncel bilgi için bkz. <https://www.justice.gov/criminal-oia/cloud-act-resources>. Ayrıca bkz. Cochrane, “Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers”, s. 159; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 419; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 96; Rojszczak, “CLOUD act agreements from an EU perspective”, s. 8-9; “Joint US-EU Statement on Electronic Evidence Sharing Negotiations”, **The United States Department of Justice**, 26.09.2019, (Çevrimiçi) <https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations>, 10.10.2021; “Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton”, **The United States Department of Justice**, 07.10.2019, (Çevrimiçi) <https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us>, 10.10.2021.

<sup>674</sup> Özgün adı ile *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (bundan sonra “UK-US Agreement” olarak adlandırılacaktır.) denmektedir, bkz. <https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern>. Ayrıca bkz. Theodore Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”, **European Law Blog**, (17.10.2019), (Çevrimiçi) <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>, 15.04.2020; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 94; Cochrane, “Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers”, s. 163.

<sup>675</sup> “Joint Statement by the United States and the United Kingdom on Data Access Agreement”, **The United States Department of Justice**, 21.07.2022, (Çevrimiçi) <https://www.justice.gov/opa/pr/joint-statement-united-states-and-united-kingdom-data-access-agreement>, 08.09.2022.

Act'in getirdiği önceki bölümde açıklanan şartları sağladığı, ABD Adalet Bakanlığı tarafından tasdik edilmiştir<sup>676</sup>. Bu nedenle tekrara düşmemek adına önceki bölümde açıklanan şartlara, söz konusu sözleşme incelenirken tekrar değinilmeyecektir.

Adli istinabe sözleşmesinin amacı kamu güvenliğinin, özel hayatın gizliliği hakkının, temel hak ve özgürlüklerin ve açık internet yapısının korunması amacıyla ceza yargılamaları kapsamındaki bilgi taleplerinin yarattığı sorunların çözülmesi olarak belirlenmiştir<sup>677</sup>. Sözleşmenin başlangıç kısmında da tarafların veri lokalizasyonu kurallarının özgür, açık ve güvenli internet ortamına zararlarının taraflarca bilindiği ve bu tür hükümlerden kaçınılmaya çalışılacağı ifade edilmiştir. Kanaatimizce söz konusu ifadeler, adli istinabe anlaşmasının en önemli hedefinin mevcut internet yapısını korurken aynı zamanda mevcut yapının yarattığı sorunları çözmeye çalışmak olduğunu göstermektedir.

Adli istinabe sözleşmesinin kapsamının sınırları birçok açıdan çizilmiştir. Konu bakımından adli istinabe sözleşmesi sadece suçların önlenmesi, tespiti, soruşturulması ya da kovuşturulması amacıyla yapılan ve dijital ortama ilişkin bilgi taleplerini kapsamaktadır<sup>678</sup>. Öte yandan sözleşme kapsamına tüm suçlar girmemekte, sadece sözleşmede ciddi suç olarak tanımlanmış suçlar girmektedir. Söz konusu tanıma göre üst sınırı en az 3 yıl hapis cezası olan suçlar<sup>679</sup>, ciddi suç (**serious crime**) olarak kabul edilmektedir<sup>680</sup>. Son olarak belirtmek gerekir ki adli istinabe sözleşmesi m. 2/3/a

---

<sup>676</sup> Stephen E. Boyd, "Certification from U.S. Department of Justice - Office of Legislative Affairs to Senate Judiciary Committee and the Senate Foreign Relations Committee", 04.12.2019, (Çevrimiçi) <https://www.justice.gov/dag/page/file/1231381/download>, 06.06.2021; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1095.

<sup>677</sup> Bkz. UK-US Agreement m.2.

<sup>678</sup> Bkz. UK-US Agreement m.2/1. Ayrıca bkz. Rojszczak, "CLOUD act agreements from an EU perspective", s. 6; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 428.

<sup>679</sup> Bkz. UK-US Agreement m. 1/14.

<sup>680</sup> Jennifer Daskal, Peter Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards", **Lawfare**, (14.03.2020), (Çevrimiçi) <https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards>, 14.03.2020; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 95; "Groups Urge Congress to Oppose US-UK Cloud Act Agreement", **Human Rights Watch**, (29.10.2019), (Çevrimiçi) <https://www.hrw.org/news/2019/10/29/groups-urge-congress->



gereğince kapsama giren suçların uluslararası nitelikte ya da uluslararası etkiye sahip olması gerekmektedir<sup>681</sup>.

Adli istinabe sözleşmesinin kişi bakımından kapsamını iki farklı grup altında değerlendirmek gerekmektedir<sup>682</sup>. Bunlardan ilki bilgileri talep edilen kişiler; ikincisi ise bilgi taleplerinin muhatabı olabilecek hizmet sağlayıcılardır. Hizmet sağlayıcılar sözleşme içerisinde (SCA ile de uyumlu olarak) kamuya açık şekilde bilgisayar sistemleri ya da telekomünikasyon sistemleri vasıtasıyla iletişim veya veri işleme ya da depolama hizmeti veren kişiler olarak tanımlanmıştır. Söz konusu kişiler adına veri işleme ya da saklama hizmeti sunan kişiler de hizmet sağlayıcı tanımı kapsamına dahil edilmiştir. Ek olarak adli istinabe sözleşmesinin amacını düzenleyen 2 numaralı madde içerisinde de iletişim hizmeti sağlayan kişilerin aynı zamanda diğer tarafın hukukuna tabi olmaları gerektiği de belirtilmiştir<sup>683</sup>.

Bilgileri talep edilen kişiler bakımından adli istinabe sözleşmesinin kapsamı ciddi şekilde sınırlanmıştır. Sözleşme kapsamında alıcı taraf kişisi şeklinde bir tanım

---

oppose-us-uk-cloud-act-agreement, 14.03.2020; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1114; Peace, “Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation”, s. 428-429. Ayrıca belirtmek gerekir ki adli istinabe sözleşmesi m. 8/4 içerisinde ABD, Birleşik Krallık’ın ifade özgürlüğüne ilişkin kanunlarının; Birleşik Krallık da ABD’nin idam cezasına ilişkin kanunlarının kendi çıkarlarını ihlal ettiğini beyan etmiştir. Anılan madde çerçevesinde bahse konu hususlara ilişkin bilgi talepleri neticesinde elde edilen bilgilerin kullanılması, bilgi talebini alan devletin yetkili makamının onayına bağlanmıştır. Söz konusu durum, sözleşme kapsamına giren suçlar bakımından özel bir sınırlama teşkil etmektedir.

<sup>681</sup> Orijinal metindeki hali ile şu şekilde ifade edilmiştir: “3. *Interests relevant to this Agreement include, but are not limited to: (a) the prevention, detection, investigation, or prosecution of Serious Crime by each Party, whether or not the crimes are transnational in nature or impact. (...)*”.

<sup>682</sup> Bkz. UK-US Agreement m. 1/9 ve m. 1/13. Ayrıca bkz. Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1097-1098.

<sup>683</sup> Orijinal metindeki hali ile şu şekilde ifade edilmiştir: “*The purpose of this Agreement is to advance public safety and security, and to protect privacy, civil liberties, and an open Internet, by resolving potential conflicts of legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party. (...)*”. Ayrıca bkz. Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”.

yapılmıştır<sup>684</sup>. Bu terim ABD ve Birleşik Krallık açısından farklı şekilde tanımlanmıştır. ABD'nin tanımına göre söz konusu kişiler; devlet kurumları, vatandaşlar, kalıcı ikamet izni sahibi olanlar, çoğunluğu vatandaşlardan veya kalıcı ikamet iznine sahip kişilerden oluşan dernek, vakıf ya da kulüp ve benzeri kuruluşlar ile ABD'de kurulmuş şirketler ya da ABD sınırları içerisinde bulunanlardan oluşmaktadır. Birleşik Krallık tanımına göre söz konusu kişiler ise devlet kurumları, Birleşik Krallık'ta bulunan kişilerden oluşan dernek, vakıf ya da kulüp ve benzeri kuruluşlar, Birleşik Krallık'ta bulunan ya da kayıtlı şirketler ya da Birleşik Krallık'ta bulunan tüm kişilerden oluşmaktadır<sup>685</sup>.

Adli istinabe sözleşmesi çerçevesinde taraf devletlerin alıcı taraf kişileri hakkında bilgi talebinde bulunmaları yasaklanmıştır. Dolayısıyla adli istinabe sözleşmesi çerçevesinde bilgi talebine konu olabilecek kişilerin temel olarak sadece her ülkenin kendi sınırları içerisinde bulunan kişiler olduğunu söylemek mümkündür. Ancak ülkeler arasındaki tanım farkı nedeniyle<sup>686</sup> Birleşik Krallık tarafından bulundukları konum fark etmeksizin ABD vatandaşları ya da ABD'de kalıcı ikamet iznine sahip kişilerin bilgileri talep edilemeyecektir<sup>687</sup>. Örnek vermek gerekirse Birleşik Krallık'ın ABD sınırlarında bulunan bir Birleşik Krallık vatandaşı hakkında ya da Birleşik Krallık'ta bulunan bir ABD vatandaşı hakkında incelemeye konu adli istinabe sözleşmesi çerçevesinde bilgi talep etmesi mümkün değildir. Aynı şekilde ABD'nin de Birleşik Krallık sınırları içerisinde bulunan bir ABD vatandaşı hakkında adli

---

<sup>684</sup> Bkz. UK-US Agreement m.1/12. Ayrıca bkz. Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 95; Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)"; "Groups Urge Congress to Oppose US-UK Cloud Act Agreement"; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 429.

<sup>685</sup> Birleşik Krallık tanımındaki farklılık, AB yükümlülükleri gereği AB vatandaşları ile Birleşik Krallık vatandaşları arasında ayırım yapma yasağından kaynaklanmaktadır.

<sup>686</sup> Bkz. UK-US Agreement m.7.

<sup>687</sup> Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)"; Daskal, Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards"; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1100; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 429.

istinabe sözleşmesi kapsamında bilgi talebinde bulunması imkân dahilinde olmayacaktır<sup>688</sup>.

Adli istinabe sözleşmesi kapsamına giren bilgiler iletişim içerikleri, bir kullanıcı için saklanmakta ya da işlenmekte olan veriler ile bunlara ilişkin trafik verileri ile meta verilerdir<sup>689</sup>. Ayrıca bir abone ya da kullanıcıyı tanımlayan isim, adres, hizmet tipi ve süresi, abone numarası ya da tanımlayıcılar (IP numarası ya da cihaz numarası gibi), telefon kayıtları, işlem zamanı ve süresi ile ödeme aracı bilgileri olarak tanımlanmış abone bilgileri de adli istinabe sözleşmesi kapsamı içerisindedir. Bilgilerin konum olarak nerede bulunması gerektiğine dair herhangi bir sınırlama sözleşme içerisinde mevcut değildir. Ancak kapsama giren bilgilerin hizmet sağlayıcıların elinde ya da kontrolünde olması gerekmektedir.

Adli istinabe sözleşmesinin uygulanması için taraf devletlerin birer yetkili makam oluşturmaları gerekmektedir<sup>690</sup>. Birleşik Krallık tarafından yetkili makam olarak İçişleri Bakanlığı atanmıştır<sup>691</sup>. ABD ise yetkili makam olarak Adalet Bakanlığı'nı atanmıştır<sup>692</sup>. Sözleşme m. 5/4'e göre taraflardan birisinin yetkili makamı, diğer tarafın ülkesinde bulunan hizmet sağlayıcıya doğrudan bilgiye erişim talebi gönderebilmektedir. Talebi alan hizmet sağlayıcının böyle bir durumda iki farklı seçeneği bulunmaktadır. Bunlardan ilki talebe uygun şekilde talep konusu bilgileri paylaşmaktır. İkincisi ise talebin, uluslararası adli istinabe sözleşmesini ihlal ettiğine yönelik olarak itirazını talebi gönderen yetkili makama iletmektir. Söz konusu itirazların mevcut sorunu çözmemesi halinde, hizmet sağlayıcı durumu bulunduğu

---

<sup>688</sup> Söz konusu talep CLOUD Act çerçevesinde yapılabilecektir. Detaylar için bkz. Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)".

<sup>689</sup> Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 95.

<sup>690</sup> Bkz. UK-US Agreement m.5. Ayrıca bkz. Daskal, Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards"; "Groups Urge Congress to Oppose US-UK Cloud Act Agreement"; Kalender, "Parçalı Bulutlar: Cloud Act ve Etkileri", s. 95; Peace, "Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation", s. 427.

<sup>691</sup> Birleşik Krallık İçişleri Bakanlığı, orijinal adı ile UK Home Office, hakkında bilgi için bkz. <https://www.gov.uk/government/organisations/home-office>.

<sup>692</sup> ABD Adalet Bakanlığı, orijinal adı ile Office of the Attorney General, hakkında bilgi için bkz. <https://www.justice.gov/ag>.

ülkenin yetkili makamına da ile bildirebilir. Talebi alanın bulunduğu ülkenin yetkili makamı, ilgili talebin adli istinabe sözleşmesi hükümlerine aykırılık teşkil ettiği sonucuna varırsa, bu durumu gönderenin yetkili makamına bildirerek ilgili bilgi talebinin sözleşme kapsamı dışına çıkarılmasını sağlayabilmektedir<sup>693</sup>.

Önemle belirtmek gerekir ki yukarıda bahsedilen bilgi talebi kararı, esasen yetkili makam tarafından verilmemektedir. Yetkili makamların ana görevi, ülke içi mahkemelerce (ve varsa diğer yetkili birimlerce) ceza yargılaması kapsamında verilen bilgi talebi kararlarını, karşı taraf ülkesindeki hizmet sağlayıcılara bildirmektedir<sup>694</sup>. Bu kapsamda da yukarıda belirtilen itiraz mekanizması sadece adli istinabe sözleşmesinin hükümleri ile sınırlıdır. Aşağıda detaylı olarak açıklanacağı üzere hizmet sağlayıcının ayrıca bilgi talebini düzenleyen iç hukuk sistemi kapsamında da itiraz hakları bulunmaktadır.

## **ii. Sözleşmenin İç Hukuk ile İlişkisi ve Karşılıklılık İlkesi Açısından Değerlendirilmesi**

ABD ile Birleşik Krallık arasında imzalanan adli istinabe sözleşmesinin bu ülkelerin iç hukukları ile çeşitli boyutlarda yakın ilişkileri bulunmaktadır. Bu ilişkiler hem sözleşmenin uygulanmasına etki etmekte hem de iç hukuk kurallarının sözleşme karşısındaki konumunun sınırlarını çizmektedir. Daha da önemlisi ise iç hukuk kuralları ile sözleşmenin ilişkisi aynı zamanda karşılıklılık prensibine etki etmektedir.

Adli istinabe sözleşmesi çerçevesinde yetkili makamlarca iletilecek tüm bilgi talebi kararları, taraf devletlerin iç hukukuna göre verilmesi gerekmektedir<sup>695</sup>. Söz konusu

---

<sup>693</sup> Bkz. UK-US Agreement m. 5/12. Ayrıca bkz. Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”; Kalender, “Parçalı Bulutlar: Cloud Act ve Etkileri”, s. 95; Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1099; Peace, “Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation”, s. 427-428.

<sup>694</sup> Bkz. UK-US Agreement m.5/5. Ayrıca bkz. Peters vd., “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, s. 1098-1099.

<sup>695</sup> Bkz. UK-US Agreement m. 5/1. Ayrıca bkz. Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”.

taleplerin hukuki etkisi de tamamen tarafların iç hukukundan kaynaklanmaktadır. Bu kapsamda bilgi talebi kararlarına iç hukuka göre itiraz imkânları da bulunmaktadır. Öte yandan hizmet sağlayıcıların ayrıca adli istinabe sözleşmesinin uygulanmasına dair yetkili makamlara yönelik itiraz imkânı da mevcuttur<sup>696</sup>.

Adli istinabe sözleşmesinde yer alan birtakım hükümler de tarafların iç hukukuna müdahale etmektedir<sup>697</sup>. Bu hükümlere örnek olarak tarafların iç hukukunun adli istinabe sözleşmesinin uygulanmasını engellemeyeceği taahhüdü gösterilebilmektedir. Ancak adli istinabe sözleşmesinin, diğer uluslararası sözleşmelerden en büyük farklılığı, bu sözleşmenin iç hukuktaki kuralların yerini almamasıdır<sup>698</sup>. Sözleşme m. 11 gereği incelenen adli istinabe sözleşmesi, ne taraflar arasında bulunan diğer adli istinabe sözleşmelerinin uygulanmasını ne de iç hukuktan doğan bilgi talebi imkânlarını ortadan kaldırmamakta yani bahse konu bilgi talepleri açısından münhasır bir yöntem olarak kabul edilmemektedir. Bunun en büyük sonucu taraflar arasında karşılıklılık ilkesinin uygulanmasının büyük oranda ortadan kalkmasıdır<sup>699</sup>.

Daha önceki bölümlerde açıklandığı üzere CLOUD Act tarafından tadil edilen SCA kapsamında ABD adli makamlarının, ABD dışında bulunan bilgileri dahi talep etme imkânı bulunmaktadır. Bu imkân tamamen ABD'nin iç hukukundan kaynaklanmaktadır. Adli istinabe sözleşmesinin, iç hukuktan doğan bilgi talebi imkânlarını ortadan kaldırmayacağına ilişkin hükmünün, özellikle SCA ile birlikte değerlendirildiğinde ortaya çıkmaktadır. Zira adli istinabe anlaşmasının özellikle kişi

---

<sup>696</sup> Bkz. UK-US Agreement m. 5/11. Ayrıca bkz. Daskal, Swire, "The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards"; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1099.

<sup>697</sup> Bkz. UK-US Agreement m.3/3. Ayrıca bkz. Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)"; Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1096.

<sup>698</sup> Bkz. UK-US Agreement m.11. Ayrıca bkz. Peters vd., "Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data", s. 1101.

<sup>699</sup> Rojszczak, "CLOUD act agreements from an EU perspective", s. 8; Christakis, "21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)"; "Groups Urge Congress to Oppose US-UK Cloud Act Agreement".

bakımından kapsamı, SCA'dan çok daha dardır. Örneğin SCA kapsamında Birleşik Krallık'ta bulunan bir kişiye ilişkin bilgilere erişmek mümkünken adli istinabe sözleşmesi kapsamında bir ABD makamlarının söz konusu bilgiye erişmesi mümkün değildir. Dolayısıyla SCA kapsamına giren bir hizmet sağlayıcı olduğu sürece ABD makamları için adli istinabe sözleşmesine başvurma konusunda fiili bir ihtiyaç doğmayacağı sonucuna varılmaktadır. Özellikle dijital ortamda hizmet sağlayan şirketlerin büyük çoğunluğunun ABD menşeli olduğu da göz önüne alındığında adli istinabe sözleşmesinin uygulama kapsamının ABD açısından ne kadar dar olduğu anlaşılabacaktır. Nitekim basında yer alan haberlere göre ABD Adalet Bakanlığı temsilcileri dahi SCA yerine adli istinabe sözleşmesine dayanılması gereken bir duruma dair örnek verememişlerdir<sup>700</sup>. Bunun sonucu olarak adli istinabe anlaşmasının ABD açısından en büyük sonucu, Birleşik Krallık adli makamlarına da dijital ortamdaki bilgilere erişim imkânı sağlamış olmasıdır<sup>701</sup>.

Karşılıklılık ilkesinin sağlanmadığı bir diğer durum da adli istinabe sözleşmesinin kapsamına giren kişi tanımlarının farklı olmasından kaynaklanmaktadır. Önceki bölümde de detaylıca açıklandığı üzere bir Birleşik Krallık vatandaşına dair bilgiler, eğer bu kişi Birleşik Krallık sınırları dışında bulunuyorsa adli istinabe sözleşmesi kapsamında ABD tarafından talep edilebilmektedir<sup>702</sup>. Buna karşılık ABD vatandaşlarına dair bilgiler bu kişiler nerede bulunursa bulunsun Birleşik Krallık tarafından adli istinabe sözleşmesi kapsamında talep edilememektedir.

#### **IV. SCA'NIN MİLLETLERARASI ÖZEL HUKUK İLE İLİŞKİSİ**

SCA'nın getirmiş olduğu hukuki düzenlemeler temel olarak ceza usul hukukuna ilişkindir. Bu nedenle SCA ile milletlerarası özel hukuk arasında herhangi bir ilişki bulunmadığını söylemek kanaatimizce mümkündür.

---

<sup>700</sup> Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”.

<sup>701</sup> “Groups Urge Congress to Oppose US-UK Cloud Act Agreement”; Christakis, “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”.

<sup>702</sup> Bkz. Yuk. s. 180 vd.

Öte yandan uluslararası adli istinabe sözleşmeleri, milletlerarası usul hukukunun incelediği konulardan birisidir. CLOUD Act ile birlikte değiştirilen SCA'nın öngördüğü yeni tip uluslararası adli istinabe sözleşmelerinin, milletlerarası usul hukuku açısından değerlendirilmesi gerekmektedir. Her ne kadar bu yeni tip sözleşmeler, daha önceki uluslararası adli istinabe sözleşmelerine kıyasla çok daha hızlı bir şekilde dijital ortamdaki delillere erişmeye imkân vermekteyse de kanaatimizce söz konusu sözleşmelerin yaygınlaşması söz konusu olmayacaktır. Zira söz konusu sözleşmelerin imzalanabilmesi için SCA içerisinde belirtilen kriterlerin sağlanmadığının kabulünün, Batı Bloğu ülkeleri haricinde mümkün olmayacağı düşünülmektedir. Kaldı ki bahse konu sözleşmelerin uluslararası hukuktaki karşılıklılık ilkesini zedeleyen yapıları; Batı Bloğu içerisinde dahi bu sözleşmelere karşı tepkiler olmasına sebebiyet vermektedir. CLOUD Act'ın yürürlüğe girmesinden işbu çalışmamızın tamamlanmasına kadar 5 yıl gibi bir süre geçmiş olmasına rağmen sadece Birleşik Krallık ve Avustralya gibi Anglosakson ülkeler ile sözleşme imzalanabilmiş olması ile AB nezdindeki müzakerelerin yeterli ilerlemeyi gösterememiş olması, düşüncemizin doğruluğu destekler niteliktedir.

SCA'nın imzalanmasını öngördüğü yeni tip uluslararası adli istinabe sözleşmelerinin, ABD menşeli bulut bilişim sağlayıcıların, ABD dışında karşılaştıkları zorlukların ortadan kaldırılmasını ve bu yolla da ABD'nin teknoloji alanındaki hegemonyasının da sürdürülmesini amaçladığı kanaatimizce malumdur. Bu sözleşmeler vasıtasıyla taraf devletlerin bilgiye erişme ihtiyacı, sözleşmeler içerisinde belirlenen şartlar ölçüsünde giderilmekte ve böylelikle söz konusu ihtiyacın giderilememesinden doğan ihtiyaçlara yönelik alternatif çözümler üretilmesinin önüne geçilmeye çalışılmaktadır. Ayrıca SCA'nın iç hukuk niteliği ile ABD makamlarına verdiği veriye erişim yetkilerinin, ABD açısından yeni tip uluslararası istinabe sözleşmelerine ihtiyaç duymadan dünyanın her yerindeki verilere erişmeye imkân vermesi, ABD açısından adli istinabe sözleşmelerine veriye erişim amacıyla ortaya atılmadığını da açık olarak göstermektedir.

## **V. SCA’NIN SINIR ÖTESİ UYGULAMA KAPSAMININ DEVLETLERİN ULUSLARARASI YETKİSİ AÇISINDAN DEĞERLENDİRİLMESİ**

SCA’nın sınır ötesi uygulama kapsamına sahip olması, aynı zamanda bu düzenlemeyi yapan ABD’nin uluslararası yetkisini sınır ötesi olarak kullandığını göstermektedirler. Dolayısıyla yapılan düzenlemenin, uluslararası yetkinin kullanımına ilişkin uluslararası hukuk kuralları açısından uygun olup olmadığının değerlendirilmesine ihtiyaç bulunmaktadır.

SCA’nın, sınır ötesi uygulama kapsamına sahip olması, uluslararası düzenleme yetkisi açısından sınır ötesi yetki kullanımının mevcut olduğunu göstermektedir. Daha önceki bölümlerde açıklandığı üzere, sınır ötesi düzenleme yetkisinin kullanımı uluslararası teamül hukukunda kural olarak yasaktır. Ancak müsamahakâr ilkeler kapsamında değerlendirilen durumların varlığı halinde, istisnai olarak sınır ötesi uygulama kapsamına sahip düzenlemeler; aynı zamanda uluslararası hukuka da uygun kabul edilmektedir. Müsamahakâr ilkeler; devletlerin vatandaşlarına kurallar koymasına imkân veren aktif kişilik ilkesi, devletlerin kendi vatandaşlarını korumak amacıyla yabancılara kurallar koymasını mümkün kılan pasif kişilik ilkesi, devletin kendi egemenlik ve bağımsızlığını korumak için kurallar koymasına izin veren koruma ilkesi ve insanlığa karşı suçların engellenmesi adına devletin kural koyabildiği evrensellik ilkesi olarak dört tane ilkedен oluşmaktadır.

Açıklanan bu ilkelerden pasif kişilik ilkesi, koruma ilkesi ve evrensellik ilkesi<sup>703</sup> nitelikleri itibarıyla SCA’nın içeriği ya da sınır ötesi uygulama kapsamı kuralları ile ilgili değildir. Zira burada SCA’nın ABD vatandaşlarını korumak adına yabancılara yönelik kurallar koyması söz konusu olmadığı gibi ABD devletinin egemenlik ve bağımsızlığına ilişkin bir durum ya da insanlığa karşı suçlarla ilgili bir konu bulunmamaktadır.

---

<sup>703</sup> Bkz. Yuk. s.32 vd.



Aktif kişilik ilkesi, SCA'nın sınır ötesi uygulama kapsamına sahip olmasının dayanağını teşkil edebilecek niteliktedir. Zira SCA ile ABD ile bağlantılı kişilerin yurtdışındaki fiillerine ilişkin kurallar getirilmektedir. Dolayısıyla aktif kişilik ilkesi açısından SCA'nın sınır ötesi uygulama kapsamına sahip olması, kanaatimizce uluslararası hukuk çerçevesinde uygun kabul edilebilecek niteliktedir. Ancak söz konusu ilkenin teamül niteliğinde olup herhangi bir uluslararası anlaşma ile kabul edilmemiş olması nedeniyle bahse konu uygunluğun uluslararası hukukun gelişimi ile birlikte ortadan kalkabileceğini de unutmamak gerekmektedir.

Hukuki düzenlemelerin gücü, bu düzenlemelerin uygulanmasını zorlayabilen bir kamu gücünün varlığından gelmektedir. Bir kanunun çıkarılması, o kanunu uygulayacak yetkili adli ve idari makamlar olmazsa, pratikte herhangi bir anlam ifade etmeyecektir. SCA'nın uygulanması noktasında kullanılan kamu gücü, bilgi talebine muhatap olan kişiye ABD sınırlarında uygulanacak yaptırımlar vasıtasıyla kullanılmaktadır. ABD kolluk kuvvetlerinin, bilgi talebine muhatap olan kişinin başka bir ülkedeki veri merkezine bilgi almak için müdahalede bulunması söz konusu olmamaktadır. Bu nedenle SCA kapsamında ABD'nin sınır ötesi uygulama yetkisini kullanmadığı ve dolayısıyla uluslararası hukuka aykırı davranmadığı düşünülmektedir. Zira uluslararası hukuk çerçevesinde bir devletin başka ülkede kamu gücü kullanması, ev sahibi devletin rızasına bağlanmıştır.

## **VI. SCA'NIN SINIR ÖTESİ UYGULAMA KAPSAMININ HUKUKLARIN ÇATIŞMASI KAVRAMI AÇISINDAN DEĞERLENDİRİLMESİ**

### **A. SCA'nın Sınır Ötesi Uygulama Kapsamının Hukukların Çatışması Durumu Yaratması**

Çalışmamızın daha önceki bölümlerinde de açıklandığı üzere, devletlerin düzenleme yetkilerini sınır ötesi kapsamlı olarak aynı olgu üzerinde kullanmaları halinde ortaya çıkan durum hukukların çatışması olarak adlandırılmıştır. İçinde bulunduğumuz internet çağının yapısı ve imkanları, verilerin farklı ülkelerde bulunmasını son derece

yaygın hale getirmektedir. Bir başka deyişle, her ÷lkeye ilişkin veriler o ÷lkede bulunmamakta, tam aksine genellikle bir ÷lkeye ilişkin veriler; diğler ÷lke ya da ÷lkeler içerisinde bulunmaktadır. Bu yapının temel sebebi, çalışmamızın bu bölümünde detaylı olarak açıklanan bulut bilişim yapılarının kullanımındır.

SCA kapsamında ABD makamlarının veri taleplerinin, verinin konumu dikkate alınmaksızın karşılanması zorunlu kılması, hukukların çatışması olgusunun kaçınılmaz olarak meydana gelmesine sebebiyet verecektir. Verinin bulunduğu ÷lkenin hukuk kurallarının, bu verinin o ÷lke dışına çıkarılmasını yasaklamış veya belirli koşullara bağlamış olması halinde; SCA kararının muhatabı olan kişinin ya ABD hukukunu ya da ilgili ÷lke hukukunu ihlal etmesi gerekecektir. Çalışmamızın dördüncü bölümünde açıklanan veri lokalizasyonu kuralları ile kişisel verilerin yurtdışına aktarımına ilişkin düzenlemeler getiren GDPR ve KVKK gibi kanunlar, SCA ile direkt olarak hukukların çatışması olgusunu yaratacak hukuk kurallarına örnek olarak gösterilebilecektir<sup>704</sup>. İlave bir örnek olarak Bankacılık Kanunu m. 73 de verilebilecektir. Anılan madde, Türk bankalarının yurtdışına veri aktarımını yasaklamaktadır. Öte yandan SCA kapsamında kalan bir kişinin Türkiye’deki veri merkezinde veri bulunduran bir bankanın, SCA çerçevesinde verilen bir mahkeme kararı üzerine bazı verilerinin yurtdışına çıkarılması halinde hem banka hem de ona veri merkezi hizmeti sunan dış hizmet sağlayıcı; Türk bankacılık mevzuatını ihlal etmiş olacaktır. İşte bu durum, yaşanabilecek hukukların çatışması durumlarına somut bir örnek teşkil etmektedir.

Birinci bölümde de açıklandığı ve yukarıda verilen örnekte de görülebileceği üzere bu tür hukukların çatışması durumlarının çözümüne ilişkin iç hukuk kuralları genellikle bulunmamaktadır. Zira devletler, iç hukuk kurallarını koyarken, yabancı devletlerin sınır ötesi uygulama kapsamına sahip kanunlarını dikkate almamaktadırlar. Ancak SCA içerisinde, hukukların çatışması durumu öngörülmüş ve bunun çözümüne ilişkin olarak milletlerarası nezaket analizi ve yeni tip uluslararası istinabe sözleşmeleri

---

<sup>704</sup> Christakis, “Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act”, s. 15.

öngörülmüştür. Ancak kanaatimizce bu çözümler de yine SCA'yı da yürürlüğe koyan ABD'nin menfaatlerini korumak üzere tasarlanmıştır. O nedenle bu unsurların hukukların çatışması sorununa objektif ve tarafsız bir çözüm getirdiği sonucuna varmamak gerektiği düşünülmektedir.

Kanaatimizce internet ve bilgi teknolojileri kullanımı arttıkça nasıl bu konudaki hukuki düzenleme sayısı artıyorsa, söz konusu hukuki düzenlemeler arasındaki hukukların çatışması durumları da artacaktır. O halde hukukların çatışması durumlarının iç hukuk sistemleri tarafından göz önüne alınmasının, yukarıda açıklandığı şekilde konuyu sadece buna muhatap olan kişilerin problemi olmaktan çıkarılacağı düşünülmektedir.

#### **B. SCA'nın Yarattığı Hukukların Çatışması Durumlarına Yönelik Çözüm Önerileri ve Ülkemizin Dijital Ortamdaki Bilgilere Erişime Dair Hukuk Politikasına İlişkin Öneriler**

Sınır ötesi uygulama kapsamına sahip olan SCA'nın, diğer ülke hukukları ile çelişkili durumlar yaratması ve bu kapsamda hukukların çatışması durumlarının oluşmasının kaçınılmaz olduğu kanaatimizce açıktır. O halde ülkemizin veriye erişim noktasındaki hukuk politikasının da bu çatışma durumunu düzenleyecek şekilde geliştirilmesi gerekmektedir. Aksi durumda SCA'nın hükümleri gereği Türkiye'de bulunan ya da Türkiye'ye ilişkin ve ABD menşeli kişilerin herhangi bir şekilde kontrolünde olan tüm veriler aynı zamanda ABD'nin erişimine açık kalmaya devam edecektir.

ABD mahkemelerinin verdiği kararlarda ve ABD hukuk doktrininde, mevcut uluslararası adli istinabe sözleşmelerinin çok yavaş sonuç doğurduğu<sup>705</sup> ve bu nedenle kolluk kuvvetlerinin söz konusu sözleşmelere dayanarak suçla mücadele etmelerinin beklenemeyeceği ifade edilmektedir. Oysaki Türk mahkemelerinin yabancı bulut bilişim sağlayıcılarından (özellikle sosyal medya şirketleri) yaptıkları bilgi talepleri,

---

<sup>705</sup> Claudia Warken, Lodewijk van Zwieten, Dan Svantesson, "Re-Thinking the Categorisation of Data in the Context of Law Enforcement Cross-Border Access to Evidence", **International Review of Law, Computers & Technology**, 2019, s. 17, (Çevrimiçi) <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1600871>, 07.05.2019.

yıllardır uluslararası adli istinabe sözleşmelerinde öngörülen prosedürlerin yürütülmesi gerektiği açıklamasıyla reddedilmektedir. ABD, karşılaştığı bu sorunu CLOUD Act'i yürürlüğe koyarak kendi iç hukuku vasıtasıyla çözmüştür. Bu çözüm sırasında hukukların çatışması durumu da dikkate alınmış ve muhtemel çatışmaların da ABD lehine çözümlenebilmesi için gerekli mekanizmalar, yine iç hukuk vasıtasıyla kurulmuştur.

Ülkemizde de 5651 sayılı kanunda 2020 ve 2022 yıllarında yapılan değişikliklerle özellikle sosyal medya şirketlerinin Türkiye sınırları içerisinde temsilci ataması ve akabinde şirketleşmelerinin sağlanmasına yönelik düzenlemeler öngörülmüştür. Yine bu değişiklikler ile sosyal medya şirketleri için veri lokalizasyonu yükümlülüğü öngörülerek verilerin Türkiye Cumhuriyeti Devleti egemenliği altında saklanması hedeflenmiştir. Çalışmamız tarihi itibarıyla temsilci atama işleminin somut bir faydasının görülemediği düşünülmektedir. Diğer önlemlerin etkileri ise önümüzdeki yıllarda görülecektir.

5651 sayılı kanunda yapılan değişiklikler, ülkemizin yurtdışında bulunan veriye erişim noktasındaki yetkinliklerini kanaatimizce yeterince arttırmamaktadır. Zira muhatap olacak yabancı sosyal medya şirketlerinin 5651 sayılı kanuna uymayı reddetmeleri halinde uygulanacak erişim engelleme veya azaltma ile idari para cezası yaptırımlarının yeterli olmadığı düşünülmektedir. İlgili sosyal medya şirketlerine erişimin engellenmesi aynı zamanda tüm Türk vatandaşlarını ve şirketlerini de olumsuz etkileyecektir. İdari para cezalarının tahsili de yine oldukça zordur. Kanaatimizce veriye erişim probleminin çözümü, Türk mahkemelerine bilgi talepleri konusunda sınır ötesi uygulama kapsamı olan SCA gibi kanunlarla yetki vermektir. Bu kanunun tıpkı Dördüncü Değişiklik ve SCA gibi farklı bilgi içeriklerine göre farklı korumalar öngörmesi ve söz konusu korumaların temel hak ve özgürlüklerin korunması noktasında uluslararası norm ve beklentilere uygun olması son derece uygun olacaktır.

SCA ile getirilen hükümler aynı zamanda bulut bilişim sağlayıcılarının üçüncü kişilere gönüllü olarak bilgi vermesini de yasaklamaktadır. Dolayısıyla başka bir ülkenin sınır

ötesi uygulama kapsamına sahip kanunu olsa dahi, SCA vasıtasıyla ABD kanun koyucusu bu kanunların ABD ülkesinde uygulanmasını engellemiş durumdadır. CLOUD Act'in kanunlaşması akabinde benzer bir düzenleme, Fransa'da da yapılmıştır. Bu çerçevede hukuki süreçlere ilişkin olarak yurtdışına bilgi aktarmak; eğer bu sürece herhangi bir Fransız mahkemesi dahil değilse, hukuka aykırı hale getirilmiştir<sup>706</sup>. Kanaatimizce benzer bir kanunun ülkemizde de yürürlüğe konulması hem karşılıklılık ilkesinin hem de Türk vatandaşlarının verilerinin ve adil yargılanma hakkının korunması açısından acil bir gerekliliktir.

Tarafımızca yukarıda sunulan tüm önerilerin esasen hukukların çatışması olgusunun yaşanması ihtimalini arttıran örnekler olduğu görülmektedir. Oysa iç hukuk kurallarından kaynaklanan bu sorun, temelde farklı ülke hukuk kurallarına uyum sağlamak zorunda olan kişileri olumsuz etkilemektedir. Kanaatimizce bu sorunun çözümlenebilmesinin en kolay yolu, her devletin iç hukuklarını hukukların çatışması yaratmayacak şekilde düzenlemesi olup bu yeknesaklaşmanın yöntemi de devletlerin uluslararası sözleşmeler imzalamalarıdır. Bahse konu sözleşmelerin imzalanması, devletlerin menfaatleri gerektirirse mümkün olabilecektir. Oysaki günümüz dünyasında söz konusu sözleşmelerin ülkemizle imzalanması için gerekli menfaat ortamının oluşmadığı tarafımızca gözlemlenmektedir. O halde ülkemizin hukuk politikası için en doğru olanın söz konusu menfaat ortamı oluşuna dek hem ülke menfaatlerinin korunmasına hem de olumsuz etkilenen yabancı bulut bilişim sağlayıcıların rahatsız olmasına elverişli düzenlemelerin yürürlüğe sokulmasıdır. Bir başka deyişle, hukukların çatışması vakıalarının sayısı, uzlaşma ortamı sağlanana dek olabildiğince arttırılmalıdır. Ancak bu şekilde bir uluslararası uzlaşma ortamının doğabileceği değerlendirilmektedir.

---

<sup>706</sup> Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", **Information Technology & Innovation Foundation**, 2017, s. 24, (Çevrimiçi) [http://www2.itif.org/2017-cross-border-data-flows.pdf?\\_ga=2.200100782.1604662306.1615630888-1194186901.1615630888](http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.200100782.1604662306.1615630888-1194186901.1615630888), 04.09.2020.

## DÖRDÜNCÜ BÖLÜM

### VERİ LOKALİZASYONU

#### I. GİRİŞ

İnternetin ve bilgi teknolojilerinin gelişmesi, günümüzde üretilen veri miktarlarını muazzam seviyede arttırmıştır<sup>707</sup>. Bu kapsamda yapılan araştırmalara göre, araştırma tarihinden önceki son 2 yılda, dünyadaki verinin %90'ı yaratılmıştır<sup>708</sup>. Söz konusu verilerin çok büyük kısmı, devasa veri merkezlerinden oluşan bulut bilişim sistemleri vasıtasıyla barındırılmakta ve işlenmektedir<sup>709</sup>.

Veri miktarının artışı aynı zamanda bu verileri işleyen ve barındıran bilgi sistemlerine olan ihtiyacı da arttırmaktadır. Ayrıca bu sistem ve veriler artık sadece eğlence gibi ihtiyari işler için kullanılmamakta; enerji, finans, sağlık ve ulaştırma gibi toplum için olmazsa olmaz alanlarda alternatifsiz olarak kullanılmaktadırlar<sup>710</sup>. Söz konusu yaygın kullanım, uluslararası veri transferlerinin hacmini arttırmış ve bu tür transferleri olmazsa olmaz hale getirmiştir. Yine kişiler arası iletişim ve etkileşimin neredeyse tamamen dijital ortama taşınmış olması, bireylerin hak ve özgürlüklerinin korunabilmesi için bu ortamlara devlet müdahalesini kaçınılmaz hale getirmiştir. Bu kapsamda söz konusu sistem ve verilerin devlet organlarınca erişilebilir halde olması, devlet organlarının müdahale edebilme imkanına sahip olabilmesinin ön şartı konumundadır.

---

<sup>707</sup> “Mapping Approaches to Data and Data Flows”, Suudi Arabistan, OECD, 2020, s. 7, (Çevrimiçi) <https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf>, 18.03.2021;

“Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”, s. 2.

<sup>708</sup> Vish, “How Much Data Is Created Every Day in 2021? [You’ll Be Shocked!]”, **TechJury**, 24.06.2020, (Çevrimiçi) <https://techjury.net/blog/how-much-data-is-created-every-day/>, 12.05.2021.

<sup>709</sup> Bkz. Yuk. s.112 vd. Ayrıca bkz. “Mapping Approaches to Data and Data Flows”, act 7; “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”.

<sup>710</sup> Joshua P. Meltzer, Peter Lovelock, “Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia”, **Brookings**, (20.03.2018), (Çevrimiçi) <https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/>, 16.05.2020.

Dijital ortamı oluşturan verileri barındıran bilgi sistemlerinin bulunduğu konumlar, bu bilgi sistemlerinin ve barındırdıkları verilerin önemlerinin artmasıyla birlikte devletlerin ilgi alanlarına girmeye başlamıştır<sup>711</sup>. Bu değişimin temel sebepleri olarak güvenlik ve ekonomi alanlarındaki endişeler gösterilebilmektedir<sup>712</sup>. Zira bir devletin toplum hayatı için kritik önemdeki bilgi sistemlerinin ve verilerin, başka bir devletin ülkesinde (yani egemenliğinde) bulunması bir takım soru işaretleri doğurmaktadır. Bunlardan ilki söz konusu verilere ve bilgi sistemlerine hangi hukuk kurallarının nasıl uygulanacağı hususudur. Diğer bir sorun da bu veri ve sistemlere ilgili devletin adli ve idari makamlarının erişememesi nedeniyle ülke içerisinde bu makamların etkin çalışmamasıdır. İşte bu endişelerin giderilmesi için bilgi sistemleri ya da verilerin bulunacakları konumu sınırlayan veri lokalizasyonuna ilişkin hukuki düzenlemeler yapılmaya başlanmıştır.

Başka ülkede bulunan verilere ya da bilgi sistemlerine, diğer bir ülke hukukunun (örneğin verilerin ve bilgi sistemlerinin ilişkili olduğu ülkenin) uygulanması fiiliyatta ciddi zorluklar barındırmaktadır. Zira daha önceki bölümlerde açıklandığı üzere uluslararası düzenleme yetkisinin sınır ötesi kullanımı birçok farklı şarta bağlıdır. Bu şartlar sağlansa dahi ev sahibi devletin mülk ilkesine dayanan uluslararası yetki kullanımı ile diğer devletin sınır ötesi yetki kullanımı neticesinde şu an için hukuki bir çözümü olmayan hukukların çatışması durumu ortaya çıkacaktır. Ayrıca devletlerin uluslararası yetkisinin diğer görünümleri olan uygulama ve yargılama yetkilerinin de sınır ötesi kullanımı pratikte mümkün olmayacaktır. Örnek olarak, BTK tarafından **Facebook** ya da **Twitter** gibi sosyal medya şirketlerine kesilen idari para cezalarının, bu şirketlerin yurtdışındaki mal varlıklarının Türk makamları tarafından haczedilememesi nedeniyle tahsilinde zorluklar yaşanması gösterilebilecektir.

---

<sup>711</sup> Tatevik Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, *International Journal of Communication*, C. 10, 2016, s. 2221; Örnek için “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020- 2023”, T.C. Ulaştırma ve Altyapı Bakanlığı, s. 23, (05.06.2022), (Çevrimiçi) <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-planlari-2020-2023.pdf>, 05.06.2022.

<sup>712</sup> Anupam Chander, Uyên P. Lê, “Data Nationalism”, *Emory Law Journal*, C. 64, S. 3, 2015, s. 682.

Veri lokalizasyonu mevzuatının çalışmamız açısından önemi, bu kuralların veriler ve bilgi sistemleri üzerinde devletin kullandığını uluslararası yetkinin dayandığı ilkeler üzerindeki etkisidir. Zira bu kurallar, kuralı yürürlüğe sokan devletin ülkesinde bilgi sistemleri ve verilerin saklanması öngörmektedir. Böylelikle söz konusu unsurların tamamen ilgili devletin mülklik ilkesine dayalı uluslararası yetkisine tabi olması sağlanmaktadır ve düzenleme, uygulama ve yargılama yetkilerinin sınır ötesi kullanımından doğabilecek sorunların önüne geçilmektedir. Ayrıca bilgi sistemleri ve verilere erişim için oldukça yavaş işleyen milletlerarası istinabe kurallarına başvurma zorunluluğu da bertaraf edilmiş olmaktadır. Yine internetin doğurduğu yabancılık unsuru içeren sorunların çözümünde kanunlar ihtilafı kurallarının yetersiz kalması<sup>713</sup>, veri lokalizasyonu yükümlülüklerini de gündeme getirmiştir.

Veri lokalizasyonu kurallarının bir diğer amacı da yabancı devletlerin ülke içerisinde bulunan bilgi sistemleri ve veriler üzerinde uluslararası yetki kullanmalarına engel olmaktadır. Bir başka deyişle, yabancı hukukların ülke içerisinde bulunan bilgi sistemlerine ve verilere uygulanmasını engellemektir<sup>714</sup>. Ancak bu hedef, sınır ötesi uygulama kapsamına sahip yabancı ülke kanunları nedeniyle zedelenmektedir ve sınır ötesi uygulama kapsamına sahip kanunlar ile ev sahibi ülke kanunları arasında hukukların çatışması durumunun doğmasına sebebiyet vermektedir.

Veri lokalizasyonunun aynı zamanda yabancı yatırım kararları açısından bir değerlendirme konusu olduğu ve serbest ticaret anlaşmaları içerisinde de gündem olduğu gözlemlenmektedir. Bu durum veri lokalizasyonunun, uluslararası ticaret ve doğrudan yabancı yatırımlar üzerinde de derin bir etkisi olduğunu ortaya koymaktadır.

Çalışmamızın bu bölümü altında öncelikle veri lokalizasyonu hakkında genel bilgiler verilecektir. Bu kapsamda özellikle kavramın hukuki tanımı, neden getirildiği, nasıl uygulandığı ve doğurduğu sonuçlar incelenecektir. Daha sonrasında ise ülkemizde ve

---

<sup>713</sup> Miriam A. Cherry, “A Global System of Work, a Global System of Regulation: Crowdsourcing and Conflicts of Law”, *Tulane Law Review*, C. 94, S. 2, 2019, s. 244.

<sup>714</sup> “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”, s. 14.



dünyada yürürlükte bulunan veri lokalizasyonu kuralları üzerinde durulacaktır. Sonraki başlıklar altında veri lokalizasyonunun milletlerarası özel hukuk ve hukukların çatışması konularına dair etkileri incelenecektir. Son olarak ise veri lokalizasyonu konusunda ülkemizin politikalarına ilişkin öneriler sunulacaktır.

## II. VERİ LOKALİZASYONU KAVRAMI HAKKINDA GENEL BİLGİLER

### A. Veri Lokalizasyonu Kavramının Tanımı

Veri lokalizasyonu kavramı, AB'nin Kişisel Olmayan Verilerin Serbest Akışı Regülasyonu<sup>715</sup> içerisinde “*üye devletin kanunları, yönetmelikleri ya da idari düzenlemeleri ya da genel ve tutarlı idari uygulamaları neticesinde verilerin belirli bir üye devlette işlenmesini gerektiren ya da belirli bir üye devlette işlenmemesini öngören her türlü yükümlülük, sınırlama, koşul, limit ya da diğer gereksinimler*” şeklinde tanımlanmıştır.

Veri lokalizasyonu kavramına ilişkin olarak doktrinde de farklı tanımlar bulunmaktadır. Bir tanıma göre veri lokalizasyonu kavramı, verinin ülke sınırları arasında aktarımını özellikle engelleyen önlemler olarak anlaşılmalıdır<sup>716</sup>. Diğer bir yazara göre veri lokalizasyonu, verinin üretildiği ülkenin sınırları içerisinde fiziksel olarak bulunan bir cihaz içerisinde saklanması anlamına gelmektedir. Başka bir yazar ise kavramı internet üzerinde bulunan kullanıcı verisinin, verinin kökeni olan ülkede bulunan bir veri merkezinde saklanması şeklinde tanımlamaktadır<sup>717</sup>. Farklı bir yazar da terimin genellikle verinin belirli bir ülke sınırları içerisinde fiziksel olarak saklanmasını ifade ettiğini; ancak bazı durumlarda sınır ötesi veri akışını sınırlayan

<sup>715</sup> “Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union”, **Official Journal of the European Union**, 2018, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>, 08.08.2021.

<sup>716</sup> Chander, Lê, “Data Nationalism”, s. 680.

<sup>717</sup> Pavan Duggal, “Data Localization: A Review of Proposed Data Localization Legislation in India, With Learnings for The United States”, **Data Catalyst**, 2019, s. 4, (Çevrimiçi) <https://datacatalyst.org/wp-content/uploads/2019/12/Data-Localization-Pavan-Duggal.pdf>, 04.10.2020.

unsurları da kapsayacak şekilde daha geniş anlamda da kullanıldığını ifade etmektedir<sup>718</sup>. Veri lokalizasyonu kavramının bir diğer tanımı, verinin belirli coğrafi alanlarda saklanması, işlenmesini ya da hareketini gerektiren uygulamalar şeklinde verilmiştir<sup>719</sup>. Başka bir çalışmaya göre veri lokalizasyonu, bir devletin yabancı ya da yerli şirketler için yerel veri işleme ve saklama altyapıları kurma veya da veri toplama ve aktarma işlemlerini toptan bırakma yükümlülükleri getirdiği hukuki şartlar anlamına gelmektedir<sup>720</sup>. Farklı bir tanıma göre ise verinin belirli bir devletin egemenlik alanı içerisinde saklanması doğrudan ya da dolaylı olarak gerektiren, bağlayıcı kanuni ya da idari yükümlülükler veri lokalizasyonu yükümlülüğüdür<sup>721</sup>.

Yukarıdaki tanımlardan da anlaşılabileceği üzere, her ne kadar farklı ifadeler kullanılmış olsa da doktrinde veri lokalizasyonu kavramı üzerinde ortak bir anlayışta uzlaşıldığı görülmektedir. Bu anlayışa göre verilerin başka bir ülkeye aktarılmasını engelleyen, başka bir bakış açısıyla verilerin belirli bir ülkede saklanmasını gerektiren her türlü yükümlülük veri lokalizasyonu yükümlülüğü olarak tanımlanmaktadır.

Veri lokalizasyonu (**data localization**) kavramına yakın anlamda kullanılan bir başka kavram ise veri egemenliği (**data sovereignty**) kavramıdır. Veri egemenliği kavramı, verinin konumundan bağımsız olarak; veri üzerinde uygulama alanı bulan hukukun, ilgili egemen devletin hukuku olması anlamına gelmektedir<sup>722</sup>. Öte yandan veri lokalizasyonu yükümlülükleri, verinin konumuna etki ederek verinin tabi olacağı

<sup>718</sup> Duggal, a.y.

<sup>719</sup> Jyoti Panday, Jeremy Malcolm, “The Political Economy of Data Localization”, **The Open Journal of Sociopolitical Studies**, Symposium 4, 2018, s. 513, (Çevrimiçi) <http://sibaese.unisalento.it/index.php/paco/article/viewFile/19553/16635>, 12.03.2021.

<sup>720</sup> Akın Ünver, Grace Kim, “Cross-Border Data Transfers and Data Localization”, Edam Cyber Policy Paper Series 2016/3, 2016, s. 6, (Çevrimiçi) [https://edam.org.tr/wp-content/uploads/2017/03/data\\_transfers\\_en.pdf](https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf), 04.09.2020.

<sup>721</sup> D. Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, OECD Digital Economy Papers, No. 301, 2020, s. 8, (Çevrimiçi) [https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges\\_7fbaed62-en](https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en), 28.12.2020.

<sup>722</sup> Yudhistira Nugraha, Kautsarina, Ashwin Sastrosubroto, “Towards Data Sovereignty in Cyberspace”, **Third International Conference of Information and Communication Technology**, 2015, s. 1, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2610314](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610314), 27.12.2020; Richard D. Taylor, “Data Localization’: The Internet in the Balance”, **Telecommunications Policy**, C. 44, S. 8, 2020, s. 4; Tambiana Madiaga, “Digital Sovereignty for Europe”, European Parliamentary Research Service, 2020, s. 1, (Çevrimiçi) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf), 18.03.2021.

hukukun, yükümlülüğü getiren ülke hukuku olmasını temin etmeye çalışmaktadır. Bu yönüyle veri lokalizasyonu yükümlülüklerinin, veri egemenliğini sağlamaya çalıştığını söylemek kanaatimizce uygun olacaktır. Ancak tek başına veri lokalizasyonu yükümlülükleri, önceki bölümlerde açıklanan sınır ötesi uygulama kapsamına sahip kanunlar nedeniyle veri egemenliğini sağlama konusunda yeterli değildirler. Zira veri lokalizasyonu yükümlülükleri, sınır ötesi uygulama kapsamına sahip kanunların uygulanmasının önüne geçmemektedir.

### B. Veri Lokalizasyonu Yükümlülüğü Tipleri

Veri lokalizasyonu yükümlülüklerinin temel olarak üç farklı şekilde görüldüğünü söylemek mümkündür<sup>723</sup>. Bunlardan ilki, verileri barından ya da verilerin işlenmesini sağlayan bilgi sistemlerinin bulundukları konumlara ilişkin sınırlamalardır. İkincisi ise verilerin (bilgi sistemlerine ilişkin yükümlülüklerden bağımsız olarak) ülke içerisinde saklanmasını öngören yükümlülüklerdir. Üçüncüsü de verilerin belirli bir bölge (ya da ülke) dışına aktarılmasını yasaklayan kurallardır. Söz konusu tiplerin hepsini veri lokalizasyonu yükümlülüğü olarak kabul etmek mümkün olmasına rağmen her bir yükümlülük tipinin yarattığı etkinin de farklı olduğu kanaatimizce açıktır.

Verilerin saklandığı bilgi sistemlerinin konumuna ilişkin yükümlülükler ile verilerin konumuna ilişkin yükümlülükler arasında pratik sonuçlar açısından bir fark bulunduğunu söylemek düşüncemize göre mümkün değildir. Çünkü veriler ile bilgi sistemlerini birbirinden ayrı düşünmek imkansızdır. Bilgi sistemleri olmadan verilerin işlenmesi ya da barındırılması mümkün olamamaktadır<sup>724</sup>. Ancak verilerin belirli bir

---

<sup>723</sup> John Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, *International Journal of Law and Technology*, C. 25, 2017, s. 214; Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, Switzerland, International Centre for Trade and Sustainable Development (ICTSD), 2016, s. 2; “Mapping Approaches to Data and Data Flows”, s. 30; Verilerin yurtdışına aktarılmasının vergiye tabi kılınması gibi yurtdışına veri aktarımını sınırlayan her türlü yükümlülüğün veri lokalizasyonu olarak kabul edilmesi gerektiği şeklinde bir görüş bulunmaktadır (Chander, Lê, “Data Nationalism”, s. 680). Ancak kanaatimizce verilerin yurtdışına aktarımını fiilen imkansız hale getirmeyen yükümlülüklerin veri lokalizasyonu olarak kabul edilmesi doğru değildir. Bu kapsamda yurtdışına veri aktarımına ilişkin vergi miktarı orantısız şekilde yüksek değilse, görüşümüze göre böyle bir verginin veri lokalizasyonu yükümlülüğü olarak kabul edilmemesi gerekir.

<sup>724</sup> Önemle belirtmek gerekir ki elektronik ortamda saklanmayan veriler de (örneğin kâğıt üzerine yazılmış bir liste) veri lokalizasyonu yükümlülüğüne tabi olabilir ve bu verilerin işlenmesi için bilgi

bölge dışına aktarılmasını kısıtlayan yükümlülükler ile bilgi sistemlerinin ya da verilerin konumunu belirleyen yükümlülükler arasında önemli bir fark bulunmaktadır. Konuma ilişkin düzenlemeler genellikle verilerin başka bir kopyasının ilgili bölge (ya da ülke) dışına aktarılmasına imkân verirken, ikinci gruptaki aktarımı kısıtlayan yükümlülükler böyle bir aktarıma dahi imkân vermemektedir<sup>725</sup>. Dolayısıyla, veri aktarımının sınırlanmasına ilişkin veri lokalizasyonu yükümlülüklerinin, diğer tip veri lokalizasyonu yükümlülerine kıyasla daha ağır sonuçlar doğurduğunu söylemek fikrimizce mümkündür. Bu sonuçlar özellikle fiziki sınırları göz önüne almaksızın işleyen dijital ortamdan ve dijital ortamda sunulan hizmetlerden yararlanma noktasında görülmektedir.

Veri lokalizasyonunun düzenlendiği hukuki enstrümanlar da çeşitlilik gösterebilmektedir. Veri lokalizasyonu, çeşitli norm tipleri (örneğin kanun, yönetmelik, tebliğ ya da karar gibi) altında bağlayıcı bir hukuki yükümlülük olarak getirilebilmektedir<sup>726</sup>. Aşağıda detaylıca açıklanacak olan Türk bankacılık mevzuatı, bu yaklaşımın bir örneğini oluşturmaktadır. Bunun yanında mevzuatın açıkça veri lokalizasyonu yükümlülüğü öngörmemesine rağmen, idareye tanınan takdir yetkisinin kullanım şekli, fiili (**de facto**) ya da dolaylı olarak veri lokalizasyonu yükümlülüğü doğurabilmektedir<sup>727</sup>. Örneğin, 6698 sayılı KVKK m. 9 çerçevesinde kişisel verilerin aktarımı imkanlarının Kişisel Verileri Koruma Kurumu tarafından etkin şekilde işletilmemesi, kanaatimizce Türkiye’de kişisel veriler açısından fiili durumda veri lokalizasyonu yükümlülüğü olduğunu göstermektedir.

Veri lokalizasyonu yükümlülüklerinin bir diğer görünümü de bağlayıcı hukuk kuralları yerine takip edilen politikalar neticesinde söz konusu yükümlülüklerin getirilmesidir. Bu yaklaşıma örnek olarak bir idari organın, idari birimler nezdinde verilerin nasıl saklanması gerektiğine dair yayınladığı rehberler ya da benzeri

---

sistemlerine gerek duyulmayabilir. Ancak bu durum çok nadir gündeme gelebileceği gibi veri hacmi açısından elektronik ortamda bulunan veriler ile kıyaslanması mümkün dahi olmayacaktır.

<sup>725</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 10.

<sup>726</sup> Svantesson, **a.g.e.**, s. 8.

<sup>727</sup> Svantesson, **a.g.e.**, s. 9.

yönlendirmeler gösterilebilmektedir. Bu yaklaşıma aşağıda detaylıca açıklanacak olan Cumhurbaşkanlığı tarafından yayınlanmış genelge ve rehber örnek teşkil edebilecektir<sup>728</sup>.

### **C. Veri Lokalizasyonu Yükümlülüğünün Gündeme Gelmesine Sebep Olan Olaylar**

İnternetin ortaya çıkışıyla birlikte, 1970’lerden itibaren ortaya çıkmaya başlayan<sup>729</sup> veri lokalizasyonu yükümlülüklerinin son yıllarda tüm dünyada yaygınlaşmaya başladığı gözlemlenmektedir<sup>730</sup>. Bu yükümlülüklerin devletlerin gündemlerine girmesinin en temel sebebi, şüphesiz ki dijital ortamın büyüüp gelişmesi ile toplum hayatında çok önemli bir yer tutmaya başlamasıdır. Bu ana gelişme ekseninde yaşanan birtakım olaylar ise veri lokalizasyonu konusunda devletlerin harekete geçmesini hızlandırmış durumdadır.

Veri lokalizasyonu yükümlülüklerinin getirilmesine sebep olan olaylar zincirinin ilk halkası, 11 Eylül 2001 tarihinde ABD’de gerçekleştirilen terör saldırılarıdır<sup>731</sup>. İkiz Kulelerin yıkılması ve Pentagon’a saldırılması olayları, ABD kamuoyunda büyük tepki yaratmıştır. Bu tepkiler neticesinde de ABD tarafından, milli güvenlik endişelerini ön planda tutan, temel hak ve özgürlükleri ciddi şekilde sınırlayan yasalar çıkarılmıştır<sup>732</sup>. Söz konusu yasalar, ABD Hükümeti’ne son derece geniş istihbarat ve bilgi toplama yetkileri vermektedir. Bu yetkilerin dijital ortamı da kapsaması, diğer devletin kendilerine ilişkin verileri bir şekilde güvende tutma reflekslerinin doğmasına sebep olmuştur.

---

<sup>728</sup> Bkz. Aş. s. 235 vd.

<sup>729</sup> Christopher Kuner, “Data Nationalism and Its Discontents”, **Emory Law Journal**, C. 64, 2015, s. 2091.

<sup>730</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 11; Mira Burri, “Interfacing Privacy and Trade”, **Case Western Reserve Journal of International Law**, C. 53, S. 1, 2021, s. 43.

<sup>731</sup> Kerr, “Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn’t”, s. 607-674.

<sup>732</sup> “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”, Authenticated U.S. Government Information, 26.10.2001, (Çevrimiçi) <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>, 26.10.2021.

ABD Hükümeti'nin sahip olduğu geniş bilgi toplama ve istihbarat faaliyetleri yürütme yetkilerinin kullanım şekilleri, 2013 yılında NSA'de görev yapmakta olan Edward **Snowden** tarafından deşifre edilmiş ve tüm dünyaya ilan edilmiştir<sup>733</sup>. **Snowden** tarafından yayınlanan belgeler, telefon dinlemelerinden dünya liderlerinin bilgisayarlarına sızılmasına kadar birçok istihbarat faaliyetinin yürütüldüğünü ifşa etmiştir. Bu belgeler arasında ülkemizin devlet görevlilerinin bilgisayarlarına izinsiz erişilmesi ya da büyükelçiliklerinin dinlenmesi gibi faaliyetleri ortaya çıkaran bilgiler de bulunmaktadır<sup>734</sup>.

**Snowden**'in ifşa ettiği istihbarat programlarından birisi de PRISM'dir<sup>735</sup>. PRISM programı, NSA'in **Google, Microsoft, Facebook, Apple** ve **Amazon** gibi teknoloji devlerinden, kullanıcı verilerini alabilmesine imkân vermektedir<sup>736</sup>. NSA'in, bahse konu teknoloji şirketlerinin sistemlerine doğrudan erişimi olduğu iddia edilmişse de bu iddialar ABD Hükümeti ve ilgili şirketler tarafından yalanlanmıştır<sup>737</sup>. ABD Hükümeti söz konusu bilgi taleplerin, bu konuya ilişkin olarak istihbarat ve takip konularında görevlendirilmiş bir bağımsız mahkemenin verdiği kararlar doğrultusunda yapıldığını iddia ederek temel hak ve özgürlüklerin yargı gözetiminde korunduğunu öne sürmüştür<sup>738</sup>.

---

<sup>733</sup> Chander, Lê, "Data Nationalism", s. 714; Burri, "Interfacing Privacy and Trade", s. 50; Deşifre edilen belgelere erişmek için bkz. "Snowden Doc Search", (17.05.2021), (Çevrimiçi) <https://search.edwardsnowden.com/>, 17.05.2021.

<sup>734</sup> İlgili haber için bkz. "Documents Show NSA and GCHQ Spied on Partner Turkey", (Çevrimiçi) <https://www.spiegel.de/international/world/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html>, 17.05.2021.

<sup>735</sup> PRISM'in açılımı, *Planning Tool for Resource Integration, Synchronization and Management* şeklindedir.

<sup>736</sup> Kemp, "Cloud Computing and Data Sovereignty", s. 6.

<sup>737</sup> Glenn Greenwald, Ewen MacAskill, "NSA Prism Program Taps into User Data of Apple, Google and Others", **The Guardian**, 2013, s. 6, (Çevrimiçi) <https://www.pulitzer.org/files/2014/public-service/guardianus/02guardianus2014.pdf>, 17.10.2021; Jonah Force 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, 2014, s. 5, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2430275](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275), 14.03.2021.

<sup>738</sup> Greenwald, MacAskill, "NSA Prism Program Taps into User Data of Apple, Google and Others", s. 2.

**Snowden**'in kamuoyuna sunduğu bilgilerden anlaşıldığı kadarıyla dünya liderlerinin telefonları ve elektronik cihazları sürekli olarak NSA tarafından takibe alınmıştır<sup>739</sup>. Bu casusluk faaliyetleri özellikle dönemin Almanya Şansölyesi Merkel tarafından sert bir şekilde eleştirilmiştir<sup>740</sup>.

**Snowden**'in açığa çıkardığı istihbarat çalışmalarından birisi de İngiltere'nin istihbarat kurumu olan GCHQ ile NSA tarafından açık denizlerde bulunan ve internet ağı altyapısını oluşturan fiber optik kablolarla müdahale ederek aktarılan verilerin bu kurumlarca ele geçirilmesidir<sup>741</sup>. Söz konusu kurumlar bu yolla kişileri takip edebilmiştir.

**Snowden** tarafından yapılan ifşalar neticesinde, tüm diğer devletler arasında veri lokalizasyonu yükümlülüklerine yönelik güçlü bir eğilim doğmuştur<sup>742</sup>. Zira **Snowden** ifşaları, ABD menşeli hiçbir teknolojinin esasen veri gizliliği ve güvenliği konusunda yeterli olmadığını göstermiştir<sup>743</sup>. Yani ABD'li teknoloji şirketlerine olan güven, **Snowden** ifşalarından sonra ciddi oranda kırılmıştır. Ayrıca internet altyapısına dahi

---

<sup>739</sup> Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", s. 34.

<sup>740</sup> Hill, **a.g.e.**, s. 9.

<sup>741</sup> Kemp, "Cloud Computing and Data Sovereignty", s. 7; Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", s. 15.

<sup>742</sup> Svantesson, "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", s. 12; Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", s. 3; Christopher Millard, "Forced Localization of Cloud Services: Is Privacy the Real Driver?", **IEEE Cloud Computing**, C. 2, S. 2, 2015, s. 11; Sargsyan, "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security", s. 2224; Taylor, "'Data Localization': The Internet in the Balance", s. 4; "Mapping Approaches to Data and Data Flows", s. 27; "Understanding Data Localization Laws"; Posman Krismanto Sitinjak, Riva'atul Adaniah Wahab, "Policy Analysis of Data Localization in Digital Market Integration in Southeast Asian Region", **Jurnal Masyarakat Telematika dan Informasi**, C. 10, S. 1, 2019, s. 44.

<sup>743</sup> Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems", s. 881-918; Vincenzo Zeno-Zencovich, "Around the CJEU Schrems Decision: Digital Sovereignty and International Governance of Telecommunication Networks", 2016, s. 16, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2788789](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2788789), 15.12.2020; Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", s. 34.

yapılan müdahaleler, devletleri hem verileri hem bilgi sistemlerini hem de internet ağını yurtiçinde tutma<sup>744</sup> gibi çalışmalara yöneltmiştir.

#### D. Veri Lokalizasyonu Yükümlülüğünü Getirilmesinin Amaçları ve Etkileri

Veri lokalizasyonu yükümlülüklerinin getirilmesinde güdülen amaçları güvenliğe ve ekonomiye ilişkin olanlar olmak üzere temel olarak iki gruba ayırmak mümkündür<sup>745</sup>. Ekonomik amaçlar ülke içerisinde yatırım yapılmasının sağlanması ve yerli teknoloji sektörünün korunması gibi konulara odaklanmaktadır. Verilerin gizliliği ve güvenliğinin sağlanması, verilere yabancı devletlerin erişiminin engellenmesi (özellikle istihbarat açısından) ile devlet kurumlarının verilere erişiminin temin edilmesi gibi amaçlar ise güvenliğe yönelik amaçlar altında değerlendirilmektedir.

Veri lokalizasyonu yükümlülüklerinin getirilmesinin etkileri de hem ekonomik hem güvenlik alanlarında kendilerini göstermektedir. Örneğin güvenlik amacıyla verilerin belirli konumdaki veri merkezlerine toplanması, hedefi bir noktaya topladığı için siber saldırılara verileri daha açık hale getirebilmesine rağmen<sup>746</sup> aynı zamanda yabancı devlet kurumlarının verilere hukuki şekilde erişmelerinin (özellikle fiziki erişimi

<sup>744</sup> “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020- 2023”, s. 21; “2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi”, (2019), (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf>, 26.09.2021; Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 10; Millard, “Forced Localization of Cloud Services: Is Privacy the Real Driver?”, s. 12; H. Jacqueline Brehmer, “Data Localization: The Unintended Consequences of Privacy Litigation”, **American University Law Review**, C. 67, S. 3, 2018, s. 932.

<sup>745</sup> Chander, Lê, “Data Nationalism”, s. 713; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 14; Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 19; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 227; Colin Bennett, Smith Oduro-Marfo, “Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?”, **UbiComp '18: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers**, 2018, s. 886; Taylor, “‘Data Localization’: The Internet in the Balance”, s. 6; Jennifer Daskal, Justin Sherman, “Data Nationalism on the Rise”, **Data Catalyst**, 2020, s. 4, (Çevrimiçi) <https://datacatalyst.org/wp-content/uploads/2020/06/Data-Nationalism-on-the-Rise.pdf>, 27.11.2020; George Yijun Tian, “Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement: Join or Withdraw”, **Wisconsin International Law Journal**, C. 34, S. 2, 2016, s. 384; Ünver, Kim, “Cross-Border Data Transfers and Data Localization”, s. 6.

<sup>746</sup> Chander, Lê, “Data Nationalism”, s. 716.



keserek) kısmen de olsa önüne geçebilmektedir<sup>747</sup>. Ekonomik açıdan bakıldığında da bazı sektörlerin büyümesini sağlayan (örneğin veri merkezi işletmecileri) veri lokalizasyonu yükümlülükleri, aynı zamanda teknolojiden yararlanan kişilerin daha yüksek maliyetlere katlanmasına sebep olabilmektedir<sup>748</sup>. Dolayısıyla veri lokalizasyonu yükümlülüklerinin hem pozitif hem de negatif etkileri bulunduğunu söylemek mümkündür.

Aşağıdaki başlıklar altında veri lokalizasyonu yükümlülüklerinin getirilme amaçları ile bunların etkileri incelenecektir. Böylelikle güdülen amaç ile fiili olarak doğan sonuçların karşılaştırılması hedeflenmektedir.

## **1. Güvenlik Amaçları**

### **a. Veri Güvenliği ve Gizliliğinin Sağlanması**

Veri lokalizasyonu yükümlülüklerinin gerekliliğine ilişkin öne sürülen gerekçelerden birisi, verilerin güvenliğinin ve gizliliğinin sağlanmasıdır<sup>749</sup>. Buradaki güvenlikten kasıt, verilerin yeterli teknik ve idari tedbirler altında yetkisiz üçüncü kişilerin erişiminden korunmasıdır<sup>750</sup>. Veri lokalizasyonu yükümlülükleri vasıtasıyla devletler, verilerin kendi mevzuatlarına uygun şekilde korunmasını ve gizliliklerinin sağlanmasını (örneğin kişisel verilerin korunması mevzuatları vasıtasıyla) temin etmeye çalışmaktadırlar<sup>751</sup>. Veri lokalizasyonu aynı zamanda verilere fiziki erişimin de kontrol altına alınmasına imkân vererek veri güvenliğinin ve gizliliğinin sağlanmasına katkıda bulunmaktadır<sup>752</sup>.

---

<sup>747</sup> Chander, Lê, **a.g.e.**, s. 717.

<sup>748</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 12.

<sup>749</sup> Berry, Reisman, “Policy Challenges of Cross-Border Cloud Computing”, s. 18; Ryan, Falvey, Merchant, “When the Cloud Goes Local: The Global Problem with Data Localization”, s. 57; Erica Fraser, “Data Localisation and the Balkanisation of the Internet”, **SCRIPTed: A Journal of Law, Technology and Society**, C. 13, S. 3, 2016, s. 363; “Mapping Approaches to Data and Data Flows”, s. 28; Francesca Casalini, Javier López González, Taku Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers”, **OECD Trade Policy Papers**, 2021, s. 8.

<sup>750</sup> Chander, Lê, “Data Nationalism”, s. 718.

<sup>751</sup> Chander, Lê, **a.y.**; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 27.

<sup>752</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 14.

Veri güvenliği açısından konuya bakıldığında, veri lokalizasyonu yükümlülüklerinin veri güvenliğini sağlama konusunda etkin olduğunu söylemek, yabancı devletlerin veriye erişiminin engellenmesi başlığı altında detaylıca açıklanan sebeplerle kanaatimizce mümkün değildir. Zira veri güvenliği tedbirlerinin, verilerin konumu ile herhangi bir ilişkisi bulunmamaktadır<sup>753</sup>. Üstelik verilerin tek bir konumda toplanması da veri güvenliği açısından zafiyet yaratabilecek niteliktedir<sup>754</sup>. Veri lokalizasyonu yükümlülüklerinin bu konuda sağlayabileceği tek fayda, verilerin korunmasını sağlamak amacıyla ilgili devlet hukukunun gerektirdiği veri güvenliği önlemlerinin alınmasını sağlamak olabilecektir.

Veri gizliliğinin (**privacy**) sağlanması amacı konusunda veri lokalizasyonu yükümlülüklerinin kısmen başarılı bir rol oynadığını söylemek kanaatimizce mümkündür. Zira, veri lokalizasyonu yükümlülükleri hem verilerin tabi olacağı hukuku mülklik ilkesi çerçevesinde belirlemekte hem de bu hukukun fiilen uygulanmasına imkân vermektedir. Öte yandan aynı sonuca KVKK<sup>755</sup> veya GDPR<sup>756</sup> gibi sınır ötesi uygulama kapsamına sahip kanunlarla da ulaşmak mümkün olabilmektedir. Yine bu düzenlemeler içerisinde bulunan ülke dışına kişisel veri aktarımı yapılabilmesi için belirli güvenlik tedbirleri alma zorunluluğu getiren kurallar aynı sonuca ulaşmayı mümkün kılabilir<sup>757</sup>. Ancak KVKK veya GDPR gibi

<sup>753</sup> Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 25; Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, s. 2223; Neha Mishra, “Data Localization Laws in a Digital World”, **The Public Sphere**, 2016, s. 143, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2848022](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2848022), 04.11.2020.

<sup>754</sup> Chander, Lê, “Data Nationalism”, s. 719; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 15; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 363; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 229; Brehmer, “Data Localization: The Unintended Consequences of Privacy Litigation”, s. 968; Peter Swire, DeBae Kennedy-Mayo, “Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data”, 2020, s. 6, (Çevrimiçi) [https://edpb.europa.eu/sites/default/files/webform/public\\_consultation\\_reply/comments\\_to\\_edpb\\_recommendations\\_by\\_swire\\_and\\_mayo\\_2020.pdf](https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/comments_to_edpb_recommendations_by_swire_and_mayo_2020.pdf), 18.03.2021; Erik van der Marel, “Data localisation in the EU: the threat from inside”, **Encompass**, (12.2016), (Çevrimiçi) <https://encompass-europe.com/comment/data-localisation-in-the-eu-the-threat-from-inside>, 04.11.2020.

<sup>755</sup> Bkz. Yuk. s. 88 vd.

<sup>756</sup> Bkz. Yuk. s. 68 vd.

<sup>757</sup> Doktrinde yer alan bir görüş (Chander, Lê, “Data Nationalism”, s. 690) kişisel verilerin korunmasına ilişkin mevzuatın veri lokalizasyonu yükümlülüğü olarak kabul edilmesi gerektiğini ileri sürmektedir.

sınır ötesi uygulama kapsamına sahip düzenlemelerin ülke dışında uygulanmalarındaki zorluklar ile yurtdışına aktarıma ilişkin önlemlerin verilerin aktarıldığı ülke hukukunun veri gizliliğini ihlal eden hükümlerini bertaraf edememesi<sup>758</sup> durumlarının, veri lokalizasyonu yaklaşımını daha makul gösterdiği de gözden kaçırılmamalıdır. Yine de veri lokalizasyonu yükümlülüklerinin, bahse konu amaç açısından tek imkân olduğunu söylemek kanaatimizce mümkün değildir.

#### **b. Devlet Kurumlarının Veriye Erişiminin Sağlanması**

Bir ülke içerisindeki devlet kurumlarının, kanunları uygulayabilme yetkinliğine sahip olması gerekmektedir. Hem idari organların hem de adli organların kanunları uygulamak amacıyla çeşitli verilere erişme ihtiyacı bulunmaktadır. Bu ihtiyaçlara örnek olarak, bir vergi incelemesinde finansal kayıtların incelenmesi ya da bir suç soruşturmasında delillerin toplanmasını vermek mümkündür.

Dijital ortama ilişkin altyapılar geliştikçe verilerin ilişkili olduğu ülkelerden başka ülkelerde saklanması da kolaylaşmıştır. Bu durum, verilerin ilişkili olduğu devlet kurumlarının söz konusu verilere erişimini son derece zorlaştırmaktadır<sup>759</sup>. Çünkü yabancı bir ülkede bulunan verilere erişmek, milletlerarası tebligat ve istinabe süreçlerinin uygulanmasını gerektirmektedir. Ancak bu süreçlerin işletilebilmesi hem ilgili devletler arasında ilgili konulara ilişkin uluslararası sözleşmeler bulunmasına bağlıdır hem de söz konusu süreçlerden netice alabilmek yıllar sürmektedir<sup>760</sup>.

---

Bu görüşü eleştiren başka bir yazar ise temel hak ve özgürlüklerin korunmasının veri lokalizasyonu yükümlülüğü olarak kabul edilemeyeceğini ifade etmektedir (Kuner, “Data Nationalism and Its Discontents”, s. 2093). Kanaatimizce kişisel verilerin korunması kuralları, kişisel verilerin yurtdışına aktarımının imkansız hale getirmiyorsa, veri lokalizasyonu yükümlülüğü olarak kabul edilmemelidir.

<sup>758</sup> Schrems II, C-311/18, (Avrupa Birliği Adalet Divanı 16 Temmuz 2020) (Çevrimiçi), paragraf 105, [http://curia.europa.eu/juris/document/document\\_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=12630077](http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=12630077), 06.08.2021.

<sup>759</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 15; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 230; Cook, “Cross-Border Data Access and Active CyberDefense: Assessing Legislative Options for a New International Cybersecurity Rulebook”, s. 223.

<sup>760</sup> Bazı yazarlar, adli istinabe prosedürlerinin varlığı nedeniyle devletlerin yurtdışındaki verilere erişebildiğini ve bu nedenle veri lokalizasyonu yükümlülüklerinin gereksiz olduğunu öne sürmektedir (Chander, Lê, “Data Nationalism”, s. 735). Ancak kanaatimizce adli istinabe prosedürlerinden sonuç almanın yıllar aldığı gerçeği karşısında bu görüşe katılmak mümkün değildir. Nitekim çeşitli ABD ve AB mahkeme kararlarında da bu durum ifade edilmiş durumdadır (In re Search Warrant No. 16-960-

Açıklanan bu soruna çare olarak veri lokalizasyonu yükümlülüklerini kullanılmaktadır<sup>761</sup>. Bu kapsamda veri lokalizasyonu yükümlülüklerinin devlet kurumlarının verilere erişimini sağlamak adına başarılı bir sonuç doğurduğunu söylemek mümkündür<sup>762</sup>.

### c. Yabancı Devletlerin Verilere Erişiminin Engellenmesi

Snowden ifşalarının da gösterdiği üzere, dijital ortamda gerçekleştirilen istihbarat faaliyetleri son derece yaygın ve etkilidir<sup>763</sup>. Yabancı devletlerin istihbarat faaliyetlerinden korunmak isteyen devletlerin başvurdukları yollardan birisi de veri lokalizasyonu yükümlülükleri vasıtasıyla verilerin kendi ülkelerinde saklanması sağlamaktır<sup>764</sup>. Her ne kadar yabancı bir ülkede verileri saklamaya kıyasla daha iyi olduğunu iddia etmek mümkün olsa da veri lokalizasyonu yükümlülüklerinin bu konuda etkin bir çözüm olduğunu söylemek mümkün değildir<sup>765</sup>. Zira verilerin belirli merkezi noktalarda toplanması, verilere erişimin fiziki bir erişimi çoğu zaman gerektirmemesi, veri aktarımlarına ilişkin trafiğin istihbarat faaliyetlerine konu olabilmesi ya da yerel çözümlerin devasa ölçekte hizmet veren bulut sistemleri ile aynı güvenlik seviyesine sahip olamaması<sup>766</sup> gibi sebepler veri lokalizasyonu

---

M-01 to Google ve In re Search Warrant No. 16-1061-M to Google de 27 [Çevrimiçi] <https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf> 05.06.2022). Benzer yönde bir görüş için bkz. Selby,

“Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 230.

<sup>761</sup> Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 23; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 365; “Mapping Approaches to Data and Data Flows”, s. 27; Casalini, González, Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers”, s. 8.

<sup>762</sup> Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, s. 2223; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 230.

<sup>763</sup> Chander, Lê, “Data Nationalism”, s. 714; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 228.

<sup>764</sup> Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 25; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 364; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 14.

<sup>765</sup> Chander, Lê, “Data Nationalism”, s. 717; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 364; Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, s. 2229; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 228.

<sup>766</sup> Bu tür sistemler yüksek güvenlik seviyeleri sunabilmekteyse de yine verilerin tek sistem içerisinde toplanması ile barındırdıkları veri hacimleri nedeniyle bu sistemlerin daha çok saldırıya hedef olması gibi durumlar da bu sistemler açısından güvenlik riskleri teşkil etmektedir.

yükümlülüğünden beklenen yabancı devletlerin istihbarat faaliyetlerini önleme amacına ulaşılmasını engellemektedir<sup>767</sup>.

Yabancı devletlerin verilere erişme sebepleri, sadece istihbarat faaliyetleri ile sınırlı değildir. Yabancı devletler de kendi kanunlarını uygulamak amacıyla gerçekleştirdikleri adli ve idari faaliyetler çerçevesinde çeşitli verilere erişme ihtiyacı duyabilmektedirler. Bu kapsamda veri lokalizasyonu yükümlülükleri vasıtasıyla belirli bir ülkede tutulması gereken verilere ilgili yabancı devletin hukuka uygun şekilde erişimi, ancak verilerin bulunduğu ülkenin bilgisi ve kontrolü dahilinde mümkün olabilmektedir. Zira burada yine milletlerarası sözleşmelere dayalı tebligat, istinabe ve bilgi paylaşımı usullerinin devreye girmesi gerekmektedir<sup>768</sup>. Bu açıdan bakıldığında da kanaatimizce veri lokalizasyonu yükümlülüklerinin kısmen başarı sağladığını söylemek mümkündür. Ancak diğer bölümlerde değinilen sınır ötesi uygulama kapsamına sahip kanunların<sup>769</sup>, veri lokalizasyonu yükümlülüklerinin bu konudaki etkilerinin azalmasına sebep olduğu düşünülmektedir.

## 2. Ekonomik Amaçlar

Veri lokalizasyonu yükümlülükleri getirilmesinin güvenlik yanında ekonomi açısından da faydaları olduğu savunulmaktadır<sup>770</sup>. Bu faydalar sırası ile ülke içindeki iş imkanlarının artması<sup>771</sup>, bilgi teknolojileri alanında yerli ve yabancı yatırımların artması ve buna bağlı olarak yerli teknoloji sektörünün gelişmesi<sup>772</sup> olarak sıralanabilmektedir.

---

<sup>767</sup> Chander, Lê, “Data Nationalism”, s. 716; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 14.

<sup>768</sup> Detaylı bilgi için bkz. (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2021/12/20211217-7.htm>, 02.03.2022

<sup>769</sup> Bkz. Yuk. s. 65 vd.

<sup>770</sup> Chander, Lê, “Data Nationalism”, s. 721; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 367; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 16; “Mapping Approaches to Data and Data Flows”, s. 28; Casalini, González, Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers”, s. 9.

<sup>771</sup> Mishra, “Data Localization Laws in a Digital World”, s. 147; Bennett, Oduro-Marfo, “Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?”, s. 886.

<sup>772</sup> Chander, Lê, “Data Nationalism”, s. 723; Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 19; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 367; Mishra, “Data Localization Laws in a Digital

Veri lokalizasyonu yükümlülüklerinin yerli teknoloji sektörünü koruma konusundaki etkisi, veri lokalizasyonu yükümlülüğü getiren ilgili ülke içerisinde bilgi teknolojilerine ilişkin yatırım yapılmasını yerli ve yabancı yatırımcılar açısından zorunlu hale getirmesi şeklindedir<sup>773</sup>. Bu da ülke içerisindeki teknoloji sektörünün gelişmesi anlamına gelmektedir. Söz konusu duruma örnek olarak, Türkiye’de uzun süredir veri lokalizasyonu yükümlülüğü altında bulunan bankaların bilgi teknolojileri alanında son derece yetkin hale gelmeleri ve büyük yatırımlar yapmaları gösterilebilmektedir. Ayrıca veri lokalizasyonu yükümlülüklerinin ülke ekonomileri açısından zararı bulunmadığını öne süren çalışmalar da bulunmaktadır<sup>774</sup>.

Öte yandan diğer sektörler için, veri lokalizasyonu yükümlülüklerinin maliyetleri arttırdığı ve hizmet kalitesini düşürdüğü de birçok çalışmada gösterilmiş durumdadır<sup>775</sup>. Bu açıdan veri lokalizasyonu yükümlülüklerinin ekonominin diğer

---

World”, s. 145; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 228; Andrew D. Mitchell, Neha Mishra, “Data at the Docks: Modernizing International Trade Law for the Digital Economy”, **Vanderbilt Journal of Transnational Law**, C. 20, S. 4, 2018, s. 1085; Susannah Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures”, **World Trade Review**, C. 18, S. 4, 2019, s. 581.

<sup>773</sup> Zira burada verilerin ilgili ülkede saklanabilmesi için o ülke içerisinde mutlaka bilgi sistemleri tutulması gerekmektedir. Söz konusu bilgi sistemleri yükümlülüğe tabi kişi tarafından direkt olarak kurulabileceği gibi yerel şirketlerden de kiralanabilecektir. Her durumda ülke içerisinde verilerin saklanması konusunda yatırım yapılması gerekecektir.

<sup>774</sup> Ike Brannon, Hart Schwartz, “The New Perils of Data Localization Rules”, **Regulation**, C. 41, S. 2, 2018, s. 31.

<sup>775</sup> Chander, Lê, “Data Nationalism”, s. 724; Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 27; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 368; Mishra, “Data Localization Laws in a Digital World”, s. 148; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 229; Brehmer, “Data Localization: The Unintended Consequences of Privacy Litigation”, s. 933; Taylor, “‘Data Localization’: The Internet in the Balance”, s. 7; Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 20; “Mapping Approaches to Data and Data Flows”, s. 11; “Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows”, World Economic Forum, 2020, s. 9, (Çevrimiçi) [http://www3.weforum.org/docs/WEF\\_Paths\\_Towards\\_Free\\_and\\_Trusted\\_Data%20Flows\\_2020.pdf](http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf), 09.12.2021; Burri, “Interfacing Privacy and Trade”; van der Marel, “Data localisation in the EU: the threat from inside”; Kyu Yub Lee, Moon hee Cho, Jungu Kang, Minji Kang, “Welfare Effects of the EU GDPR and Data Localization Measures”, **World Economy Brief**, C. 9, S. 7, 2019, s. 5, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3407208](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407208), 04.08.2020; Cody Ankeny, “The Costs of Data Localization”, **Information Technology Industry Council**, (17.08.2016), (Çevrimiçi) <https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization>, 04.04.2020; Brannon, Schwartz, “The New Perils of Data Localization Rules”, s. 13; Matthias Bauer, Martina F. Ferracane, Erik van der Marel, “Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization”, **Centre for International Governance Innovation and Chatham House**, Paper Series No. 30, 2016, s. 10.

alanlarında yabancılara karşı uygulanan ek mali yükümlülük ya da vergi gibi koruma önlemleriyle aynı sonuçları doğurduğunu söylemek mümkündür<sup>776</sup>. Ayrıca veri lokalizasyonu nedeniyle uluslararası serbest veri akışının kesilmesi, bazı ticari faaliyetlerin de aksamasına sebebiyet verebilmektedir<sup>777</sup>. Ancak devletlerin başka menfaatler uğruna ekonomik zorluklara katlanmayı seçebileceklerini de göz önünde bulundurmak, veri lokalizasyonu yükümlülüklerinin getirilme amaçlarının anlaşılabilirliği açısından önem arz etmektedir<sup>778</sup>.

#### **E. Veri Lokalizasyonu Yükümlülüğüne Dair Farklı Devletlerin Bakış Açıları**

Veri lokalizasyonu yükümlülüklerinin öngörülmesi ve uygulanma yöntemleri konusunda devletlerin farklı yaklaşımları bulunmaktadır. Bu yaklaşım farklılıkları devletlerin uluslararası ilişkilerdeki pozisyonları, coğrafi konumları, teknoloji üretme kapasiteleri ve yönetim şekilleri gibi unsurlar neticesinde meydana gelmektedir.

ABD, veri lokalizasyonu yükümlülüklerine tamamen karşı bir duruş sergilemektedir<sup>779</sup>. Bu yaklaşımın temelinde teknoloji devleri olan şirketlerin neredeyse tamamının ABD menşeli olması ile bu şirketlerin tüm dünyaya hizmet sunması gelmektedir<sup>780</sup>. Ayrıca verinin ABD şirketleri elinde toplanması aynı

<sup>776</sup> Chander, Lê, “Data Nationalism”, s. 722; Mishra, “Data Localization Laws in a Digital World”, s. 145; Panday, Malcolm, “The Political Economy of Data Localization”, s. 513.

<sup>777</sup> Swire, Kennedy-Mayo, “Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data”, s. 7.

<sup>778</sup> Kuner, “Data Nationalism and Its Discontents”, s. 2095.

<sup>779</sup> Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 215; Buna rağmen ABD meclisinde konu gündeme gelmiş ve Rusya ve Çin menşeli şirketlerin ABD vatandaşlarına ilişkin verileri ABD sınırları içerisinde saklamasını zorunlu kılan bir kanun teklifi tartışılmıştır (Daskal, Sherman, “Data Nationalism on the Rise”, s. 2) Bu öneri kabul edilmemiş olsa da milli güvenlik incelemesi gibi bir takım önlemler, söz konusu şirketler için uygulamaya alınmıştır (Daskal, Sherman, “Data Nationalism on the Rise”, s. 3). Jacqueline Varas Jennifer Huddleston, “Impact of Data Localization Requirements on Commerce and Innovation”, American Action Forum, 16.06.2020, (Çevrimiçi) <https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/>, 14.02.2021; Burri, “Interfacing Privacy and Trade”, s. 55; Jamie Davies, “US Government to consider strict data localisation laws”, Telecoms.com, (19.11.2019), (Çevrimiçi) <https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/>, 22.05.2020.

<sup>780</sup> Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, s. 2222; Mishra, “Data Localization Laws in a Digital World”, s. 149; Selby, “Data localization laws:

zamanda verinin ABD'nin uluslararası yetkisi içerisinde (hem mülkilik ilkesi hem de aktif kişilik ilkesi çerçevesinde) ve dolayısıyla bu devletin erişiminde olduğu anlamına gelmektedir<sup>781</sup>. Son olarak veri lokalizasyonu yükümlülükleri, serbest ticareti olumsuz etkilediği için ABD bu tür yükümlülükleri desteklemekten kaçınmakta ve milletlerarası sözleşmelerde veri lokalizasyonu yükümlülüklerini engellemeye yönelik hükümlere yer vermeye çalışmaktadır<sup>782</sup>. Netice itibarıyla ABD'nin güvenlik ve ekonomi alanlarındaki çıkarlarının, bu devletin veri lokalizasyonu yükümlülüklerine karşı olmasını gerektirdiği anlaşılmaktadır<sup>783</sup>.

AB tarafından ise özellikle **Snowden** ifşalarının da etkisiyle verilerin AB sınırları içerisinde tutulması ya da AB hukuku çerçevesinde korunmak kaydıyla AB dışına aktarılması yaklaşımı benimsenmiş durumdadır<sup>784</sup>. Bu kapsamda her ne kadar AB veri lokalizasyonu yükümlülüklerini direkt olarak benimsememiş olsa da veri aktarımlarına ilişkin çeşitli hukuki düzenlemeler ve yerel teknoloji altyapılarının kullanımına ilişkin teşviklerle birlikte verilerin AB içerisinde kalmasını sağlamaya çalışmaktadır<sup>785</sup>.

---

trade barriers or legitimate responses to cybersecurity risks, or both?", s. 216; Graham Webster, Scarlet Kim, "The Data Arms Race Is No Excuse for Abandoning Privacy", **Foreign Policy**, (14.08.2018), (Çevrimiçi) <https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/>, 20.05.2020.

<sup>781</sup> Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", s. 216.

<sup>782</sup> Selby, **a.g.e.**, s. 217.

<sup>783</sup> Öte yandan belirtmek gerekir ki, ABD dahi Savunma Bakanlığı için çalışan bulut hizmeti sağlayıcılar ile federal vergi bilgilerini içeren bilgi sistemleri açısından veri lokalizasyonu yükümlülüğü öngörülmektedir (Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures", s. 580).

<sup>784</sup> Bennett, Oduro-Marfo, "Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?", s. 881.

<sup>785</sup> W. Kuan Hon, Christopher Millard, Jatinder Singh, Ian Walden, "Policy, Legal and Regulatory Implications of a Europe-Only Cloud", **International Journal of Law and Information Technology**, C. 24, S. 3, 2016, s. 28; Daskal, Sherman, "Data Nationalism on the Rise", s. 3; Taylor, "Data Localization: The Internet in the Balance", s. 9; Benjamin Wong, "Data Localization and ASEAN Economic Community", **Asian Journal of International Law**, C. 10, S. 1, 2020, s. 174; Madiega, "Digital Sovereignty for Europe", s. 2.



Çin ve Rusya gibi Batı Bloğu ülkeleri ile mesafeli olan devletler genellikle kapsamlı veri lokalizasyonu yükümlülüklerini benimseme yoluna gitmektedirler<sup>786</sup>. Bu ülkelerin gerek coğrafi konumları gerekse ekonomik yapıları, veri lokalizasyonu yükümlülüklerinin uygulanmasına da elverişlidir. Ayrıca söz konusu devletlerin veri lokalizasyonu yükümlülükleri vasıtasıyla, siyasi yapılanmalarına da uygun olarak, vatandaşlarını takip etme gibi bir amaçları da bulunmaktadır<sup>787</sup>.

Son olarak ifade etmek gerekir ki G20 ülkeleri tarafından güven içerisinde uluslararası serbest veri akışının sağlanmasının önemi vurgulanmaktadır<sup>788</sup>. Dolayısıyla global çapta uluslararası serbest veri akışının sağlanmasının önemli olduğunun kabul edildiği, ancak buna ne kapsamda izin verilmesi gerektiği konusunda fikir ayrılıkları bulunduğu sonucuna varılabilecektir<sup>789</sup>.

### III. TÜRKİYE VE DÜNYADA VERİ LOKALİZASYONU YÜKÜMLÜLÜKLERİ

#### A. Türkiye’de Veri Lokalizasyonu Yükümlülüğü Getiren Mevzuat

Türk hukukunda veri lokalizasyonu yükümlülüğü getiren kurallar, ağırlıklı olarak düzenleyici ve denetleyici kurumların yetkisi altında bulunan çeşitli sektörlerle yönelik mevzuat içerisinde bulunmaktadır. Bu sektörlerin başında, sermaye piyasaları da dahil olmak üzere bankacılık ve finans gelmektedir. Ayrıca kamu kurum ve kuruluşlarının

<sup>786</sup> Justin Sherman, Holden Triplett, “Why Russia, China, and Other Countries Are Demanding Big Tech Companies Build Local Offices”, **Future Tense**, (2022), (Çevrimiçi) <https://slate.com/technology/2022/02/data-localization-laws-china-russia-authoritarian.html>, 18.04.2022.

<sup>787</sup> Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders”, s. 4; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 366.

<sup>788</sup> “G20 Osaka Leaders’ Declaration”, 2019, s. 2, (Çevrimiçi) [https://www.consilium.europa.eu/media/40124/final\\_g20\\_osaka\\_leaders\\_declaration.pdf](https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf), 20.07.2020; “G20 Riyadh Summit Leaders’ Declaration”, 2020, s. 5, (Çevrimiçi) <https://www.oecd.org/g20/g20-riyadh-summit.pdf>, 20.01.2021; “G20 Rome Leaders’ Declaration”, 2021, s. 15, (Çevrimiçi) <https://www.governo.it/sites/governo.it/files/G20ROMELEADERSDECLARATION.pdf>, 13.02.2022.

<sup>789</sup> Sam Sacks, Justin Sherman, “The Global Data War Heats Up”, **The Atlantic**, (26.06.2019), (Çevrimiçi) <https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/>, 21.05.2020.

altyapılarına, kritik altyapı niteliği taşıyan özel hukuk kişilerine ait altyapılara ve vergi kayıtlarına ilişkin düzenlemeler de mevcuttur.

Yukarıdaki açıklamadan da anlaşılacağı üzere, ülkemizde genel bir veri lokalizasyonu (yani niteliğine veya içeriğine bakmaksızın tüm veriler için geçerli olan) getiren bir hukuk kuralı bulunmamaktadır. Ancak KVKK'nın yurtdışına kişisel veri aktarımı hükümlerinin getirdiği sıkı şartlar nedeniyle kişisel veriler açısından **de facto** bir veri lokalizasyonu yükümlülüğü bulunduğunu söylemek kanaatimizce mümkündür.

Sonraki başlıklar altında Türk hukukunda yürürlükte bulunan veri lokalizasyonu yükümlülüklerine<sup>790</sup> ilişkin mevzuat incelenecektir.

## **1. Bankacılık ve Finans Sektörüne Yönelik Veri Lokalizasyonu Yükümlülükleri**

### **a. Bankacılık Kanunu ve İkincil Düzenlemeleri**

Mevcut ekonomik sistemlerin işleyişindeki önemleri nedeniyle bankalar ülke ekonomileri için son derece kritiktir. Bankaların faaliyetlerinde yaşanabilecek aksaklıklar çok büyük ekonomik krizler yaşanmasına sebep olabilmektedir<sup>791</sup>. Bu nedenle Türkiye dahil hemen her ülkede bankalar sıkı hukuki düzenlemelere tabi tutulmaktadır.

5411 sayılı Bankacılık Kanunu ile ülkemizdeki bankacılık faaliyetleri düzenlenmiştir. Aynı kanunla kurulan BDDK<sup>792</sup>, bankalar için düzenleyici ve denetleyici kurum olarak

<sup>790</sup> Yürürlükten kalkan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin 5/5 numaralı maddesi, sağlık verilerinin yurtdışına aktarılmasını yasaklayarak veri lokalizasyonu yükümlülüğü öngörmekteydi. Benzer şekilde Elektrik Piyasası Lisans Yönetmeliğine 22 Ekim 2016 tarihinde eklenen 29/j maddesi ile bilgi sistemlerinin ve verilerin yurtiçinde tutulması gerektiği ifade edilerek veri lokalizasyonu yükümlülüğü getirilmiştir. Ancak her iki yükümlülük de daha sonra yapılan değişikliklerle birlikte kaldırılmıştır. Çalışmamız tarihinde yürürlükte olmayan bu tür yükümlülüklerle ilerleyen başlıklar altında yer verilmeyecektir.

<sup>791</sup> Bankacılık krizleri örnekleri için bkz. Hilal Altıntaş, “Bankacılık Krizleri, Nedenleri ve Ekonomik Maliyetleri”, **Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, S. 22, 2004, s. 56.

<sup>792</sup> BDDK'nın açılımı, “Bankacılık Düzenleme ve Denetleme Kurumu” şeklindedir. İnternet sitesi için bkz. “Bankacılık Düzenleme ve Denetleme Kurumu”, (03.11.2021), (Çevrimiçi) <https://www.bddk.org.tr/>, 03.11.2021.

görev yapmaktadır. Bankacılık Kanunu'nun verdiği yetkiler çerçevesinde bankacılık faaliyetlerine ilişkin ikincil düzenlemeleri (yönetmelik ya da tebliğler gibi) yapma yetkisi de BDDK'ya aittir.

Bankacılık Kanunu ve ikincil düzenlemeler içerisinde veri lokalizasyonu gerektiren hükümler ile verilerin yurtdışına aktarımını sınırlayan hükümler bulunmaktadır. Dolayısıyla Türkiye'de faaliyet gösteren bankaların hem sahip oldukları verileri yurtiçinde tutmaları hem de mevzuatta izin verilen haller haricinde bu verileri yurtdışına aktarmamaları gerekmektedir.

Bankacılık Kanunu m. 73 altında, bankaların sahip olduğu verilere ilişkin iki adet kavram kullanılmaktadır. Bunlar, müşteri sırrı ve banka sırrı olarak adlandırılmaktadır. Müşteri sırrı kavramı, m. 73/3 altında bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler olarak tanımlanmıştır. Banka sırrı kavramının tanımı ise Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik<sup>793</sup> m. 5/5 numaralı maddesinde müşteri sırrı niteliğinde olmayıp sadece bankaya ait bilgileri içeren bilgiler olarak ifade edilmiştir.

Bankacılık Kanunu m. 73/3, ana kural olarak müşteri sırrı niteliği taşıyan bilgilerin yurtiçindeki ya da yurtdışındaki üçüncü kişilerle paylaşamayacağını hüküm altına almıştır. Bu ana kurala getirilen üç istisna bulunmakta olup bu istisnalardan ilki müşteriden gelen bir talimat ya da talep olmasıdır. Kanun, burada KVKK kapsamında verilen açık rızaları, bir talimat ya da talep olarak kabul etmemiştir. Ana kurala getirilen ikinci istisna, yine aynı madde altında sayılan sır saklama yükümlülüğü kapsamı dışında kabul edilen hallerdir. Son istisna kuralı ise diğer kanunların bu konudaki emredici hükümlerinin saklı tutulmasıdır.

Bankacılık Kanunu m. 73/3 altında banka sırları ile müşteri sırlarının paylaşılmasına imkân veren ve sır saklama yükümlülüğü kapsamı dışında kabul edilen hallerden ilki,

---

<sup>793</sup> “Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik”, (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39171&MevzuatTur=7&MevzuatTertip=5>, 17.10.2021.

sosyal güvenlik ve sosyal yardımlaşmaya ilişkin konularda ilgili kurum ve kuruluşlara yine ilgili mevzuat çerçevesinde bilgi paylaşılmasıdır. İkinci hal ise bankalar ve finansal kuruluşlar arasında, doğrudan ya da Risk Merkezi<sup>794</sup> veya kurulacak şirketler vasıtalarıyla yapılacak bilgi ve belge alışverişleridir. Üçüncü halde ise doğrudan veya dolaylı pay sahipliği yoluyla bankanın sermayesinin yüzde onunu veya daha fazlasını temsil eden payların satışı amacıyla, muhtemel alıcılarla değerlendirme yapılabilmesi için bilgi paylaşılmasıdır. Bilgi paylaşılacak diğer bir hal ise bankaların yüzde on veya daha fazla payına sahip ana ortaklıkları ile çeşitli finansal faaliyetler (konsolide finansal tablo hazırlanması, risk yönetimi, iç denetim, menkul kıymet satışı) için bilgi paylaşılabilmesidir. Bankaların değerlendirme, derecelendirme, destek hizmeti alımı, bağımsız denetim ve diğer hizmet alımlarına yönelik işlemleri kapsamında yapacakları bilgi paylaşımları da yine veri paylaşılacak hallerden biri olarak sayılmıştır. Söz konusu paylaşım imkanları ile sır saklama yükümlülüğü kapsamında tutulan hallere ilişkin daha detaylı ve geniş kapsamlı hükümlere, Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik içerisinde yer verilmiştir.

Banka sırları ve müşteri sırları olarak kabul edilen verilerin paylaşımına ilişkin yukarıda çerçevesi çizilen kurallar yurtdışına yapılacak veri aktarımlarını da kapsamaktadır. Ancak bankaların müşteri sırrı ya da bankacılık sırrı teşkil etmeyen verileri hakkında, Bankacılık Kanunu kapsamında yurtiçindeki ya da yurtdışındaki kişilerle paylaşımına dair bir sınırlama öngörülmemiştir.

Bankacılık faaliyetlerine ilişkin yürürlüğe konmuş olan ikincil mevzuat ile getirilen bir diğer önemli kural, bankaların birincil ve ikincil sistemlerinin yurtdışında bulundurulması zorunluluğudur. Söz konusu zorunluluk Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik<sup>795</sup> m. 11/4 ile

---

<sup>794</sup> Türkiye Bankalar Birliği Risk Merkezi için bkz. “Türkiye Bankalar Birliği Risk Merkezi”, (11.01.2022), (Çevrimiçi) <https://www.riskmerkezi.org/tr>, 11.01.2022.

<sup>795</sup> “Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik”, (2014), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19864&MevzuatTur=7&MevzuatTertip=5>, 17.10.2021.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik<sup>796</sup> m. 25/1 altında düzenlenmiş durumdadır.

Birincil ve ikincil sistem kavramlarının tanımları, anılan yurtiçinde bulundurma zorunluluğunun kapsamını belirleme konusunda kritiktir. Bu kavramların tanımları, Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik içerisinde mevcuttur. Birincil sistemler; bankacılık faaliyetlerinin yürütülmesini, bankacılık mevzuatı ile ilgili diğer mevzuatta bankalar için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı olarak tanımlanmıştır. İkincil sistemler ise birincil sistemlerin kesilmesi halinde devreye alınacak olan birincil sistem yedekleri olarak tanımlanmıştır<sup>797</sup>. Tanımlardan da anlaşılacağı üzere birincil ve ikincil sistemler hem bilgi sistemi altyapılarını hem de bu sistemlerde mevcut olan verileri kapsamaktadır. Dolayısıyla birincil ve ikincil sistemlerin yurtiçinde saklanması yükümlülüğü aynı zamanda bir veri lokalizasyonu yükümlülüğüdür.

Gerek bankacılık sırları ve müşteri sırlarına ilişkin düzenlemeler gerekse birincil ve ikincil sistemlere ilişkin düzenlemeler, Türkiye’de faaliyet gösteren bankalar açısından oldukça kapsamlı bir veri lokalizasyonu yükümlülüğü bulunduğunu göstermektedir. Buna ek olarak, KVKK’nın aşağıda detayları paylaşılacak yurtdışına kişisel veri aktarımına ilişkin sınırlamalarının bankalara da uygulanacağını vurgulamak gerekmektedir. Bankacılık sektörüne yönelik bu geniş kapsamlı veri lokalizasyonu kurallarının temel amacı, bankaların denetlenebilir olmasını temin

---

<sup>796</sup> “Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik”, (2020), (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=34360&MevzuatTur=7&MevzuatTertip=5>,  
26.05.2020.

<sup>797</sup> Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik m. 25/5 çerçevesinde bankaların, destek hizmetleri de dahil olmak üzere dış hizmet almaları halinde; hizmet sağlayıcıların bilgi sistemleri de birincil ve ikincil sistemlere ilişkin hükümlere tabi şekilde yurtiçinde bulundurulmak zorundadır.

etmektedir<sup>798</sup>. Bu sıkı kuralların aynı zamanda ülkemizdeki bankaların güçlü bilgi sistemi altyapısına sahip olmalarını sağladığı, ülkemizin bilgi teknolojileri alanında gelişmesine ve ülkemizde bir ekosistem oluşmasına katkı sunduğu da açıkça görülmektedir. Buna karşılık sıkı veri lokalizasyonu kurallarının bankaların bazı ticari faaliyetlerini zorlaştırdığını ve aynı zamanda yurtdışı kaynaklı bazı teknolojik gelişmelerden yararlanmalarını imkansızlaştırdığı ya da geciktirdiğini söylemek de kanaatimizce mümkün olabilecektir<sup>799</sup>.

#### **b. Banka Kartları ve Kredi Kartlarına İlişkin İkincil Düzenlemeler**

Ülkemizde banka kartları ve kredi kartlarına ilişkin olarak 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu<sup>800</sup> bulunmaktadır. Bu kanun altında BDDK tarafından Banka Kartları ve Kredi Kartları Hakkında Yönetmelik<sup>801</sup> ile Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ<sup>802</sup> çıkarılmıştır.

Bahse konu tebliğin 5/2 numaralı maddesine göre, Risk Merkezi, bilgi alışverişi kuruluşları ile takas ve mahsuplaşma kuruluşlarının birincil ve ikincil sistemleri yurtiçinde bulundurulmak zorundadır. Banka ve kredi kartlarının çalışabilmesi için gerekli altyapı ve hizmetleri sunan bu kuruluşlara ait birincil sistemler ise faaliyetlerin yürütülmesini ve ilgili düzenlemelerde kuruluşlar için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını

---

<sup>798</sup> Fatih Burak Uzun, “Cloud Computing as an Investment under the ICSID Convention”, **Public and Private International Law Bulletin**, C. 38, S. 2, 2019, s. 522.

<sup>799</sup> Örnek vermek gerekirse henüz Google, Microsoft ve Amazon gibi büyük ölçekli bulut sağlayıcılarının ülkemizde veri merkezleri olmadığı için, bankaların bu şirketlerin sunduğu bulut bilişim hizmetlerinden yararlanmaları mümkün olmamaktadır. Söz konusu durum, Türk bankalarının veri işleme kapasiteleri ile yapay zekâ gibi bir takım yeni teknolojileri kullanmalarını olumsuz olarak etkilemektedir.

<sup>800</sup> “5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu”, 01.03.2006, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5464&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

<sup>801</sup> “Banka Kartları ve Kredi Kartları Hakkında Yönetmelik”, 10.03.2007, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=11180&MevzuatTur=7&MevzuatTertip=5>, 18.10.2021.

<sup>802</sup> “Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ”, (2013), (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2013/12/20131204-9.htm>, 18.10.2021.

sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı olarak yine tebliğ içerisinde tanımlanmıştır. İkincil sistemler ise birincil sistemlerin kesilmesi halinde devreye alınacak olan birincil sistem yedekleri olarak tanımlanmıştır

Adı geçen yönetmeliğin 26/B/5 numaralı maddesi altında ise bilgi alışverişi, takas ve mahsuplaşma kuruluşlarının yedek verilerini yine yurtiçinde tutması gerektiği bir kez daha hüküm altına alınmıştır.

Bankacılık mevzuatına benzer bir şekilde bilgi alışverişi, takas ve mahsuplaşma kuruluşları açısından da verinin saklanması gereken konuma ilişkin veri lokalizasyonu kurallarının mevcut olduğu açıktır. Buna karşılık Bankacılık Kanunu m. 73 içerisinde yer alanlara benzer şekilde veri paylaşımını sınırlayan hükümlere banka kartları ve kredi kartları mevzuatı içerisinde yer verilmediği görülmektedir. Yine banka ve kredi kartları mevzuatı kapsamında kalan verilerin aynı zamanda Bankacılık Kanunu kapsamına girmesi söz konusu olacağından, Bankacılık Kanunu m. 73'teki sınırlamaların aynı zamanda banka ve kredi kartları için de uygulama alanı bulması sonucuna ulaşılabilecektir.

### **c. Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ve İkincil Düzenlemeleri**

Türkiye’de sunulan elektronik para ve ödeme hizmetlerine ilişkin düzenlemelerin başında 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun<sup>803</sup> gelmektedir. Bu kanun kapsamında faaliyet gösterebilecek olan ödeme sistemi işleticilerinin, ödeme kuruluşlarının ve elektronik para kuruluşlarının faaliyetlerinin düzenlenmesi ve denetlenmesi konusunda TCMB<sup>804</sup> yetkili kılınmıştır<sup>805</sup>.

---

<sup>803</sup> “6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun”, 27.06.2013, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6493&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

<sup>804</sup> TCMB’nin açılımı, “Türkiye Cumhuriyet Merkez Bankası” şeklindedir. İnternet sitesi için bkz. “TCMB”, (03.11.2021), (Çevrimiçi) <https://www.tcmb.gov.tr/>, 03.11.2021.

<sup>805</sup> Anılan kanunda 2019 tarihinde yapılan değişiklik öncesinde, ödeme kuruluşları ve elektronik para kuruluşları hakkında düzenleme ve denetleme yetkisi BDDK’ya aittir.

6493 sayılı kanunun 23 numaralı maddesi çerçevesinde ödeme sistemi işleticilerinin, ödeme kuruluşlarının ve elektronik para kuruluşlarının kanun kapsamındaki hususlarla ilgili belge ve kayıtları en az 10 yıl süreyle yurtiçinde saklamaları gerektiği hüküm altına alınmıştır. Buna ek olarak sistem işleticilerinin faaliyetlerini yürütmede kullandıkları bilgi sistemleri ile bunların yedeklerinin yurtiçinde tutulması zorunluluğu da düzenlenmiştir<sup>806</sup>. Kanunun ilk halinde aynı zorunluluk ödeme ve elektronik para kuruluşları için de bulunmaktaysa da 27 Mart 2015 tarihinde yapılan değişiklik<sup>807</sup> ile bu konu BDDK'nın takdir yetkisine bırakılmıştır. 2019 yılındaki değişiklik ile de bu yetki TCMB'ye geçmiştir.

6493 sayılı kanunda mevcut olan yetkiler çerçevesinde ödeme sistemlerine ilişkin olarak 27 Haziran 2014 tarihinde Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ<sup>808</sup> çıkarılmıştır. 27 Mart 2015 tarihinde yapılan kanun değişikliğine rağmen, BDDK tarafından bu tebliğ içerisinde sonraki tarihlerde herhangi bir değişiklik yapılmamıştır. 1 Aralık 2021 tarihinde yayınlanan Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ<sup>809</sup>, önceki tebliği yürürlükten kaldırmıştır.

Anılan eski tebliğin 16. maddesi ile yeni tebliğin 21. Maddesi, ödeme ve elektronik para kuruluşlarının birincil ve ikincil sistemlerini yurtiçinde bulundurmalarını zorunlu

---

<sup>806</sup> 6493 sayılı kanunda mevcut olan yetkiler çerçevesinde ödeme sistemlerine ilişkin olarak Ödeme ve Menkul Kıymet Mutabakat Sistemlerinin Faaliyetleri Hakkında Yönetmelik çıkarılmıştır. Bu yönetmeliğin 24 numaralı maddesinde de kanuna uygun şekilde sistem işleticilerinin bilgi sistemlerinin ve bunların yedeklerinin yurtiçinde kurulu olması zorunluluğu ifade edilmiştir. Ayrıca yönetmelik, dış hizmet sağlayıcılarının bilgi sistemlerinin ve bunların yedeklerinin de Türkiye'de tutulmasını gerektirmektedir.

<sup>807</sup> “6639 Sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun”, (27.03.2015), (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2015/04/20150415-1.htm>, 10.05.2021.

<sup>808</sup> “Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ”, (18.10.2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19817&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

<sup>809</sup> “Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ”, (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39081&MevzuatTur=9&MevzuatTertip=5>, 15.01.2022.



kılmaktadır. Her iki tebliğde de birincil sistemler, kanunda yer alan hususlarla ilgili bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanıldığı sistemler ile faaliyetlerin yürütülmesinde kullanılan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı olarak tanımlanmıştır. İkincil sistemler ise birincil sistemlerin yedekleri olarak ifade edilmiştir. Tebliğlerin ilgili maddeleri, ayrıca aynı kuruluşun kullanıcıları ya da farklı kuruluşların kullanıcıları arasındaki ödeme işlemlerinin yürütülmesinde kullanılan tüm bilgi sistemleri ve bunların yedeklerinin yurt içinde bulunması esas kılmıştır. Ek olarak kuruluşların dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de yurt içinde tutmak zorundadır.

Sonuç olarak ülkemizde faaliyet gösteren ödeme sistemi işleticileri, elektronik para kuruluşları ve ödeme kuruluşları için kapsamlı veri lokalizasyonu yükümlülükleri bulunduğunu sonucuna varmak mümkündür. 6493 sayılı kanun çerçevesinde verilerin konumuna müdahale edilmiş olmakla beraber, verilerin aktarımına ilişkin herhangi bir sınırlama olmadığı görülmektedir.

#### **d. Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin İkincil Düzenlemeler**

Finansal kiralama, faktoring ve finansman faaliyetleri ülkemizde 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu<sup>810</sup> çerçevesinde yürütülebilmektedir. Anılan kanun, söz konusu faaliyetlerin düzenlenmesi ve denetlenmesi konusunda BDDK'yı yetkilendirmiştir.

Bahse konu kanun çerçevesinde, finansal kiralama, faktöring ve finansman şirketlerinin bilgi sistemlerine ilişkin olarak Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin

---

<sup>810</sup> “6361 Sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu”, 13.12.2012, (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6361&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

Tebliğ<sup>811</sup> çıkarılmıştır. Anılan tebliğin 15 numaralı maddesi, finansal kiralama, faktöring ve finansman şirketlerinin birincil ve ikincil sistemlerini yurtiçinde bulundurma zorunluluğu getirmiştir. Tebliğ içerisinde birincil sistemler, kanunda yer alan hususlarla ilgili bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanıldığı sistemler ile faaliyetlerin yürütülmesinde kullanılan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı olarak tanımlanmıştır. İkincil sistemler de birincil sistemlerin yedekleri olarak ifade edilmiştir. Söz konusu şirketlerin dış hizmet alımları sırasında dış hizmet sağlayıcılar tarafından kullanılan bilgi sistemleri ile bunların yedeklerinin de Türkiye’de tutulması gerekmektedir.

Sonuç olarak ülkemizde faaliyet gösteren finansal kiralama, faktoring ve finansman şirketleri için kapsamlı veri lokalizasyonu yükümlülükleri bulunduğunu sonucuna varmak mümkündür. 6361 sayılı kanun çerçevesinde verilerin konumuna müdahale edilmiş olmakla beraber, verilerin aktarımına ilişkin herhangi bir sınırlama olmadığı görülmektedir.

#### **e. Sermaye Piyasası Kanunu ve İkincil Düzenlemeleri**

6362 sayılı Sermaye Piyasası Kanunu<sup>812</sup>, ülkemizdeki sermaye piyasasını düzenlemek amacıyla çıkarılmıştır. Bu kanun ile kurulan SPK<sup>813</sup>, sermaye piyasalarının düzenlenmesi ve denetlenmesi konusunda yetkilendirilmiş durumdadır.

6362 sayılı kanun ile verilen yetkiler doğrultusunda SPK tarafından 5 Ocak 2018 tarihinde Bilgi Sistemleri Yönetimi Tebliği (VII-128.9)<sup>814</sup> çıkarılmıştır. Bu tebliğin 26

---

<sup>811</sup> “Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ”, (2019), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=31395&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

<sup>812</sup> “6362 Sayılı Sermaye Piyasası Kanunu”, 30.12.2012, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6362&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

<sup>813</sup> SPK’nin açılımı, “Sermaye Piyasası Kurulu” şeklindedir. İnternet sitesi için bkz. “SPK”, (03.11.2021), (Çevrimiçi) <https://www.spk.gov.tr/>, 03.11.2021.

<sup>814</sup> “Bilgi Sistemleri Yönetimi Tebliği (VII-128.9)”, (2018), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=24296&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

numaralı maddesi ile tebliğ kapsamına girenlerin birincil ve ikincil sistemlerini Türkiye’de tutmaları zorunlu kılınmıştır. Tebliğ, birincil sistem kavramını kanundan ve kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerin yerine getirilmesi için gerekli bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı olarak tanımlamıştır. İkincil sistemler ise birincil sistemlerin yedekleri olarak ifade edilmiştir.

Birincil ve ikincil sistemlerin yurtiçinde tutulmasına ilişkin zorunluluğa tabi olan kişiler; Borsa İstanbul A.Ş., borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri, emeklilik yatırım fonları, İstanbul Takas ve Saklama Bankası A.Ş., Merkezi Kayıt Kuruluşu A.Ş., portföy saklayıcısı kuruluşlar, Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş., sermaye piyasası kurumları, Türkiye Sermaye Piyasaları Birliği ve Türkiye Değerleme Uzmanları Birliği olarak tebliğ içerisinde sayılmıştır.

Anılan tebliğ kapsamına halka açık ortaklıklar da girmektedir. Ancak SPK tarafından yayımlanan i-SPK.62.1 (01.03.2018 tarihli ve 9/327 s.k.) sayılı İlke Kararı<sup>815</sup> ile halka açık ortaklıkların bilgi sistemlerine bağımsız denetim yaptırma zorunlulukları olmadığı hatırlatılarak birincil sistemlerini de şimdilik yurtiçinde bulundurma mecburiyetine tabi olmadıkları ifade edilmiştir. Bu muafiyet, halka açık ortaklıkların bilgi sistemlerine bağımsız denetim yaptırımlarının SPK tarafından zorunlu kılınacağı belirsiz bir tarihe kadar tanınmıştır.

Netice olarak mevcut durumda sermaye piyasasının işleyişine ilişkin kuruluşlar hakkında kapsamlı veri lokalizasyonu yükümlülüğü bulunduğu sonucuna varmak mümkündür. Ancak bu kuruluşların sayısı az olduğu için önemli ölçüde etki doğuracak bir veri lokalizasyonu yükümlülüğünden bahsetmek kanaatimizce mümkün olmayacaktır. Öte yandan veri lokalizasyonu yükümlülüğünün halka açık ortaklıklara

---

<sup>815</sup> “Sermaye Piyasası Kurulu Bülteni”, Sermaye Piyasası Kurulu, 08.03.2018, (Çevrimiçi) <https://spk.gov.tr/Bulten/Goster?year=2018&no=10&year=2018&no=10>, 05.05.2021.

da getirilmesi halinde, kanaatimizce çok kapsamlı bir veri lokalizasyonu yükümlülüğünden bahsedilebilecektir. Zira halka açık ortaklıklar ülkemizin en büyük ve önemli şirketleridir. Bunların içinde bulunduğu ulusal ve uluslararası ticari ilişkilerin, veri lokalizasyonu yükümlülüğünden etkilenecek olması; aynı zamanda ülke ekonomisinin de bu yükümlülükten etkileneceği anlamına gelecektir.

#### **f. Sigortacılığa İlişkin İkincil Düzenlemeler**

5684 sayılı Sigortacılık Kanunu<sup>816</sup> ile düzenlenmekte olan sigortacılık sektörü açısından düzenleyici ve denetleyici kurum olarak SEDDK<sup>817</sup> kurulmuştur. Bu kurum sigortacılık sektörüne ilişkin ikincil mevzuatı yürürlüğe koyma yetkisine sahiptir.

25 Kasım 2021 tarihinde Resmî Gazete’de yayımlanan Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik<sup>818</sup> ile sigortacılık sektöründe faaliyet gösteren şirketler açısından veri lokalizasyonu yükümlülükleri öngörülmüştür. Söz konusu yönetmeliğin 16 numaralı maddesine göre, yönetmelik kapsamındaki kişilerin birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunlu tutulmuştur. Elektronik posta hizmetleri, telekonferans veya video konferans gibi hizmetler ise yurt içinde bulundurma zorunluluğundan istisna tutulmuştur.

Yönetmelik, birincil sistem kavramını sigortacılık ve özel emeklilik faaliyetlerinin yürütülmesi ve kanunda, kanuna ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta yönetmelik kapsamındaki kuruluşlar için tanımlanan esas faaliyet konusuyla ilgili tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istendiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamı şeklinde tanımlamıştır. İkincil sistem kavramı ise yönetmelikte birincil sistemler

---

<sup>816</sup> “5684 Sayılı Sigortacılık Kanunu”, (2007), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5684&MevzuatTur=1&MevzuatTertip=5>, 22.12.2021.

<sup>817</sup> SEDDK’nin açılımı, “Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu” şeklindedir. İnternet sitesi için bkz. “SEDDK”, (03.11.2021), (Çevrimiçi) <https://seddk.gov.tr/>, 03.11.2021.

<sup>818</sup> “Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik”, (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39063&MevzuatTur=7&MevzuatTertip=5>, 29.01.2022.

dışında kalan faaliyetlerin yürütüldüğü sistemler ile tüm sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve kanunda, kanuna ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta sigorta sektöründe faaliyet gösteren kişiler için tanımlanan tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istendiği an erişilmesini sağlayan birincil sistem yedekleri olarak açıklamıştır.

Netice itibarıyla ülkemizde sigorta sektöründe faaliyet gösteren kişiler için kapsamlı veri lokalizasyonu yükümlülükleri bulunduğunu sonucuna varmak mümkündür. Öte yandan bu kişilerin bilgi sistemlerinin ve dolayısıyla verilerinin konumuna ilişkin düzenlemeler mevcut olmasına rağmen, yurtdışına veri aktarımı konusunda herhangi bir özel kısıtlamaya tabi olmadıkları da gözlemlenmektedir.

## **2. Kamu Kurum ve Kuruluşları ile Kritik Altyapılara Yönelik Veri Lokalizasyonu Yükümlülükleri**

Devletin elindeki verilerin güvenliğinin sağlanması milli güvenlik açısından büyük önem arz etmektedir. Bu amaçla, Cumhurbaşkanlığı tarafından 6 Temmuz 2019 tarihinde 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi<sup>819</sup> yayınlanmıştır. Genelgenin son kısmında, genelgenin uygulanmasına dair detayları içeren Bilgi ve İletişim Güvenliği Rehberi<sup>820</sup>,nin CBDDO<sup>821</sup> koordinasyonunda hazırlanacağı beyan edilmiştir. Genelgeye göre tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin bu rehbere uyum sağlaması gerekecektir. Nitekim söz konusu Bilgi ve İletişim Güvenliği Rehberi de 10 Temmuz 2020 tarihinde yayınlanmıştır.

---

<sup>819</sup> 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi.

<sup>820</sup> “Bilgi ve İletişim Güvenliği Rehberi”, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 07.2020, (Çevrimiçi) [https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg\\_rehber.pdf](https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf), 27.06.2021.

<sup>821</sup> CBDDO’nun açılışı, “Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi” şeklindedir. İnternet sitesi için bkz. “CBDDO”, (03.11.2021), (Çevrimiçi) <https://cbddo.gov.tr/>, 03.11.2021.

Genelgenin amacı dijitalleşen altyapıların ve bilgi yönetim sistemlerinin yaygın kullanımının getirdiği güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanmasıdır. Bu amaca yönelik olarak alınacak önlemler genelge ve rehber içerisinde sıralanmıştır.

Genelge m. 1'e göre nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde depolanacaktır. Kritik bilgi ve veriler rehber içerisinde, güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri; kritiklik derecesi rehberde göre 3 olarak hesaplanan varlıkların (yani en kritik) işlediği veriler ve 6698 sayılı KVKK ile tanımlanan özel nitelikli kişisel veriler şeklinde üç kategori olarak tanımlanmıştır.

Genelge m. 3 kapsamında ise kamu kurum ve kuruluşlarına ait verilerin kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç, bulut depolama hizmetlerinde saklanması yasaklamıştır. Her ne kadar buradaki kurum kontrolü ifadesinden ne anlaşılması gerektiği ve yerli hizmet sağlayıcı kavramının yabancı sermayeli olup Türk hukuka göre kurulmuş şirketleri kapsayıp kapsamadığı net değilse de bu kavramlardan yurtdışında bulunan hizmet sağlayıcılarından hizmet alınmasının büyük ölçüde yasaklandığı sonucuna ulaşmak mümkündür. Rehberde ise söz konusu yasağın sadece yukarıda tanımlanan kritik veriler açısından uygulama alanı bulacağı ifade edilmiştir. Dolayısıyla kamu kurum ve kuruluşları için de kritik veriler açısından bilgi sistemi lokalizasyonu yükümlülüğü bulunduğu söylenebilecektir.

Genelgeye göre rehber aynı zamanda kritik altyapı niteliğinde hizmet veren işletmelerde de uygulanacaktır<sup>822</sup>. Ancak bu işletmelerin hangi işletmeleri kapsadığı

---

<sup>822</sup> Kanaatimizce açık bir kanuni dayanak olmadan, sadece bir genelge ile özel hukuk kişilerine de uyulması zorunlu yükümlülükler getirmek, kanaatimizce hukuk tekniğine uygun değildir. Bahse konu

genelgede açıklanmamıştır. Rehberde atıf yapılan Ulusal Siber Güvenlik Stratejisi’ne göre kritik altyapı sektörlerinin elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri sektörleri olduğu belirtilmiştir<sup>823</sup>. Dolayısıyla rehberde ifade edilen bilgi sistemleri lokalizasyonu yükümlülüğünün bu tür işletmeler açısından da uygulanacağı sonucuna varılabilmektedir.

Genelge ve rehberde açıklanan bilgi sistemleri lokalizasyonu yükümlülüğü, aynı zamanda bir veri lokalizasyonu yükümlülüğü teşkil etmektedir. Gerekli durumlarda ilgili mevzuat çerçevesinde veri aktarımı mümkün olabilecekse de genelge ve rehber, verilerin de yurtiçinde saklanması, söz konusu bilgi sistemleri lokalizasyonu yükümlülüğü vasıtasıyla gerektirmektedir.

### **3. Telekomünikasyon Sektörüne Yönelik Veri Lokalizasyonu Yükümlülükleri**

Telekomünikasyon sektörü ülkemizde 5809 sayılı Elektronik Haberleşme Kanunu<sup>824</sup> ile düzenlenmektedir. 2000 yılında kurulmasına rağmen bu kanun ile son şekli verilen BTK<sup>825</sup>, telekomünikasyon sektörünü düzenleme ve denetleme ile yetkili ve görevli kılınmıştır. BTK’nın görev ve yetkisi sadece elektronik haberleşme altyapısına ve hizmetlerine (örneğin internet altyapısı ve tarifeler, cep telefonu ya da sabit telefon hatları ve tarifeleri) ilişkindir. Buna karşılık internet üzerinde çalışan ürün ve hizmetlerle<sup>826</sup> ilgili olarak 5809 sayılı kanun çerçevesinde BTK’nın herhangi bir yetkisi ya da görevi bulunmamaktadır.

---

yükümlülüklerin bir kanun ile getirilmesi, hukuk tekniği açısından daha uygun olacaktır. Genelge kapsamındaki geniş yükümlülükler getirmek uygun olmayacaktır. Bu tür yükümlülüklerin kanunlarla getirilmesi yerinde olacaktır.

<sup>823</sup> “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020- 2023”, s. 9.

<sup>824</sup> “5809 Sayılı Elektronik Haberleşme Kanunu”, 10.11.2008, (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>, 30.06.2021.

<sup>825</sup> BTK’nın açılımı, “Bilgi Teknolojileri ve İletişim Kurumu” şeklindedir. İnternet sitesi için bkz. “BTK”, (03.11.2021), (Çevrimiçi) <https://www.btk.gov.tr/>, 03.11.2021.

<sup>826</sup> Over-the-Top (OTT) hizmetler olarak adlandırılan bu hizmet türünün tanımı, internet servis sağlayıcıların (örneğin Türk Telekom) sunduğu altyapı vasıtasıyla erişilebilen çevrimiçi uygulama ve hizmetler olarak yapılmaktadır (“Consultation Paper on Regulatory Framework for Over-the-top (OTT) Services”, New Delhi, Telecom Regulatory Authority of India, 18.11.2018, s. 5, (Çevrimiçi) [https://www.trai.gov.in/sites/default/files/CPOTT12112018\\_0.pdf](https://www.trai.gov.in/sites/default/files/CPOTT12112018_0.pdf), 11.10.2022). Sosyal medya mecraları, video siteleri veya mesajlaşma uygulamaları gibi pek çok örnek gösterilebilmektedir.

BTK tarafından çıkarılan iki kararda, değişik konularda veri lokalizasyonu yükümlülükleri öngörülmüştür. Bunlar haricinde GSM operatörü olan işletmecilerle yapılan imtiyaz sözleşmeleri içerisinde de veri lokalizasyonuna yönelik hükümler bulunması ihtimali bulunmaktadır. Ancak bu sözleşmeler kamuya açık olmadığı için kesin olarak bilinmesi imkân dahilinde değildir.

BTK'nın 22.01.2018 tarihli ve 2018/DK-YED/27 sayılı 112 tabanlı araç içi acil çağrı sistemlerine (e-call) ilişkin kararı<sup>827</sup> mevcuttur. Bu karar ile araçlar içerisine yerleştirilen acil çağrı sistemlerinin (örneğin bir otomobilin acil bir durum halinde 112'yi arayabilmesine ilişkin teknik donanımlar) tabi olacağı kurallar düzenlenmiştir. Söz konusu kararın 3 numaralı maddesi ile acil çağrı sistemleri ile bu sistemlerle birlikte katma değerli hizmetler sunulmasına imkân sağlayan haberleşme sistemlerine hizmet verecek bilgi sistemlerinin ülkemiz sınırları içerisinde bulundurulması zorunluluğu getirilmiştir.

BTK'nın 12.02.2019 tarihli ve 2019/DK-TED/053 sayılı uzaktan programlanabilir SIM teknolojilerine (eSIM) ilişkin kararı<sup>828</sup> yukarıda bahsedilen kararlardan ikincisidir. Uzaktan programlanabilir SIM teknolojisi, genellikle GSM operatörlerinden alınan plastik SIM kartları yerine bir elektronik çipin kullanılması anlamına gelmektedir. Bu çip sayesinde kullanıcı plastik SIM kart kullanımı ihtiyacı duymaksızın GSM hizmetlerinden yararlanabilmektedir. Ayrıca GSM operatörünü değiştirmek istediğinde de yeni bir SIM karta ihtiyaç duymamakta, mevcut çip uzaktan yeniden programlanarak yeni GSM operatörü ile çalışabilir hale gelmektedir. eSIM teknolojileri özellikle akıllı telefonlarda ve kendi kendine internete bağlanabilen akıllı araçlarda (örneğin buzdolabı ya da otomobil gibi) kullanılmaktadır. Anılan BTK kararı

---

<sup>827</sup> “Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2018/DK-YED/27”, 22.01.2018, (Çevrimiçi) <https://www.btk.gov.tr/uploads/boarddecisions/112-tabanlı-arac-ici-acil-cagri-sistemi-e-call/027-05-112-tabanlı-arac-ici-acil-cagri-sistemi-e-call-22-01-2018.pdf>, 05.06.2021.

<sup>828</sup> “Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2019/DK-TED/053”, 12.02.2019, (Çevrimiçi) <https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf>, 05.06.2021.



kapsamında eSIM teknolojilerine ilişkin veri ve sistemlerin<sup>829</sup> Türkiye sınırları içerisinde tutulması gerekmektedir.

Netice itibarıyla telekomünikasyon sektörü içerisinde geniş kapsamlı bir veri lokalizasyonu yükümlülüğünden bahsetmek, kanaatimizce mümkün değildir. Buna karşılık BTK'nın milli güvenlik ve hizmet kalitesinin sağlanması gibi hususlarla sınırlı alanlarda veri lokalizasyonu yükümlülükleri getirdiği görülmektedir.

#### 4. Fatura ve Ticari Defterlere Yönelik Veri Lokalizasyonu Yükümlülükleri

İnternet ve bilişim teknolojilerinin gelişmesine bağlı olarak daha önceden kâğıt üzerinde yapılan işlemlerin elektronik ortama taşınması yani dijitalleşme çalışmaları başlamıştır. Bu çalışmalar kapsamında faturaların ve ticari defterlerin de dijital ortama taşınabilmesi amacıyla Türk Ticaret Kanunu'na uygun şekilde Elektronik Defter Genel Tebliği (Sıra No:1)<sup>830</sup>; Vergi Usul Kanunu'na uygun şekilde de Vergi Usul Kanunu Genel Tebliği (Sıra No: 509)<sup>831</sup> çıkarılmıştır.

Elektronik Defter Genel Tebliği (Sıra No:1) ile yevmiye defteri, defteri kebir, envanter defteri, karar ve işletme defterinin elektronik ortama taşınmasına ilişkin usul ve esasları düzenlemektedir. Anılan tebliğin 4.4.1.d numaralı maddesine göre defter ve berat dosyalarının Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde yerine getirilmesi zorunludur. Ancak madde içerisinde, dosyaların yurtdışında muhafaza edilmesi, muhafaza ve ibraz

<sup>829</sup> BTK kararının ilgili 2 numaralı maddesi şu şekildedir: "... 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 birimleri ...".

<sup>830</sup> "Elektronik Defter Genel Tebliği (Sıra No:1)", (17.07.2020), (Çevrimiçi) <https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=15570&mevzuatTur=Tebliğ&mevzuatTertip=5,17.07.2020>.

<sup>831</sup> "Vergi Usul Kanunu Genel Tebliği (Sıra No:509)", s. 509, (18.07.2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=33905&mevzuatTur=Tebliğ&mevzuatTertip=5,18.07.2021>.

zorunluluğunu ortadan kaldırmayacağı ifade olduğu için dosyaların bir kopyası yurtiçinde bulunduğu sürece, ilgili dosyaları yurtdışına aktarmanın yasak olmadığı sonucuna ulaşılmaktadır.

Vergi Usul Kanunu Genel Tebliği (Sıra No: 509) ise kâğıt olarak basılan ve kesilen faturaların elektronik ortama taşınmasına yönelik usul ve esasları düzenlemektedir. Anılan tebliğin VI numaralı maddesi altında tebliğ kapsamında düzenlenen tüm elektronik belgeler için muhafaza ve ibraz yükümlülükleri hüküm altına alınmıştır. Bu madde çerçevesinde söz konusu belgelerin Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti kanunlarının geçerli olduğu yerlerde saklanması gerektiği belirtilmiştir. Ek olarak bu zorunluluğun, yurtdışında söz konusu belgelerin yedeklerinin saklanmasına engel teşkil etmeyeceğini ifade edilerek bahse konu belgelerin yurtdışına aktarımının yasak olmadığı da açıkça belirtilmiştir.

Her iki tebliğ içerisinde yer alan veri lokalizasyonu yükümlülüklerinin esas olarak bahse konu belgelerin muhafaza ve ibraz yükümlülüğünü güçlendirme amacını taşıdığını söylemek mümkündür. Zira söz konusu veri lokalizasyonu yükümlülükleri, belgelerin bir kopyasının yurtiçinde saklanmasını temin ederek gerektiğinde adli ve idari makamların bu belgelere erişebilmesini güvence altına almaktadır. Öte yandan ise bu verilerin yurtdışına çıkarılmasını tamamen yasaklamayarak belge sahiplerine ihtiyaçlarına göre yurtdışına aktarım imkânı vermektedir. Kanaatimizce bu yaklaşım son derece dengeli ve doğrudur.

## **5. Elektrikli Skuterlere Yönelik Veri Lokalizasyonu Yükümlülüğü**

14 Nisan 2021 tarihli Elektrikli Skuter Yönetmeliği<sup>832</sup>, paylaşımlı elektrikli skuter işletmeciliği faaliyetlerini düzenlemek ve geliştirmek amacıyla yürürlüğe konmuştur. Anılan yönetmeliğin 8/c numaralı maddesi, elektrikli skuter işletmeciliği faaliyetinde bulunmak isteyen kişilerin, söz konusu faaliyetlere ilişkin verilerin tutulacağı veri

---

<sup>832</sup> “Elektrikli Skuter Yönetmeliği”, Resmi Gazete, 14.04.2021, (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2021/04/20210414-3.htm>, 23.05.2021.

tabanının saklanacağı sunucuları Türkiye Cumhuriyeti sınırları içerisinde barındırmasını gerektirmektedir.

Anılan yükümlülük, elektrikli skuter işletmecilerinin bilgi sistemleri açısından lokalizasyon yükümlülüğüne tabi tutulduğunu göstermektedir. Aynı zamanda bu işletmecilerin verileri yurtiçinde bulunan sunucularda saklamak zorunda olmaları, işletmeciler açısından veri lokalizasyonu yükümlülüğü bulunduğunu da göstermektedir. Buna karşın söz konusu işletmecilerin verileri yurtdışındaki kişilerle paylaşımları yönünde, yönetmelik çerçevesinde herhangi bir engel olmadığı düşünülmektedir.

## **6. Sosyal Ağ Sağlayıcılarının Veri Lokalizasyonunu Sağlamaya Yönelik Tedbirler Alma Yükümlülüğü**

Ülkemizde internet ortamında bulunan içeriklere ilişkin hukuki kurallar, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun<sup>833</sup> içerisinde bulunmaktadır. Bu kanun ve ikincil düzenlemeleri, erişim engelleme ve içerik kaldırma konularına ilişkin usul ve esasları belirlemektedir.

29 Temmuz 2020 tarihinde 7253 sayılı kanun<sup>834</sup> ile yapılan değişiklikler neticesinde, 5651 sayılı kanun içerisine sosyal ağ sağlayıcı tanımı eklenmiştir. Bu tanıma göre sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişiler, sosyal ağ sağlayıcı olarak adlandırılmaktadır. Örneğin **Facebook, Instagram, Twitter** ya da **Tiktok** gibi şirketler, söz konusu tanım çerçevesinde sosyal ağ sağlayıcı olarak kabul edilmektedir.

<sup>833</sup> “5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”, 16.08.2021, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5>.

<sup>834</sup> “İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun”, (29.07.2020), (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>.

5651 sayılı kanunun ek m. 4/5'ine göre Türkiye'den günlük erişimi bir milyondan fazla yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcıların, Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alma yükümlülüğü bulunmaktadır. Konuya ilişkin olarak BTK'nın 29 Eylül 2020 tarihli, 2020/DK-İD/274 sayılı, Sosyal Ağ Sağlayıcı Hakkında Usul ve Esaslar<sup>835</sup> başlıklı bir karar yayınlanmıştır. Bu kararın 12 numaralı maddesi ise veri lokalizasyonu açısından temel kullanıcı bilgileri ile BTK tarafından bildirilebilecek hususlara ilişkin verilerin Türkiye'de barındırılması yönünde gerekli tedbirlerin alınmasına öncelik verilmesi gerektiğini hüküm altına almıştır. Aynı zamanda veri lokalizasyonuna ilişkin tedbirler açısından sosyal ağ sağlayıcıların BTK'ya her altı ayda bir bilgi vermeleri gerekmektedir.

Çalışmamızın tarihi itibarıyla herhangi bir sosyal ağ sağlayıcının veri lokalizasyonu konusunda aldığı tedbirlere ilişkin olarak kamuya açık herhangi bir bilgi bulunmamaktadır.

Yukarıda açıklanan verilerin Türkiye'de barındırılmasına gerekli tedbirlerin alınması kuralının bir veri lokalizasyonu yükümlülüğü olarak değerlendirilip değerlendirilemeyeceği kanaatimizce net değildir. Diğer veri lokalizasyonu yükümlülüklerinde açıkça verilerin ülke içerisinde tutulması gerektiği ifade edilirken, 5651 sayılı kanunda bu yönde gerekli tedbirlerin alınması gerektiği ifade edilmiştir. Bu tedbirlerin neler olduğu, ne derecede alınmak zorunda olduğu veya tedbirlerin tamamlanması halinde verilerin artık yurtiçinde mi saklanması gerekeceği gibi konular tamamen belirsizdir. O halde düşüncemize göre bu hükmü, mevcut hali ile bir veri lokalizasyonu olarak değerlendirmek doğru olmayacaktır. Söz konusu hüküm gelecekte getirilmesi planlanan kesin ve kapsamı net veri lokalizasyonu yükümlülüğü için bir hazırlık dönemi öngörmesi açısından getirildiğini söylemek, kanaatimizce yerinde olacaktır.

---

<sup>835</sup> “Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2020/DK-İD/274”, 29.09.2020, (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2020/10/20201002-5.pdf>, 20.10.2021.

## 7. Kişisel Verilere Dair De Facto Veri Lokalizasyonu Yükümlülüğü

Kişisel verilerin korunmasına dair ülkemizdeki temel kanun, 6698 sayılı KVKK'dır. Bu kanun ile kişisel verilerin korunması konusunda düzenleyici ve denetleyici kurum ve kurul olarak Kişisel Verileri Koruma Kurulu ve Kurumu<sup>836</sup> kurulmuştur.

KVKK'nın 9 numaralı maddesi kişisel verilerin yurtdışına aktarımını düzenlemektedir. Bu madde kapsamında kişisel verilerin yurtdışına aktarılması için üç farklı imkân tanınmıştır. Bunlar sırasıyla ilgili kişinin açık rızasının alınması, Kişisel Verileri Koruma Kurulu tarafından yeterli korumayı sağladığı ilan edilen ülkelere kişisel verilerin herhangi bir ek işleme ihtiyaç olmaksızın aktarılması ya da Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt ederek Kişisel Verileri Koruma Kurulundan izin almalarıdır<sup>837</sup>.

KVKK'da sayılan bu üç imkân, kanunun yayınlanıp yürürlüğe girdiği 2016 tarihinden beri pratikte uygulanabilir çözümler üretmekten uzaktır. Şöyle ki işbu çalışma tarihi itibarıyla Kişisel Verileri Koruma Kurum tarafından verilen, herhangi bir ülkenin yeterli korumayı sağladığına dair bir karar bulunmamaktadır. Bu nedenle Kişisel Verileri Koruma Kurumu'nun tüm yabancı ülkelerin yetersiz koruma sağladığını kabul ettiği sonucuna varılmaktadır. Dolayısıyla söz konusu yurtdışına kişisel veri aktarma imkânı uygulamada kullanılamamaktadır.

İkinci kişisel veri aktarımı imkânı olan veri sorumlularının<sup>838</sup> kişisel verilere ilişkin yeterli korumayı taahhüt ederek Kişisel Verileri Koruma Kurumu'na izin başvurusunda bulunmaları da hızlı çözümler gerektiren pratik ihtiyaçlara bir çare

---

<sup>836</sup> Kişisel Verileri Koruma Kurumu'nun internet sitesi için bkz. "Kişisel Verilerin Korunması Kurumu", **KVKK**, (03.11.2021), (Çevrimiçi) <https://www.kvkk.gov.tr/>, 03.11.2021.

<sup>837</sup> Önemle belirtmek gerekir ki kişisel veri işleme faaliyetinin açık rıza gerektirmesi halinde, yurtdışına kişisel veri aktarımı için sadece açık rıza imkânı kullanılabilir. Ancak kişisel veri işleme faaliyeti açık rıza gerektirmiyorsa, yurtdışına kişisel veri aktarımı için her üç imkânın da kullanılması mümkündür.

<sup>838</sup> Her ne kadar KVKK m.9'un lafzı sadece veri sorumlularını kapsamaktaysa da Kişisel Verileri Koruma Kurulu, veri sorumlusundan veri işleyene yapılan aktarımları da bu kapsamda değerlendirmektedir (Şehriban İpek Aşıkoğlu, Fatih Burak Uzun, "Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri", **Prof. Dr. Türkan Rado'nun Anısına Armağan**, 1.bs, İstanbul, On İki Levha Yayıncılık 2020, s. 927).

olarak kullanılmaya son derece elverişsizdir. Nitekim bu durum, Kişisel Verileri Koruma Kurumu'nun kurulduğu günden işbu çalışma tarihine kadar geçen sürede (yaklaşık 7 yıl) Kişisel Verileri Koruma Kurulu'nun sadece yedi adet başvuruya olumlu şekilde döndüğüne dair kamuoyu duyurusu yapmasından da anlaşılabilmektedir (değerlendirme aşamasında olan ya da reddedilen başvuru sayısı bilinmemektedir). Ayrıca Kişisel Verileri Koruma Kurulu'nun yayınladığı bir duyuru metni<sup>839</sup> ile imzalanacak taahhütnameler hakkında çok sıkı şartlar öngörmesi, değerlendirme süreci kapsamında dikkate alınacak kriterlerin şeffaf olmaması ve kişisel veri aktarımı gerçekleştirilmesinden önce izin alınması gerekmesi ile izin başvurusunun ne kadar sürede sonuçlandırılacağına belirsiz olması gibi sebepler söz konusu izin sisteminin uygulamada neden çalışmadığını açıklamaktadır. Örnek vermek gerekirse Türkiye merkezli bir havayolu şirketinin herhangi bir ülkeye uçuş yapabilmesi için Kişisel Verileri Koruma Kurulundan uçuşlara başlamadan önce uçağı ülkeye kişisel veri aktarımı izni alması gerekmektedir. Bunun için ilgili şirket öncelikle uçağı ülkede kişisel veri aktarımı yapması gerekecek muhataplarını tespit etmeli; bu muhataplara Kişisel Verileri Koruma Kurulu tarafından yayınlanan standart sözleşmeleri herhangi bir değişiklik kabul etmeden imzalatmalı ve daha sonra Kişisel Verileri Koruma Kurulu'na başvurarak belirsiz bir süre boyunca (sürecin birkaç yıl alabileceğı de kanaatimizce son derece olasıdır) beklemeli ve sonrasında olumlu yanıt alabilirse uçuşlarına başlamalıdır. Bu havayolu şirketinin tüm uçuş yapılacak ülkeler için ve bu ülkelerde veri aktarımı yapması gereken veri sorumlusu sayısı kadar söz konusu izin prosedürünü tekrarlaması gerekmektedir<sup>840</sup>.

Ayrıca bu izin sürecinin yurtdışına kişisel veri aktarımı yapan ülkemizdeki tüm veri sorumluları için de bulunduğu ve tüm bu kişilerin de Kişisel Verileri Koruma Kurulu'na başvurması gerektiğı göz önüne alındığında Kişisel Verileri Koruma

---

<sup>839</sup> “Yurtdışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru”, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISSEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU>, 28.05.2020.

<sup>840</sup> Aşkoğlu, Uzun, “Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri”, s. 928.

Kurulu'nun izin değerlendirme süresinin çok fazla uzayabileceği sonucuna da ulaşabilmektedir.

Kişisel Verileri Koruma Kurulu tarafından yayınlanan 3 Eylül 2021 tarihli duyuru ile **WhatsApp**'a yurtdışına kişisel veri aktarımdan dolayı ceza kesildiği ilan edilmiştir<sup>841</sup>. Bu kapsamda yurtdışında yerleşik olan bir veri sorumlusunun direkt olarak Türkiye'deki ilgili kişilerin verilerini toplaması, yurtdışına kişisel veri aktarımı olarak kabul edilmiştir. Kişisel Verileri Koruma Kurumu tarafından yayınlanan taahhütlerin imzalanabilmesinin ancak iki veri sorumlusu ya da bir veri sorumlusu ve bir veri işleyen arasında mümkün olduğu düşünüldüğünde Kişisel Verileri Koruma Kurulu'na izin başvurusu imkanının yurtdışında yerleşik veri sorumlularının Türkiye'deki faaliyetlerini kapsayamayacağı sonucuna varılmaktadır. Zira bu kişilerin yeterli korumayı taahhüt edebilmek için sözleşme imzalayabilecekleri bir veri sorumlusu ya da veri işleyen karşı taraf bulunmamaktadır. Buna rağmen ilgili kişilere yaptırım uygulanmış olması, Kişisel Verileri Koruma Kurulu'nun yurtdışına veri aktarımı aleyhindeki sert tutumunu göstermektedir.

Yukarıdaki tüm açıklamalar birlikte değerlendirildiğinde, veri aktarımı gerçekleştirecek veri sorumluları ya da veri işleyenlerin kişisel verilere ilişkin yeterli korumayı taahhüt ederek Kişisel Verileri Koruma Kurulu'na izin başvurusunda bulunmalarının, uygulamadaki ihtiyaçları karşılamaktan son derece uzak olduğunu ve bu veri aktarım imkânının fiilen çalışmadığını söylemek kanaatimizce mümkündür.

Üçüncü kişisel veri aktarımı imkânı ise kişisel verileri işlenen ilgili kişilerden yurtdışına kişisel veri aktarımı için açık rıza alınmasıdır. Açık rıza alınması fiilen sadece az sayıda ilgili kişinin kişisel verilerini işleyen veri sorumluları için mümkün olabilecektir. Çünkü ancak bu veri sorumlularının az sayıdaki ilgili kişilere ulaşarak rıza talebinde bulunabilmesi mümkündür. Ancak havayolu şirketleri ya da bankalar

---

<sup>841</sup> “WhatsApp Uygulaması Hakkında Yürütülen Resen İncelemeye İlişkin Kamuoyu Duyurusu”, 03.09.2021, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/7045/WHATSAPP-UYGULAMASI-HAKKINDA-YURUTULEN-RESEN-INCELEMAYE-ILISKIN-KAMUOYU-DUYURUSU>, 04.11.2021.

gibi çok daha büyük kitlelere hizmet veren ve dolayısıyla on binlerce ilgili kişinin kişisel verilerini işleyen veri sorumlularının açık rıza alma talebinde bulunabilmeleri dahi mümkün değildir. Söz konusu duruma ek olarak KVKK uygulaması çerçevesinde ilgili kişilerin açık rıza verebilmesi için, ilgili kişilerin hiçbir şekilde zorlanmadan tamamen özgür irade ile hareket ederek ayrı bir beyan ile açık rıza verdiklerini ifade etmeleri gerekmektedir. Bu kapsamda açık rızanın bir mal ya da hizmetten yararlanmaya ilişkin ön şart olarak konumlandırılması da mümkün olmamaktadır. Dolayısıyla önceki bölümde örneğini verdiğimiz havayolu şirketinin, tüm yolcularından açık rıza alabilmesi fiili durumda mümkün olmayacaktır. Çünkü bilet satın almasına rağmen açık rıza vermeyen ya da bilet alırken verdiği açık rızasını geri çeken bir yolcunun kişisel verilerinin varılacak ülkeye aktarılması 6698 sayılı kanunun ihlali anlamına gelecektir. Ancak bilet satışı nedeniyle ifa edilmesi gereken taşıma borcunun akıbeti ilgili havayolu şirketinin başka hukuka aykırılıklar ile karşılaşmasına sebep olabilecek niteliktedir. Dolayısıyla açık rızanın, kişisel verilerin yurtdışına aktarımı konusunda güvenilir ve uygulanabilir bir imkân olmadığı kanaatimizce açıktır.

Yukarıda yer alan açıklamalardan da anlaşılabileceği üzere KVKK çerçevesinde kişisel verilerin yurtdışına aktarılması için tanınan üç imkanının her biri uygulanabilir ve sürdürülebilir şekilde işlev gösterememektedir. Bu durum kişisel verilerin yurtdışına aktarılmasını hukuki olarak zorlaştırmakta, hatta çoğu durumda imkânsız hale getirmektedir. İşte bu nedenle kanaatimizce KVKK'nın **de facto** olarak kişisel veriler açısından veri lokalizasyonu yükümlülüğü getirdiğini söylemek mümkündür. Zira kanunun getirdiği imkanlardan birini kullanmak haricinde kişisel verilerin yurtdışına aktarımı hukuka aykırıdır ve kanunun getirdiği imkanlar sağlıklı bir kişisel veri akışı kurulmasına imkân vermemektedir. Çalışmamızın tarihi itibarıyla gündemde olan KVKK'nın güncelleştirilmesi süreci çerçevesinde yeni getirilecek düzenlemelerle söz konusu veri lokalizasyonu yükümlülüğünün ortadan kalkması da söz konusu olabilecektir.

Veri lokalizasyonu getiren mevzuatı inceleyen diğer başlıklar belirli sektörlerle ya da özel konulara ilişkindir. Ancak kişisel verilere dair uygulanmakta olan **de facto** veri



lokalizasyonu yükümlülüğü herhangi bir sektör ya da alan fark etmeksizin genel olarak herkese uygulanmaktadır. İlaveten KVKK'nın genel kanun niteliği sebebiyle kişisel veri içeren tüm durumlara uygulanması da (yine ilgili diğer kanun hükümleri saklı kalmak kaydıyla) söz konusu olmaktadır. Bu nedenlerle anılan veri lokalizasyonu yükümlülüğünün kapsamı çok daha geniştir. **De facto** veri lokalizasyonu yükümlülüğünün sert bir şekilde uygulanması halinde ticari faaliyetlerin, kamu hizmetlerinin ve bireylerin günlük hayatlarının ciddi şekilde aksamalarla karşılaşacağını söylemek kanaatimizce uygun olmaktadır. İşte bu nedenle, mehz AB düzenlemelerine de uygun olarak KVKK'da yer alan kişisel veri aktarımı imkanlarının genişletilmesi gerektiği düşünülmektedir.

## **B. Çeşitli Ülkelerin Veri Lokalizasyonu Yükümlülüğü Getiren Hukuki Düzenlemeleri**

Veri lokalizasyonu yükümlülüğü getiren hukuki kurallar sadece ülkemize has değildir. Dünyanın pek çok yerinde bu tür kurallar bulunmaktadır. Söz konusu kuralların getirilme gerekçelerine önceki bölümlerde değinilmiş olmasına rağmen, veri lokalizasyonu yükümlülüklerine ilişkin olarak ülkelerin siyasi, ekonomik ve coğrafi durumlarına göre farklı yaklaşımlar benimsendiği ifade etmek yerinde olacaktır. Örnek vermek gerekirse internet ve teknoloji alanında ekonomik olarak hakimiyet kurmuş olan ABD, veri lokalizasyonu yükümlülükleri getirmemekte ve diğer ülkelerin bu konudaki yaklaşımlarını engellemeye çalışmaktadır. Buna karşılık Çin ve Rusya'da ise veri lokalizasyonu yükümlülüğü hem ABD'ye karşı bir güvenlik meselesi olarak ele alınmakta hem de ekonomik kalkınmanın bir aracı olarak kullanılmaktadır. Veri lokalizasyonu yükümlülükleri yanında ülke politikalarına ilişkin bu tür açıklamalara aşağıdaki başlıklar altında yer verilmeye çalışılacaktır. Söz konusu örnek ülke incelemeleri, dünyanın değişik yerlerindeki ülkelerin benzer sorunlara getirdiği farklı bakış açıları içeren çözümleri göstermeleri bakımından da önemlidir.

## 1. Batı Bloğu Ülkelerinde Veri Lokalizasyonu Yükümlülükleri

### a. Avrupa Birliği

#### (1) AB Nezdinde Veri Lokalizasyonu Yaklaşımı

AB, İkinci Dünya Savaşı ardından doğu ve batı olarak ikiye bölünen Avrupa'nın batı tarafında, ekonomik bir birlik olarak kurulmuştur. Daha sonraları AB, Avrupa'daki hemen hemen tüm ülkelerin devletlerin ile genişlemiştir. Kuruluş aşamalarındaki ekonomik birlik yaklaşımı da zaman içerisinde genişleyerek siyasi alanlardaki konuları da içerir hale gelmiştir. Üye ülkeler arasında mal ve hizmetlerin serbestçe dolaşımını sağlamaya odaklanmış olan AB, aynı zamanda dünyanın en büyük pazarlarından birisidir<sup>842</sup>. Bu nedenle başta ABD ve Çin olmak üzere yabancıların ticaret ve yatırım faaliyetlerinin önemli bir kısmı AB ile ilişkili olmaktadır<sup>843</sup>.

Teknoloji alanında yaşanan gelişmeler ve AB'nin dünyanın en önemli pazarlarından birisi olması, AB vatandaşlarının ve şirketlerinin verilerini kıymetli hale getirmiştir. Başta büyük bulut hizmeti sağlayıcıları, sosyal medya şirketleri ve e-ticaret şirketleri olmak üzere birçok tacir, AB'ye ilişkin verilere ilgi duymakta ve bunların ekonomik değerinden faydalanmak istemektedir. Özellikle bu tür şirketlerin AB dışından olması, AB içerisinden bunlara rakip şirketler çıkarılamaması ile ABD'nin istihbarat faaliyetleri, AB'nin AB'deki veriler açısından çeşitli çalışmalar yapmasına sebebiyet vermiştir<sup>844</sup>.

---

<sup>842</sup> “EU Position in World Trade - Trade - European Commission”, 09.02.2019, (Çevrimiçi) <https://ec.europa.eu/trade/policy/eu-position-in-world-trade/>, 12.10.2021.

<sup>843</sup> a.y.

<sup>844</sup> Hon vd., “Policy, Legal and Regulatory Implications of a Europe-Only Cloud”, s. 256; Tian, “Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement”, s. 384; “European Digital Infrastructure and Data Sovereignty - A Policy Perspective”, EIT Digital, 2020, s. 6, (Çevrimiçi) <https://www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/full-report/EIT-Digital-Data-Sovereignty-Full-Report.pdf>, 12.02.2022; Madiega, “Digital Sovereignty for Europe”, s. 3; “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”, s. 4.

Bu çalışmalardan ilki, her ne kadar temel hak ve özgürlüklerden olan özel hayatın ve kişisel verilerin gizliliğinin korunması amaçlanmış da olsa, GDPR'ın yürürlüğe alınmasıdır. GDPR vasıtasıyla AB'de bulunan kişilerin kişisel verilerinin işlenmesine ve AB dışına aktarımına ciddi sınırlamalar getirilmiş ve bu verilerin güvende tutulması yönünde hukuki yükümlülükler belirlenmiştir. Bu kapsamda AB sınırları içerisinde bulunan verilerin AB dışındaki kamu otoriteleri dahil üçüncü kişilerle, söz konusu yükümlülüklerle aykırı şekilde paylaşılması da yasaklanmış olmaktadır<sup>845</sup>. GDPR aynı zamanda kişisel verilerin AB içerisinde serbest dolaşımı imkanının sınırlandırılmasını da engellemektedir.

İkinci olarak, Kişisel Olmayan Verilerin Serbest Akışı Regülasyonu<sup>846</sup> ile AB üyesi devletlerin birbirleri aleyhinde veri lokalizasyonu yükümlülüğü getirmeleri yasaklanmıştır. Buna karşılık AB dışındaki ülkeler açısından veri lokalizasyonu yükümlülüğü getirilmesi yönünde herhangi bir engel bulunmamaktadır.

Yukarıda sayılan mevzuatın yürürlüğe sokulması yanında AB tarafından 19 Şubat 2020 tarihinde Avrupa Veri Stratejisi<sup>847</sup> belgesi yayınlanmıştır. Bu belge içerisinde verilerin AB sınırları içerisinde saklanması ve işlenmesi için gerekli çalışmaların yapılması gerektiği; ancak AB sınırları içerisinde veri saklama ve işlemenin kanuni bir zorunluluktan değil; gönüllü tercihlere dayalı olarak yapılması hedeflendiği ifade edilmektedir<sup>848</sup>. Strateji içerisinde AB menşeli bulut hizmet sağlayıcılarının eksikliği sebebiyle ekonomik açıdan dezavantajlar bulunduğu söylenmesinin yanı sıra verilerin konumunun hukuki açıdan da riskler yarattığı belirtilmiştir. Bu riskler,

---

<sup>845</sup> Hon vd., “Policy, Legal and Regulatory Implications of a Europe-Only Cloud”, s. 27; Söz konusu düzenlemenin de bir tür veri lokalizasyonu yükümlülüğü olduğu yönündeki görüş için bkz. Abe Yoshinori, “Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?”, **Policy Research Institute, Ministry of Finance, Japan, Public Policy Review**, S. 5, 2021, s. 2; Söz konusu yükümlülüklerle nasıl uyum sağlanması gerektiğine dair rehber için bkz. Swire, Kennedy-Mayo, “Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data”.

<sup>846</sup> “Shaping Europe’s Digital Future - Free Flow of Non-Personal Data”, **European Commission**, (19.12.2021), (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>, 19.12.2021.

<sup>847</sup> “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”.

<sup>848</sup> **a.g.e.**, s. 4.

verilerin başka bir ülkenin hukukuna tabi olması nedeniyle AB vatandaşlarına yönelik olumsuz durumların (özellikle Çin'in siber güvenlik ve istihbarat yasaları nedeniyle) meydana gelmesi ile diğer ülkelerin hukuk kurallarına dayanarak verilere erişimin AB vatandaşlarının haklarının ihlal edilmesi olarak belirtilmiştir<sup>849</sup>. Ayrıca AB dışındaki bulut hizmet sağlayıcıların, AB hukukuna uyup uymadığının belirsiz olması da bir sorun olarak değerlendirilmiştir<sup>850</sup>. Kanaatimizce burada bahsedilen sorunların tamamı, devletlerin uluslararası yetkisinin veriler üzerinde nasıl kullanılacağı konusuyla ilgilidir.

Strateji içerisinde AB'nin, verilerin hukuki durumu hakkındaki ana ilkesinin; AB'ye mal ve hizmet satan tüm şirketlerin AB mevzuatına uyum sağlaması ile bu uyumun AB dışındaki devletlerin hukuk kuralları nedeniyle zedelenmemesi gerektiği olduğu belirtilmiştir<sup>851</sup>. Dolayısıyla AB'nin, verilerin sadece AB'nin uluslararası yetkisi içerisinde olması gerektiği görüşünde olduğu sonucuna varmak kanaatimizce mümkündür.

Son olarak Strateji Belgesi, AB kaynaklı bulut bilişim sağlayıcılarının ortaya çıkarılmasına yönelik politika, strateji ve teşvikler vasıtasıyla AB verilerinin AB dışına teknik ve altyapısal eksiklikler nedeniyle gitmesinin önüne geçilmesini hedeflemektedir<sup>852</sup>. Bu hedef vasıtasıyla aynı zamanda ABD menşeli bulut şirketlerine karşı AB menşeli bulut şirketlerinin ortaya çıkması amaçlanarak ekonomik kalkınma da sağlanacaktır<sup>853</sup>. AB menşeli bulut şirketlerini ortaya çıkartmak adına AB tarafından, AB'de bulunan ufak ölçekli bulut şirketlerinin katılımı

---

<sup>849</sup> a.g.e., s. 9.

<sup>850</sup> a.y.

<sup>851</sup> a.g.e., s. 14.

<sup>852</sup> "Establishing a Trusted Cloud Europe", Publications Office of the European Union, 2014, s. 9; Madiega, "Digital Sovereignty for Europe", s. 5; "Declaration Building the next generation cloud for businesses and the public sector in the EU", the Informal Video Conference of the Ministers responsible for Telecommunications/Digital Policy, 15.10.2020, s. 3, (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>, 18.03.2021; "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", s. 16.

<sup>853</sup> Hon vd., "Policy, Legal and Regulatory Implications of a Europe-Only Cloud", s. 6; "Establishing a Trusted Cloud Europe", s. 24; Madiega, "Digital Sovereignty for Europe", s. 7.

ile **Gaia-X Projesi**<sup>854</sup> ile **European Alliance for Industrial Data, Edge and Cloud Projesi** başlatılmıştır.<sup>855</sup>

Yukarıda açıklanan unsurların hiçbirisi, bu çalışma anlamında veri lokalizasyonu yükümlülüğü teşkil etmemektedir. Buna karşılık verilerin AB dışına çıkışının kontrolüne ve verilerin AB içerisinde serbest dolaşımını sağlamaya yönelik düzenlemeler, AB'nin veriler üzerindeki uluslararası yetki görüşü, AB menşeli bulut şirketlerinin geliştirilme çabaları birlikte değerlendirildiğinde; AB'nin de genel olarak kendi verileri üzerinde kontrol sahibi olma amacını güttüğü sonucuna varmak mümkündür. Bir başka deyişle AB, veriler üzerinde kendi hukukunun uygulanmasını ve aynı zamanda başka hukukların uygulanmamasını (bu hukuk kuralları vasıtasıyla verilere erişim imkânı doğmaması için) amaçlamaktadır<sup>856</sup>. Bu amaç, aynı zamanda veri lokalizasyonu yükümlülüğü getiren diğer devletlerin de ulaşmaya çalıştığı amaçtır. Yine benzer şekilde AB, bu amaca yönelik verilerin AB sınırları içerisinde depolanmasını ve işlenmesini sağlamak yoluyla ulaşmaya çalışmaktadır. AB'nin diğer devletlerden en önemli farkı, AB'nin veri lokalizasyonunu direkt olarak kanuni bir zorunluluk şeklinde değil; ekonomik ve hukuki kolaylıklar vasıtasıyla gönüllü bir tercih şeklinde getirmeyi hedeflemesidir<sup>857</sup>. AB'nin yaklaşımındaki bu farklılığın görülebilmesi amacıyla AB'ye ilişkin duruma bu bölüm altında yer verilmiştir.

## (2) Bazı AB Ülkelerinde Veri Lokalizasyonu Yükümlülükleri

AB ülkelerinin birçoğunda, çeşitli veri tiplerine ilişkin veri lokalizasyonu yükümlülüğü getiren düzenlemeler bulunmaktadır. Ancak bu veri lokalizasyonu

<sup>854</sup> "What Is Gaia-X?", (Çevrimiçi) <https://www.data-infrastructure.eu/GAIA/Navigation/EN/Home/home.html>, 17.10.2021; Madiega, "Digital Sovereignty for Europe", s. 5; Laurens Cerulus, "Europe's litmus test over cloud computing push", **Politico**, (28.07.2020), (Çevrimiçi) <https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/>, 28.09.2020.

<sup>855</sup> "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", s. 18; "Towards a next generation cloud for Europe | Shaping Europe's digital future", European Commission, (10.11.2021), (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>, 10.11.2021.

<sup>856</sup> Hon vd., "Policy, Legal and Regulatory Implications of a Europe-Only Cloud", s. 28; "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", s. 14.

<sup>857</sup> "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", s. 24.

yükümlülükleri, dünyanın diğer yerlerindeki gibi genel ve kapsayıcı nitelikte değildir. Buna ek olarak Kişisel Olmayan Verilerin Serbest Akışı Regülasyonu'nun uygulanması yaygınlaştıkça bu yükümlülüklerin ya tamamen ortadan kalkacağı ya da sadece AB dışındaki ülkelere karşı etkili olacak şekilde düzenleneceği öngörülmektedir<sup>858</sup>. Yine de aşağıda bazı AB ülkelerinde mevcut bulunan veri lokalizasyonu yükümlülükleri incelenecektir<sup>859</sup>.

Almanya'da federal seviyede yürürlükte bulunan Telekomünikasyon Kanunu'nun 1 Temmuz 2017 tarihinde yürürlüğe giren 113b numaralı maddesi; telefon, mesajlaşma ve internet servislerine ilişkin meta verilerin (telefon numaraları, iletişim süresi, iletişim içeriği, iletişim tarihleri, abone ve cihaz bilgileri ve IP adresleri gibi) Almanya sınırları içerisinde saklanması gerektirmektedir<sup>860</sup>. Bunun yanında Alman Ticaret Kanunu ve Alman vergi mevzuatı, muhasebe verilerinin ve belgelerinin Almanya'da tutulmasını gerektirmektedir<sup>861</sup>. **Brandenburg** Eyaleti ise vatandaşlarının verilerinin sadece eyalet sınırları içerisinde veri merkezi bulunan bulut sağlayıcılarında saklanabileceğini hüküm altına almıştır<sup>862</sup>.

Fransa ve Hollanda'da kamu otoritelerinin tüm verileri, kamu verisi olarak kabul edilmekte olup bu verilerin Fransa ve Hollanda ülke sınırları içerisinde tutulması zorunluluğu mevcuttur<sup>863</sup>. Lüksemburg'da ise finansal kuruluşların verilerini Lüksemburg içerisinde işlenmesi zorunluluğu bulunmaktadır<sup>864</sup>. İsveç Finansal

---

<sup>858</sup> "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union", **Official Journal of the European Union**, 2018, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>, 08.08.2021.

<sup>859</sup> AB ülkelerindeki veri lokalizasyonu yükümlülüklerinin daha detaylı bir listesi için bkz. Moritz Godel, Joshi Alexander, Robert Bond, Jose Manuel Cabello, Daniel Fernandez, **Facilitating Cross Border Data Flow in the Digital Single Market**, European Commission, Directorate-General of Communications Networks, Content & Technology, 2016, s. 11.

<sup>860</sup> Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", s. 42.

<sup>861</sup> Godel vd., **Facilitating Cross Border Data Flow in the Digital Single Market**, s. 14.

<sup>862</sup> Godel vd., **a.y.**

<sup>863</sup> Godel vd., **a.g.e.**, s. 11; Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", European Centre for International Political Economy, 2016, s. 7, (Çevrimiçi) <https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>, 05.04.2022.

<sup>864</sup> Godel vd., **Facilitating Cross Border Data Flow in the Digital Single Market**, s. 15.

Hizmetler Kurumu ise denetlediği tüm kuruluşların verilerini bulundurduğu sunuculara fiziki erişim talep etmekte ve bu yükümlülük de **de facto** veri lokalizasyonu yükümlülüğü olarak kabul edilmektedir<sup>865</sup>.

## **b. Kanada**

Kuzey Amerika’da kurulmuş olan Kanada, dünyanın en zengin ve gelişmiş ülkelerinden birisidir<sup>866</sup>. Federal sistem ile yönetilen ülke, ağırlıklı olarak Avrupalı göçmenlerden oluşmaktadır ve Batı Bloğu’nun bir parçasıdır.

Kanada’da federal düzeyde veri lokalizasyonu öngören herhangi bir hukuki düzenleme bulunmamaktadır. Buna karşın eyaletlerin iç hukukları, yine bu eyaletler içerisinde geçerli olacak şekilde bazı veri lokalizasyonu yükümlülükleri öngörmektedir. Ayrıca kişiler arasında yapılan sözleşmeler çerçevesinde veri lokalizasyonu yükümlülüğü eğilimi Kanada’da bulunmaktadır<sup>867</sup>.

British Columbia eyaletinde 21 Ekim 2004 tarihinde yürürlüğe konan Bilgi Özgürlüğü ve Gizliliğin Korunması Kanunu’nun 30.1 numaralı maddesi, kamu otoritelerinin ellerinde ya da kontrollerinde bulunan kişisel bilgilerin sadece Kanada içerisinde saklanması ve sadece Kanada içerisinde erişilebilir olmasını zorunlu kılmaktadır<sup>868</sup>. Bu zorunluluğun istisnaları ise rıza ve veri aktarımının bir elektronik sistemin kurulması, bakımı, onarımı veya güncellenmesi için zorunlu olması ile bir elektronik sistemin hata vermesi sonucu veri kurtarma çalışmalarının yapılması olarak belirlenmiştir.

---

<sup>865</sup> Bauer, Ferracane, Lee-Makiyama, “Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States”, s. 6.

<sup>866</sup> Ralph R. Kruger, David J. Bercuson, William Lewis, Norman L. Nicholson, Roger D. Hall, “Canada”, **Encyclopedia Britannica**, 27.07.2022, (Çevrimiçi) <https://www.britannica.com/place/Canada>, 30.07.2022.

<sup>867</sup> Justin Ling, “National | CBA National - Canadian Legal Affairs: The Battle Over Data Localization”, (2019), (Çevrimiçi) <https://www.nationalmagazine.ca/en-ca/articles/law/opinion/2019/the-battle-over-data-localization>, 22.10.2020.

<sup>868</sup> Shaun Brown, “Data Localization: An Exercise in Futility?”, IAPP Canada Privacy Symposium, 23.05.2019, (Çevrimiçi) <https://nnovation.com/wp-content/uploads/2019/05/SBrown-Data-Localization-May2019.pdf>, 11.09.2020; Bennett, Oduro-Marfo, “Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?”, s. 885.

**Nova Scotia** eyaletinde 15 Kasım 2006’da yürürlüğe giren Kişisel Bilgilerin Uluslararası Paylaşımı Kanunu’nun 5.1 numaralı maddesine göre kamu otoritelerinin (ya da bunlara hizmet sağlayan kişilerin) ellerinde ya da kontrollerinde bulunan kişisel bilgilerin sadece Kanada içerisinde saklanması ve sadece Kanada içerisinde erişilebilir olmasını zorunlu kılmaktadır<sup>869</sup>. Bu kuralın istisnaları olarak rıza ya da Kanada dışında saklama ya da Kanada dışından erişimin, ilgili kamu otoritesinin baş yöneticisi tarafından ilgili kamu otoritesinin faaliyetlerini yürütmesi için zorunlu olduğunun onaylanması belirlenmiştir. 2017 yılı itibarıyla 80 civarı kamu otoritesinin baş yöneticinin onayı ile Kanada dışından aktarım ya da Kanada dışında saklama istisnasına dayandığı raporlanmıştır<sup>870</sup>. Söz konusu işlemler çoğunlukla ilgili kamu görevlilerinin Kanada dışından kendi mobil cihazları ile verilere erişmesine ilişkindir. Bunun yanında çeşitli ödeme hizmetlerinin ya da bulut servislerinin kullanıldığı da görülmektedir<sup>871</sup>.

Kanada’da veri lokalizasyonu yükümlülükleri öngörülmesinin temel sebebi, 11 Eylül 2001 tarihinde ABD’ye yapılan terör saldırılarından sonra ABD hükümetinin bilgi toplama yetkilerini aşırı şekilde genişleten PATRIOT Act gibi ABD iç hukuku düzenlemeleridir<sup>872</sup>. Öte yandan aşağıda değinilecek olan ABD, Meksika ve Kanada Anlaşması ile Kanada’nın veri lokalizasyonu öngörmeme taahhüdü vermesi, Kanada’nın bu konudaki düzenleme yetkisini sınırlamış durumdadır<sup>873</sup>.

---

<sup>869</sup> Brown, “Data Localization: An Exercise in Futility?”

<sup>870</sup> Brown, **a.y.**

<sup>871</sup> Brown, **a.y.**

<sup>872</sup> Brown, **a.y.**

<sup>873</sup> Michael Geist, “What the USMCA means for Data Localization Rules and Local Businesses in Canada”, **Bot Populi**, 2019; “Canada: Cross-border transfers and data localisation after the USMCA | Insights | DataGuidance”, **OneTrust Data Guidance**, (06.2020), (Çevrimiçi) <https://www.dataguidance.com/opinion/canada-cross-border-transfers-and-data-localisation>, 11.09.2020.



## 2. Doğu ve Güneydoğu Asya Ülkelerinde Veri Lokalizasyonu Yükümlülükleri

### a. Çin Halk Cumhuriyeti

Çin Halk Cumhuriyeti son yıllarda yaşadığı kalkınma sayesinde, Soğuk Savaş'ın sona ermesinden itibaren ortaya çıkan tek kutuplu dünya düzeninin başat aktörü olan ABD'ye hemen her alanda meydan okumaktadır<sup>874</sup>. Söz konusu alanlardan birisi de bilgi ve iletişim teknolojileridir. Bilgi ve iletişim teknolojilerine ekonomi ve güvenlik açısından oldukça önem veren Çin Halk Cumhuriyeti, bu alana ilişkin birçok düzenlemeyi yürürlüğe koymuştur<sup>875</sup>.

Çin Halk Cumhuriyeti'nin izlediği politikaların ve yürürlüğe koyduğu hukuk kurallarının mantıklarının anlaşılabilmesi için aynı zamanda bu ülkenin tarihi boyunca batı ülkeleri ile ilişkilerinin de bilinmesi gerekmektedir. Çin, 1800'lü yıllara kadar bölgesinin ve belki de dünyanın en güçlü ve kalabalık ülkesi olarak varlığını sürdürmüştür<sup>876</sup>. Ancak bu tarihlerden sonra batı ülkelerinin üstünlüklerini kabul ettirmesi, Çin'i gelişme ve kalkınma konusunda yeni çabalara itmiş ve aynı zamanda batıya karşı şüpheci bir tavır takınmasına sebebiyet vermiştir. İşte bu yaklaşımın sonucu olarak günümüzde Çin Halk Cumhuriyeti **Facebook**, **Twitter** ya da **Google**

<sup>874</sup> Walter Lohman, Riley Walters, "Understanding the Chinese Challenge to the United States", **The Heritage Foundation**, (2020), (Çevrimiçi) <https://www.heritage.org/asia/commentary/understanding-the-chinese-challenge-the-united-states>, 22.10.2021.

<sup>875</sup> Çin Halk Cumhuriyeti'nin bilgi ve iletişim teknolojileri ile internet konularındaki düzenleyici otoritesi olan Çin Siber Alan Yönetimi'nin (Cyberspace Administration of China) internet sitesi ("Cyberspace Administration of China", [03.11.2021], (Çevrimiçi) <http://www.cac.gov.cn/>, 03.11.2021), söz konusu düzenlemeleri içermektedir.

<sup>876</sup> Çin'in egemenlik alanı kuzeyde göçebe Türklerin ve Moğolların bölgeleri sınırlanmıştır. Doğu'da ise Kore yarımadasına kadar uzanan egemenlik alanı, Japonya'ya geçememiştir. Güney tarafında Çin egemenliği Çin Denizi'ne ve bazı adalara (Singapur gibi) yayılabilmektedir. Batıda ise Hindistan ve İran – Arap medeniyetleri Çin egemenlik alanının sınırlarını oluşturmaktadır. Çin, 1800'lü yıllara kadar dünyanın en zengin ve gelişmiş bölgelerinden biri olarak kalmıştır. Çin İmparatorları, adeta kralların kralı gibi protokol açısından üst bir seviye olarak muamele görmüşlerdir. Japonya başta olmak üzere çevre ülkeler, gelişmişlik seviyesi olarak Çin'i (tıpkı bugün batının örnek alınması gibi) örnek almışlardır. 1839 – 1842 ve 1856 – 1860 yıllarında yaşanan Afyon Savaşları neticesinde Avrupalı güçler Çin'de üstünlüklerini kabul ettirerek ticari serbest bölgeler ve kapitülasyonlar elde etmişlerdir. 1860 yılında İngiltere ve Fransa askerleri, Çin Hanedanlığının Pekin'de bulunan yazlık sarayını tamamen yok etmişlerdir. Tüm bu savaşlar ve bunlar sırasında meydana gelen küçük düşürücü olaylar, Çin'in hem kurtuluş çareleri aramasına hem de batıya karşı şüpheci bir tavra bürünmesine sebep olmuştur. Söz konusu etkiler günümüzde de devam etmektedir.

gibi şirketlere mesafeli yaklaşmakta ve ülkesi içerisinde batı ile irtibatlı olabilecek hemen her şeyi kontrol etmeye çalışmaktadır<sup>877</sup>.

Veri lokalizasyonu konusu, Çin Halk Cumhuriyeti içerisinde milli güvenliğin ve ekonomik kalkınmanın tesisi amaçları kapsamında değerlendirilmektedir<sup>878</sup>. Milli güvenlik kavramı altında Çin Halk Cumhuriyeti'nin bir küresel güç haline gelmesi, bütüncül milli güvenlik anlayışı çerçevesi içerisinde siber alanın Çin kültürüne karşı bir tehdit olarak ele alınması, politik sistemin korunması ile adli ve idari makamların görevlerini yerine getirmek için verilere erişim imkânı bulunması gibi hususlar bulunmaktadır<sup>879</sup>. Ekonomik kalkınma altında özellikle veri depolama endüstrisinin gelişimi ile uzun vadeleri teknolojik gelişmeler yakalanması için büyük verinin kullanılması gibi hedefler mevcuttur<sup>880</sup>. Tüm husus ve hedefler, Çin Halk Cumhuriyeti'nin kapsamlı şekilde veri lokalizasyonu yükümlülüğü getirmesine sebebiyet vermiştir<sup>881</sup>.

1 Haziran 2017 tarihinde yürürlüğe giren Çin Halk Cumhuriyeti Siber Güvenlik Kanunu<sup>882</sup> m. 37 ile birlikte Çin anayasası içerisindeki faaliyetleri sırasında kişisel bilgi ya da önemli veri toplayan ya da üreten kritik bilgi altyapısı işleticileri, söz konusu bilgi ve verileri Çin anayasası içerisinde saklamakla yükümlü kılınmışlardır<sup>883</sup>. Bu kurala istisna olarak ise ticari faaliyetlerin anakara dışına bilgi ve veri aktarımı gerektirmesi hali gösterilmiştir. Böyle bir durumda, ilgili makamların belirlediği

---

<sup>877</sup> Jeanne Huang, "Chinese private international law and online data protection", **Journal of Private International Law**, C. 15, S. 1, 2019, s. 201; Sargsyan, "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security", s. 2226.

<sup>878</sup> Jinhe Liu, "China's Data Localization", **Chinese Journal of Communication**, C. 13, S. 1, 2020, s. 98; Sargsyan, "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security", s. 2226; Yanqing Hong, "The Cross-Border Data Flows Security Assessment", Working Paper, 2017, s. 6.

<sup>879</sup> Liu, "China's Data Localization", s. 95 vd.

<sup>880</sup> Liu, **a.g.e.**, s. 91.

<sup>881</sup> Liu, **a.g.e.**, s. 87.

<sup>882</sup> Kanunun İngilizce tercümesi için bkz. "Cybersecurity Law of the People's Republic of China", (2017), (Çevrimiçi) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>, 25.07.2020.

<sup>883</sup> Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", s. 225; Abe Yoshinori, "Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?", s. 3; Hong, "The Cross-Border Data Flows Security Assessment", s. 5.

kriterlere göre güvenlik deęerlendirmesi yapılarak ve dięer hukuk kurallarına uygun davranılarak aktarım yapılabilmesi mümkündür<sup>884</sup>. Kişisel bilgilerin yurtdışına aktarımında, veri sahibi kişilerin rızasını almak da kullanılabilecek bir dięer yöntem olarak karşımıza çıkmaktadır.

Anılan madde çerçevesinde veri lokalizasyonu ile yükümlü kılınan kişiler, kritik bilgi altyapısı işleticileridir. Kritik bilgi altyapıların nelerden oluştuęuna dair düzenleme, aynı kanunun 31 numaralı maddesinde yer almaktadır. Buna göre kamuoyuna açık iletişim ve bilgi paylaşım hizmetleri, enerji, trafik, su kaynakları, finans, kamu hizmetleri, elektronik ortamda sunulan kamu hizmetlerine ilişkin sistemler; kritik bilgi altyapısı olarak sınıflandırılmıştır<sup>885</sup>. Buna ek olarak yok edilmeleri, belirli fonksiyonlarını kaybetmeleri ya da veri sızıntısına maruz kalmaları halinde ulusal güvenliği, ulusal refahı, halkın geçimini ya da kamu menfaatlerini ciddi şekilde tehlikeye atabilecek her türlü bilgi sistemi de kritik bilgi altyapısı olarak kabul edilmektedir. Devlete, kritik bilgi altyapılarını koruma görevi yüklenmiştir. Ayrıca devletin, kritik bilgi altyapısı statüsünde olmayan bilgi sistemlerinin işleticilerini de gönüllü olarak devletin alacaęı koruma önlemlerine uygun hareket etmeye teşvik etme ödevi bulunmaktadır.

Kişisel bilgi kavramı, kanunun 76 numaralı maddesinde, bir gerçek kişinin kimliğini belirlemeye yeterli olacak her türlü bilgi olarak tanımlanmıştır. Önemli veri kavramının tanımı ise kanun içerisinde yer almamaktadır<sup>886</sup>. Buna karşılık DTÖ Hizmet Ticareti Konseyi tutanaklarında Çin Halk Cumhuriyeti temsilcisi tarafından önemli veri kavramının işletmeler ya da bireyler için deęil; ulus için önemli verileri kapsadığı ifade edilmiştir<sup>887</sup>.

---

<sup>884</sup> Yanqing Hong, “The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China’s Basic Strategic Resources”, Working Paper, Yale Law School Paul Tsai China Center, 20.06.2017, s. 9, (Çevrimiçi) <http://apide.org/apru-asia-eu-dialogue/readings/CrossBorderDataFlows.pdf>, 27.07.2020.

<sup>885</sup> Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 225.

<sup>886</sup> Hong, “The Cross-Border Data Flows Security Assessment”, s. 8.

<sup>887</sup> “Report of the Meeting Held on 6 October 2017, Note by the Secretariat, S/C/M/133”, World Trade Organization, 06.11.2017, s. 24, (Çevrimiçi)

Yukarıda verilen açıklamalardan da anlaşılacağı üzere Çin Halk Cumhuriyeti hukuku, son derece büyük ölçekli bir veri lokalizasyonu yükümlülüğü öngörmektedir. Üstelik Siber Güvenlik Kanunu içerisindeki tanımların son derece geniş olması, veri lokalizasyonu yükümlülüğünün zaman içerisinde genişleyebileceğini de kanaatimizce göstermektedir.

Çin Halk Cumhuriyeti tarafından yürürlüğe konan Siber Güvenlik Kanunu’nun getirdiği veri lokalizasyonu dahil çeşitli yükümlülüklerin yabancı aktörlerin Çin pazarına girmesini engellediği ve yabancılar ile yerliler arasında GATS’a aykırı şekilde eşitsiz bir durum yarattığı endişeleri Japonya ve ABD tarafından DTÖ Hizmet Ticaret Konseyi gündemine taşınmıştır. AB, Yeni Zelanda, Hindistan, Avustralya, Brezilya ve Tayvan da Japonya ve ABD’yi destekler tutum almıştır. Bu çalışma tarihi itibarıyla konu sonraki Konsey görüşmelerinde de ele alınmış olsa da Çin Halk Cumhuriyeti’ne herhangi bir yaptırım uygulanması söz konusu olmamıştır<sup>888</sup>. Çin Halk Cumhuriyeti tarafından 1 Kasım 2021 tarihinde yürürlüğe girmek üzere kabul edilen Kişisel Bilgileri Koruma Kanunu’nun<sup>889</sup> 40 numaralı maddesi, veri

---

<https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M133.pdf&Open=True>, 29.07.2020; Benzer yönde bir tanım için bkz. Hong, “The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China’s Basic Strategic Resources”.

<sup>888</sup> Konunun görüşüldüğü tutanaklar için bkz. “Report of the Meeting Held on 2 March 2018, Note by the Secretariat, S/C/M/134”, World Trade Organization, 05.04.2018, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M134.pdf&Open=True>, 29.07.2020; “Report of the Meeting Held on 30 May 2018, Note by the Secretariat, S/C/M/135”, World Trade Organization, 11.07.2018, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M135.pdf&Open=True>, 29.07.2020; “Report of the Meeting Held on 12 October 2018, Note by the Secretariat, S/C/M/136”, World Trade Organization, 26.11.2018, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M136.pdf&Open=True>, 28.07.2020; “Report of the Meeting Held on 24 January 2019, Note by the Secretariat, S/C/M/137”, World Trade Organization, 24.01.2019, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M137.pdf&Open=True>, 29.07.2020; “Report of the Meeting Held on 24 April 2019, Note by the Secretariat, S/C/M/138”, World Trade Organization, 24.04.2019, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M138.pdf&Open=True>, 29.07.2020; “Report of the Meeting Held on 13 December 2019, Note by the Secretariat, S/C/M/141”, World Trade Organization, 13.12.2019, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/M141.pdf&Open=True>, 29.07.2020.

<sup>889</sup> Rogier Creemers, Graham Webster, “Translation: Personal Information Protection Law of the People’s Republic of China”, 20.08.2021, (Çevrimiçi) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>, 12.10.2021.

sorumlularının Çin'den topladıkları kişisel verilerin belirli bir hacme erişmesi halinde Çin Halk Cumhuriyeti sınırları içerisinde saklanmasını zorunlu tutmaktadır. Bahse konu hacmi belirleme yetkisi ise ilgili kamu kurumuna verilmiş olup henüz bu yetki kapsamında herhangi bir belirleme yapılmamıştır.

## **b. Hindistan**

Hindistan gerek nüfusu gerek ise ekonomik büyüklüğü ile Asya kıtasının önemli ülkelerinden biridir<sup>890</sup>. Hindistan özellikle yazılım ve teknoloji önemli gelişmeler kaydetmiştir. Veri lokalizasyonu konusu hemen her ülkede olduğu gibi Hindistan'da da gündemdedir.

Hindistan'da bulunan veri lokalizasyonu mevzuatından birisi, Hindistan Merkez Bankası tarafından çıkarılan ve bankacılık sektörüne yönelik olarak 6 Nisan 2018 tarihinde yürürlüğe giren genelgedir<sup>891</sup>. Anılan genelge ile ödeme sistemlerine ilişkin tüm veriler, sadece Hindistan sınırlarında bulunan bilgi sistemleri içerisinde saklanabilecektir. Söz konusu veriler içerisinde, uçtan uca olacak şekilde ödeme işlemi ile ilgili her türlü kayıt dahildir. Eğer söz konusu finansal işlemin bir tarafı yabancı ise, bu durumda söz konusu işleme ilişkin verilerin başka bir ülkede saklanması önünde herhangi bir engel bulunmamaktadır. Anılan düzenlemenin amacı, ödeme sistemlerinin izlenmesi ve denetlenmesi olarak açıklanmaktadır<sup>892</sup>.

1993 ve 2012 tarihli çeşitli kanunlar, Hindistan'ın devlete ilişkin her türlü verinin ve kamu kaydının ülke dışına aktarılmasını yasaklamış ve bunların Hindistan sınırları içerisinde saklanmasını zorunlu kılmıştır<sup>893</sup>.

---

<sup>890</sup> Romila Thapar, Joseph E. Schwartzberg, A.L. Srivastava, "India", **Encyclopedia Britannica**, 27.07.2022, (Çevrimiçi) <https://www.britannica.com/place/India>, 30.07.2022.

<sup>891</sup> "The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or A Patchwork of Requirements?", 22.06.2021, (Çevrimiçi) <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/>. Duggal, "Data Localization: A Review of Proposed Data Localization Legislation in India, With Learnings for The United States", s. 6.

<sup>892</sup> "The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or A Patchwork of Requirements?"

<sup>893</sup> Anirudh Burman, Upasana Sharma, "How Would Data Localization Benefit India?", 14.04.2021, (Çevrimiçi) <https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291>, 09.09.2021.

Hindistan'daki bir diğ er veri lokalizasyonu y uk uml l ğ u kendisini Ki isel Verilerin Korunması Kanunu taslağı i erisinde g stermektedir<sup>894</sup>. Bu kanunun 2018 yılında yayınlanan ikinci taslağının 40/1 numaralı maddesine g re, kanun kapsamındaki t m ki isel verilerin bir kopyasının Hindistan'da tutulması gerekmektedir. 40/2 numaralı madde ise Hindistan h k metinin belirleyeceğı kritik ki isel verilerin sadece Hindistan sınırları i erisinde saklanabileceğı ve Hindistan sınırları dı ına aktarılamayacağı h k m altına alınmıştır. Ancak kanun i erisinde kritik ki isel verilerin hangi kriterlere g re belirleneceğine ili kin herhangi bir h k m bulunmamaktadır. Ki isel veriler ile  zel nitelikli ki isel verilerin<sup>895</sup> Hindistan dı ına aktarımı ise m. 41 altında d zenlenen bazı  artlara (ilgili kurumlarca onaylanan s zle meler  er evesinde aktarım ya da g venli olarak kabul edilen  lkelere aktarım gibi AB ile uyumlu  artlar) baėlanmıştır.

Ki isel Verilerin Korunması Kanunu taslağı, 2019 yılında deėi tirilerek Hindistan Parlamentosu'na sunulmu tur<sup>896</sup>. Bu taslak i erisinde, 2018 versiyonunun getirdiğı sıkı kurallardan b y k oranda vazge ilmiştir. Bu kapsamda ki isel verilerin bir kopyasının Hindistan sınırları i erisinde saklanması ile ki isel verilerin Hindistan dı ına aktarılması i in uyulması gereken  artlar sadece  zel nitelikli ki isel veriler i in uygulanacak  ekilde d zenlenmiştir.  zel nitelik ta ımayan ki isel verilerin Hindistan dı ına aktarımı konusunda ise herhangi bir ko ul  ng r lmemi tir. Hindistan h k metinin kritik nitelikteki ki isel verileri belirleme yetkisi ile bunların Hindistan sınırları dı ına  ıkarılması yasağı ise tamamen korunmu tur. S z konusu taslak, bu  alı ma tarihi itibarıyla hen z yasala arak y r rl ėe girmemi tir.

---

<sup>894</sup> Rishab Bailey, Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends", **National Institute of Public Finance and Policy**, Working Paper No:242, 2018, s. 8.

<sup>895</sup> Kanun taslağının 2019 versiyonunun 3/36 maddesi ile 2018 versiyonunun 3/35 numaralı maddesi  er evesinde  zel nitelikli ki isel veriler  ifreler, finansal veriler, saėlık verileri, resmi kimlik tanımlayıcılar, cinsel hayat ve y nelim, biyometrik veri, cinsiyet deėi imi durumu, erdi i durumu, kast ya da kabile bilgisi, dini ya da siyasi eėilim ve ili kiler ile veri koruma otoritesince belirlenebilecek diğ er veriler anlamına gelmektedir.

<sup>896</sup> Duggal, "Data Localization: A Review of Proposed Data Localization Legislation in India, With Learnings for The United States", s. 6; Rishab Bailey, "The issues around data localisation", **The Hindu**, (25.02.2020), ( evrimi i) <https://www.thehindu.com/opinion/op-ed/the-issues-around-data-localisation/article30906488.ece>, 04.08.2020.

### c. Endonezya

Endonezya, Güney Doğu Asya’da yer alan, yüksek nüfuslu ve adalardan oluşan bir ülkedir<sup>897</sup>. Endonezya, dünyanın en işlek deniz yolları üzerinde bulunmaktadır. Endonezya ayrıca ASEAN Güneydoğu Asya Uluslar Birliği’nin<sup>898</sup> bir üyesidir.

Endonezya, 2012 tarihli ve 82 numaralı Hükümet Yönetmeliği ile birlikte geniş kapsamlı bir veri lokalizasyonu yükümlülüğü öngörmüştür<sup>899</sup>. Söz konusu veri lokalizasyonu yükümlülüğü ülkede kamu hizmeti sunan elektronik sistem işleticilerini kapsamaktadır. Elektronik sistem kavramı, elektronik bilgileri hazırlamaya, toplamaya, işlemeye, analiz etmeye, saklamaya, görüntülemeye, duyurmaya, göndermeye veya yaymaya yarayan her türlü elektronik setler ya da prosedürler olarak tanımlanmıştır<sup>900</sup>. Elektronik sistemleri işleten tüm kişiler (kamu – özel ya da gerçek – tüzel kişi ayrımları fark etmeksizin) de elektronik sistem işleticileri olarak ifade edilmiştir. 82 numaralı yönetmelik içerisinde, kamu hizmeti kavramının tanımına yer verilmemiştir<sup>901</sup>. Ancak diğer mevzuattan anlaşıldığı kadarıyla toplumun tüm fertlerinin yararlanma ihtiyacı içerisinde bulunduğu tüm hizmetler, kamu hizmeti olarak tanımlanmaktadır<sup>902</sup>. 82 numaralı yönetmelik ayrıca kapsam içerisine giren tüm elektronik sistem işleticilere, yönetmelik gereklerine uyum sağlamaları için 5 yıllık bir süre tanımlanmıştır.

<sup>897</sup> “Indonesia”, **Encyclopedia Britannica**, 05.01.2022, (Çevrimiçi) <https://www.britannica.com/place/Indonesia>, 06.01.2022.

<sup>898</sup> Wong, “Data Localization and ASEAN Economic Community”, s. 9.

<sup>899</sup> “Regulation of the Government of the Republic of Indonesia number 82 of 2010 concerning Electronic System and Transaction Operation”, (Çevrimiçi) <https://media2.mofo.com/documents/indonesia+government+regulation+no.+82+of+2012.pdf>, 22.08.2020; Wong, “Data Localization and ASEAN Economic Community”, s. 166; Sitinjak, Wahab, “Policy Analysis of Data Localization in Digital Market Integration in Southeast Asian Region”, s. 46.

<sup>900</sup> Mark Innis, Adhika Wiyoso, “General Data Localization Requirements in Indonesia”, Jakarta, Baker McKenzie, 07.2018, s. 1, (Çevrimiçi) [https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al\\_generaldatalocalizationrequirements\\_july2018.pdf?la=en](https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf?la=en), 18.08.2020.

<sup>901</sup> Innis, Wiyoso, **a.g.e.**, s. 2.

<sup>902</sup> Innis, Wiyoso, **a.g.e.**, s. 3.

Yukarıda da açıklandığı üzere 82 numaralı yönetmelik kapsamına giren kişilerin kimler olduğu konusunu son derece belirsizdir<sup>903</sup>. Bu belirsizlikler uyum çalışmalarının tamamlanamamasına sebep olmuştur. Ayrıca başta çok uluslu teknoloji şirketleri olmak üzere, yabancı yatırımcılar arasında söz konusu düzenleme ciddi rahatsızlık yaratmıştır<sup>904</sup>. Zira bu tür yatırımcılar her ülke için özel bilgi sistemi altyapısı kurmamakta ve belirli merkezlerden birçok ülkeye hizmet vermektedirler<sup>905</sup>. Tüm bu sorunları çözmek adına Endonezya hükümeti tarafından 82 numaralı yönetmeliği değiştiren 2019 tarihli ve 71 sayılı Hükümet Yönetmeliği yürürlüğe konmuştur<sup>906</sup>.

71 sayılı yönetmelik ile birlikte elektronik sistem işleticileri, özel ve kamu elektronik sistem işleticileri olarak ikiye ayrılmıştır. Kamu elektronik sistem işleticileri, devlet kurumları ya da devlet kurumları tarafından bir elektronik sistemi işletmesi için atanan kişiler olarak tanımlanmıştır<sup>907</sup>. 71 sayılı yönetmelik, kamu hizmeti kavramını veri lokalizasyonu yükümlüğünü belirleme aracı olarak kullanma yaklaşımını terk etmiştir. Bunun yerine veri lokalizasyonu yükümlülüğü sadece kamu elektronik sistem işleticileri için öngörülmüştür<sup>908</sup>. Söz konusu yükümlülüğe göre hem verilerin hem de elektronik sistemlerin Endonezya sınırları içerisinde tutulması gerekmektedir. Bu kurala istisna olarak gereken veri saklama teknolojisinin Endonezya içerisinde

<sup>903</sup> “Government Relaxes Data Localisation Requirement”, Assegaf Hamzah & Partners, 25.10.2019, s. 1, (Çevrimiçi) <https://id.rajahtannasia.com/media/3544/ahpclientupdate-25october2019.pdf>, 21.07.2020.

<sup>904</sup> “Indonesia Relaxes Data Storage Rules to Allow Placement Abroad”, **Reuters**, (24.10.2019), (Çevrimiçi) <https://www.reuters.com/article/us-indonesia-tech-data-idUSKBN1X31P5>, 19.08.2020.

<sup>905</sup> “Government Relaxes Data Localisation Requirement”, s. 1.

<sup>906</sup> “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam”, (19.08.2020), (Çevrimiçi) <https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/>, 19.08.2020.

<sup>907</sup> Daniel Pardede, Adhika Wiyoso, “GR 82 No More! Now It Is GR 71!: New Regulation on Electronic System and Transactions”, Jakarta, Baker McKenzie, 10.2019, s. 1, (Çevrimiçi) [https://f.datasrvr.com/fr1/319/37527/Corporate\\_Commercial\\_-\\_GR\\_82\\_no\\_more\\_Now\\_it\\_is\\_GR\\_71\\_\(Oct\\_2019\)\\_-Final.pdf](https://f.datasrvr.com/fr1/319/37527/Corporate_Commercial_-_GR_82_no_more_Now_it_is_GR_71_(Oct_2019)_-Final.pdf), 18.08.2020; ABNR-Agus Ahadi Deradjat, “Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems | Lexology”, (19.08.2020), (Çevrimiçi) <https://www.lexology.com/library/detail.aspx?g=cd6e5251-6dd7-4b46-b6be-759c78c9bf7b>, 19.08.2020.

<sup>908</sup> Pardede, Wiyoso, “GR 82 No More! Now It Is GR 71!: New Regulation on Electronic System and Transactions”, s. 2.



bulunmaması hali getirilmiştir<sup>909</sup>. Özel elektronik sistem işleticileri için veri lokalizasyonu yükümlülüğü bulunmasa da onların da denetim ve adli makamların bilgi taleplerini karşılayabilecek kadar erişim imkanını sağlamak kaydıyla verilerini ve elektronik sistemlerini yurtdışında barındırmalarına izin verilmiştir<sup>910</sup>. Söz konusu erişim imkanının kapsamı ve gereklilikleri ileride çıkarılacak yeni yönetmeliklerle netleştirilecektir<sup>911</sup>.

#### d. Vietnam

Güneydoğu Asya’da yer alan Vietnam Sosyalist Cumhuriyeti, Vietnam Savaşı’ndan sonra 1976 yılında Güney ve Kuzey Vietnam’ın birleşmesi ile kurulmuştur<sup>912</sup>. 1986 yılına kadar dışa kapalı kalan ülke, bu tarihten sonra tekrar dış ilişkilere açılarak önemli bir ekonomik merkez haline gelmiş ve hızlı bir büyüme göstermiştir<sup>913</sup>.

Vietnam’da veri lokalizasyonu konusu, 1 Ocak 2019 tarihinde yürürlüğe giren Vietnam Siber Güvenlik Kanunu ile gündeme gelmiştir<sup>914</sup>. Bu kanunun 26/3 numaralı maddesine göre yerli ya da yabancı telekomünikasyon hizmetleri sağlayıcıları, internet hizmetleri sağlayıcıları ve katma değerli hizmet sağlayıcılarının, Vietnam dijital ortamında sundukları hizmetlerin kullanıcılarına ilişkin tüm kişisel bilgileri, kullanıcıların birbirleriyle ilişkilerine dair verileri ve kullanıcılar tarafından üretilen tüm verileri; Vietnam sınırları içerisinde, hükümet tarafından belirlenecek süreler boyunca saklanması gerekmektedir.

<sup>909</sup> “The Retreat of the Data Localization Brigade”; “Government Relaxes Data Localisation Requirement”, s. 1.

<sup>910</sup> Pardede, Wiyoso, “GR 82 No More! Now It Is GR 71!: New Regulation on Electronic System and Transactions”, s. 3; “Indonesia Relaxes Data Storage Rules to Allow Placement Abroad”, s. 1; Deradajat, “Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems | Lexology”.

<sup>911</sup> Pardede, Wiyoso, “GR 82 No More! Now It Is GR 71!: New Regulation on Electronic System and Transactions”, s. 3.

<sup>912</sup> “Vietnam”, **Encyclopedia Britannica**, 26.08.2021, (Çevrimiçi) <https://www.britannica.com/place/Vietnam>, 10.09.2021.

<sup>913</sup> “Vietnam After the War”, **Asia Pacific Foundation of Canada**, (10.10.2021).

<sup>914</sup> “Data Localisation Requirements Narrowed in Vietnam’s Cybersecurity Law”, **The Business Times**, (15.10.2019), (Çevrimiçi) <https://www.businesstimes.com.sg/asean-business/opinion/data-localisation-requirements-narrowed-in-vietnams-cybersecurity-law>, 15.05.2020; Kanunun tercümesi için bkz. “Law on Cybersecurity”, C. 24, C. 24 §, (2018), (Çevrimiçi) <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>, 17.03.2020.

Gerek getirilen yükümlülüğün kapsamının çok geniş ve belirsiz olması gerekse bu kadar geniş bir yükümlülüğün dijital ortamda faaliyet gösteren yerli ve yabancı yatırımcılardan tepki görmesi üzerine, hükümet tarafından ilgili yükümlülüğün uygulanmasına dair çıkarılması planlanan ikincil düzenleme içerisinde birtakım esnemeler getirileceği ifade edilmiştir<sup>915</sup>. Bu kapsamda aşağıda bahsedilen üç adet kriteri birlikte sağlayan hizmet sağlayıcıların veri lokalizasyonu yükümlülüğüne tabi olacağı belirtilmiştir<sup>916</sup>.

Anılan kriterlerden ilki telekomünikasyon ağı, internet ya da benzeri siber alanlarda hizmet vermektir. İkinci kriter ise hizmet sağlayıcısının Vietnam'daki kullanıcıların kişisel bilgilerini, bu kullanıcıların ürettiği verileri ya da Vietnam'daki kullanıcıların birbirleriyle ilişkilerine dair verileri toplaması, bunlardan faydalanması, bunları analiz etmesi ya da işlemesi olarak belirlenmiştir. Üçüncü ve düzenleme kapsamına etki eden kriter ise sunduğu hizmetlerin Vietnam hukukunu ihlal etmek amacıyla kullanıldığına dair bilgilendirilen ve buna rağmen ilgili hukuka aykırılıkları engellemek ya da bunlarla mücadele etmek adına önlem almayan; veya ilgili hukuka aykırılıklarla mücadele etmekle görevli resmi makamların taleplerini karşılamayan veyahut da resmi makamlarca alınmış siber güvenlik koruma önlemlerini ortadan kaldıran ya da etkisizleştiren hizmet sağlayıcılardan olmak şeklinde ifade edilmiştir.

Belirlenen bu üçüncü kriter esasen veri lokalizasyonu yükümlülüğünün kapsamını sadece Vietnam resmi makamları ile uyumlu hareket etmeyen hizmet sağlayıcılarla sınırlayarak, veri lokalizasyonu yükümlülüğünü adeta bir ceza mekanizmasına dönüştürmüştür. Böylelikle Vietnam resmi makamları ile uyumlu hareket eden hizmet sağlayıcılar açısından veri lokalizasyonunun devletler için getirdiği menfaatlerden yararlanılabilirken; veri lokalizasyonunun ilgili kişiler için yarattığı külfetlere katlanılması gerekmeyecektir. Uyumlu hareket etmeyen hizmet sağlayıcılar ise veri lokalizasyonu yükümlülükleri vasıtasıyla adeta cezalandırılmaktadırlar. Aynı zamanda veri lokalizasyonu vasıtasıyla, mülklik ilkesi çerçevesinde ilgili verilere

---

<sup>915</sup> Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam".

<sup>916</sup> Basu, a.y.

Vietnam hukukunun uygulanması temin edilmektedir. Önemle belirtmek gerekir ki söz konusu düzenleme henüz yürürlüğe girmediği için uygulamadaki sonuçlarının ne olacağı belirsizdir.

#### e. Güney Kore

Kore Cumhuriyeti ya da yaygın bilinen adıyla Güney Kore, Doğu Asya bölgesinde Çin, Rusya ve Japonya gibi güçlü ülkeler arasında kurulmuş bir devlettir. Kore, tarihi boyunca Çin ya da Japonya'ya bağlı olarak yaşamıştır (1897 ile 1910 yılları arasında kurulan Kore İmparatorluğu dönemi hariç)<sup>917</sup>. 1950 ile 1953 tarihleri arasında gerçekleşen Kore Savaşı'ndan sonra, güneyde kapitalist sisteme sahip olan Kore Cumhuriyeti; kuzeyde ise komünist sisteme dahil olan Kore Demokratik Halk Cumhuriyeti ya da yaygın bilinen adıyla Kuzey Kore kurulmuştur.

Güney Kore gerek etrafındaki büyük güçlerin etkisinden gerekse Kuzey Kore'nin saldırı ihtimalinden korunmak adına kuruluşundan beri sürekli olarak kalkınmaya ve güçlü güvenlik politikalarına odaklanmış durumdadır<sup>918</sup>. Bu politikalar, veri lokalizasyonu konusunda da etkisini göstermektedir.

Güney Kore'nin veri lokalizasyonu getiren en önemli mevzuatı; 2009 tarihli Arazi Etüdü, Su Etüdü ve Kadastro Kayıtları Hakkında Kanun'dur<sup>919</sup>. Anılan kanun, benzer hükümleri içeren 1961 tarihli başka bir kanun yerine çıkarılmıştır<sup>920</sup>. 2009 tarihli kanunun 16 numaralı maddesine göre, harita verileri ile etüt çalışmalarının sonuçlarının Güney Kore topraklarına ilgili bakanlığın izni olmadan çıkarılması yasaklanmıştır. Söz konusu yasağın amacı, Güney Kore haritalarının düşman güçler eline geçmesini engellemektir<sup>921</sup>. Bu hüküm, verileri Güney Kore dışında saklayan dijital harita hizmetlerinin Güney Kore'de çalışmasını engellemektedir<sup>922</sup>. Örneğin,

---

<sup>917</sup> “South Korea”, **Encyclopedia Britannica**, 06.01.2022, (Çevrimiçi) <https://www.britannica.com/place/South-Korea>, 07.01.2022.

<sup>918</sup> Yoon, “South Korean Data Localization: Shaped by Conflict”.

<sup>919</sup> Yoon, **a.y.**

<sup>920</sup> Yoon, **a.y.**

<sup>921</sup> Yoon, **a.y.**

<sup>922</sup> Yoon, **a.y.**

**Google** Haritalar hizmeti Güney Kore sınırları içerisinde çalışmamaktadır<sup>923</sup>. Diğer ülkelere göre oldukça farklı olan bu düzenleme, Güney Kore'nin içinde bulunduğu savaş halinin ihtiyaçlarını yansıtmaktadır.

Güney Kore'nin veri lokalizasyonu getiren ikinci düzenlemesi, 2011 yılında yürürlüğe konulan Kişisel Bilgilerin Korunması Kanunu'dur<sup>924</sup>. Söz konusu kanunun 17 numaralı maddesi çerçevesinde kişisel bilgilerin Güney Kore sınırları dışına aktarılması ancak veri sahiplerinin rızasının alınması ile mümkün kılınmıştır. Aynı maddeye göre rızanın alınabilmesi için öncelikle veri sahiplerine kişisel bilgilerin kime aktarılacağı, alıcının bu bilgileri hangi amaçlarla kullanacağı, hangi kişisel bilgilerin aktarılacağı, alıcısının kişisel bilgileri ne kadar süreyle saklayıp kullanacağı ve veri sahibinin rıza vermekten imtina edebileceği ile imtina etmesi halinde karşılaşacağı dezavantajların açıklanması gerekmektedir. Gerek rıza toplama gerekse sunulması gereken bilgilerin detay seviyesi, Güney Kore sınırları dışına kişisel bilgi aktarılmasını neredeyse imkânsız hale getirmektedir<sup>925</sup>. Bu nedenle söz konusu yükümlülüğü bir **de facto** veri lokalizasyonu yükümlülüğü olarak yorumlamak kanaatimizce mümkündür.

Son olarak belirtmek gerekir ki Güney Kore, finansal kuruluşların verileri Güney Kore sınırları içerisinde işlemlerini zorunlu kılmakta olup bu kuralın istisnası da müşteri talebi olarak belirlenmiştir<sup>926</sup>.

---

<sup>923</sup> Yoon, **a.y.**

<sup>924</sup> M. James Daley, Jason Priebe, Patrick Zeller, "The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery", **Sedona Conference Journal**, C. 16, 2015, s. 219.

<sup>925</sup> Daley, Priebe, Zeller, **a.g.e.**, s. 228.

<sup>926</sup> Berry, Reisman, "Policy Challenges of Cross-Border Cloud Computing", s. 18; Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders", s. 11; Daley, Priebe, Zeller, "The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery", s. 227.

### 3. Diğer Bazı Ülkelerde Veri Lokalizasyonu Yükümlülükleri

#### a. Rusya

Sovyet Sosyalist Cumhuriyetler Birliği'nin yıkılmasından sonra kurulan Rusya Federasyonu, Doğu Avrupa'dan başlayarak doğuya doğru Büyük Okyanus'a kadar uzanan geniş bir ülkedir. Ülke içerisinde onlarca etnik grup yaşamaktadır. Rusya, tarihi boyunca ülkesinde, batılı güçlerin etkisini ortadan kaldırma politikası gütmüştür<sup>927</sup>. Ayrıca ülke sınırlarının son derece geniş olması ile çok sayıdaki etnik grubun mevcudiyeti, devlet politikalarının özgürlüklerden veya ekonomik kalkınmadan yana değil; güvenlikten yana olmasına sebebiyet vermiştir.

Rusya'nın batı etkilerine karşı olan şüpheli tavrı, dijital ortamın gelişmesi ile birlikte bu alanda da kendisini göstermeye başlamıştır. 1 Eylül 2015 tarihinde yürürlüğe giren ve mevcut Kişisel Veri Kanunu'nu değiştiren 21 Temmuz 2014 tarihli 242-FZ numaralı Federal Kanun, Rus vatandaşlarının tüm kişisel verilerine dair kapsamlı bir veri lokalizasyonu yükümlülüğü getirmiştir<sup>928</sup>.

Anılan yükümlülük çerçevesinde Rus vatandaşlarının kişisel verileri üzerinde yapılan kayıtlama, sistematikleştirme, biriktirme, saklama, uyarılma veya değiştirme ile kurtarma işlemlerinin hepsinin Rusya toprakları içerisinde tutulan veri tabanları vasıtasıyla gerçekleştirilmek zorundadır.<sup>929</sup> Ayrıca toplanan kişisel verilerin ilk önce Rusya'da bulunan veri tabanlarına kaydedilmesi de mecburidir. Her iki yükümlülük

<sup>927</sup> Dominic Lieven, Martin McCauley, "Ethnic Relations and Russia's 'near-Abroad'", **Encyclopedia Britannica**, 18.12.2021, (Çevrimiçi) <https://www.britannica.com/place/Russia>, 18.12.2021.

<sup>928</sup> Iva Mihaylova, "Could the Recently Enacted Data Localization Requirements in Russia Backfire?", U. of St. Gallen Law & Economics Working Paper No. 2015-07, 2015, s. 3 (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2629533](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2629533), 13.03.2021; Fraser, "Data Localisation and the Balkanisation of the Internet", s. 369; Sargsyan, "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security", s. 2227; Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", s. 222; Abe Yoshinori, "Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?", s. 4; Daniel Garrie, Irene Byhovskiy, "Privacy and Data Protection in Russia Country Briefings", **Journal of Law & Cyber Warfare**, C. 5, S. 2, 2017, s. 242.

<sup>929</sup> Mihaylova, "Could the Recently Enacted Data Localization Requirements in Russia Backfire?", s. 4; Fraser, "Data Localisation and the Balkanisation of the Internet", s. 370; Garrie, Byhovskiy, "Privacy and Data Protection in Russia Country Briefings", s. 242; Kemp, "Cloud Computing and Data Sovereignty", s. 26.

birlikte değerlendirildiğinde, Rus vatandaşlarının kişisel verilerini işleyerek sunulan her türlü hizmetin, Rusya’da bulunan bilgi sistemleri vasıtasıyla sunulması gerektiği sonucuna ulaşılmaktadır.

Öte yandan belirtmek gerekir ki Rus vatandaşlarının kişisel verilerinin yurt dışına aktarımı konusunda açık bir yasak, Rus mevzuatında mevcut değildir. Yukarıda açıklanan veri lokalizasyonuna uyum sağlanması kaydıyla kişisel verilerin ikinci kopyalarının Rusya dışına aktarılmasına izin verilmektedir<sup>930</sup>.

#### **b. Kazakistan**

Sovyet Sosyalist Cumhuriyetler Birliği’nin yıkılmasından sonra 1991 yılında bağımsızlığını ilan eden Kazakistan, Türk devletleri ile İslam devletleri arasında en geniş topraklara sahip ülke konumundadır<sup>931</sup>.

Veri lokalizasyonu konusu, Kazakistan’da da dünyanın pek çok yerinde olduğu gibi gündeme gelmiştir. 94-V numaralı Kazakistan Cumhuriyeti Kişisel Veri ve Kişisel Verinin Korunması Kanunu’nun 12 numaralı maddesi, bu kanunun bölgesel uygulama kapsamına giren tüm kişisel verilerin, Kazakistan topraklarında bulunan veri tabanlarında saklanması zorunlu tutmuştur<sup>932</sup>. Ancak bu yükümlülük, kişisel verilerin başka kopyalarının Kazakistan dışına aktarılmasına engel teşkil etmemektedir.

Bilgi Toplumuna Dönüşme Amacıyla Çıkarılan Kanun’un 38 numaralı maddesi de kamu otoritelerinin bilgi sistemlerinin Kazakistan sınırları içerisinde bulunmasını

---

<sup>930</sup> Justin Sherman, Samuel Bendett, “Russia’s ‘Data Localization’ Efforts May Guide Other Governments”, **Defense One**, (04.09.2020), (Çevrimiçi) <https://www.defenseone.com/ideas/2020/01/russias-data-localization-push-may-guide-other-governments/162380/>, 04.09.2020; Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 372; Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 222.

<sup>931</sup> “Kazakhstan”, **Encyclopedia Britannica**, 16.12.2021, (Çevrimiçi) <https://www.britannica.com/place/Kazakhstan>, 17.12.2021.

<sup>932</sup> Arindrajit Basu, Elonnai Hickok, Aditya Singh Chawla, “The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India”, **The Centre for Internet & Society**, 2019, s. 54.

gerektirmektedir<sup>933</sup>. Yine aynı kanunun 56 numaralı maddesi de Kişisel Veri ve Kişisel Verinin Korunması Kanunu içerisinde yer alan kişisel verilerin Kazakistan sınırları içerisinde saklanması yükümlülüğünü tekrarlamaktadır.

Kazakistan Savunma ve Havacılık Endüstrisi Bakanlığı'nın 38/NK numaralı emrine göre, Kazakistan alan adları taşıyan internet sitelerinin donanımlarının ve yazılımlarının Kazakistan toprakları içerisinde bulunması gerekmektedir<sup>934</sup>.

Kazakistan İletişim Kanunu'nun 15 numaralı maddesi de iletişim hizmetlerine ilişkin abonelik bilgilerinin Kazakistan sınırları içerisinde (istihbaratın ve adli makamların bilgi taleplerinin karşılanması amaçlarıyla) saklanmasını zorunlu kılmaktadır<sup>935</sup>. Söz konusu abonelik bilgileri abone tanımlama numarası, abonenin cihazına ilişkin tanımlayıcı kodlar, fatura bilgileri, konum bilgisi, ağ adresi, internet kaynağı tanımlama bilgisi ve veri aktarımı ağ protokollerinden oluşmaktadır.

### c. Brezilya

Brezilya, Güney Amerika'nın yüz ölçümü olarak en büyük ülkesidir.<sup>936</sup> Federal bir cumhuriyet olan Brezilya, zengin doğal kaynaklarına ve yüksek nüfusuna rağmen orta gelir grubunda yer almaktadır.

Yabancı hizmet sağlayıcıların elinde bulunan kişisel verilere erişim konusu, Brezilya'da da gündem olmuş bir konudur. Bu çerçevede **WhatsApp** uygulamasının kullanıcılarına dair verilerin, bu uygulamanın sahibi olan **Facebook** şirketi tarafından paylaşılmaması üzerine, **Facebook**'un Brezilya yöneticileri 2016 yılında

<sup>933</sup> Kanunun İngilizce tercümesi için bkz. "Kazakistan Cumhuriyeti Kişisel Veri ve Kişisel Verinin Korunması Kanunu", (09.09.2020), (Çevrimiçi) <https://adilet.zan.kz/eng/docs/Z1500000418>, 09.09.2020.

<sup>934</sup> Shyngyssov, Aset, Bakhytzhany Kadyroz, Zhamilya Bilisbekova, "Data Localization Laws: Overview (Kazakhstan)", 2019, s. 1, (Çevrimiçi) <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/data-localization-law-overview-kazakhstan.pdf>, 22.10.2020.

<sup>935</sup> Shyngyssov vd., a.y.

<sup>936</sup> "Brazil", **Encyclopedia Britannica**, 20.12.2021, (Çevrimiçi) <https://www.britannica.com/place/Brazil>, 20.12.2021.

tutuklanmıştır<sup>937</sup>. Benzer bir tutuklama işlemi yine aynı konu nedeniyle **Microsoft**'un Brezilya yöneticilerine karşı da yapılmaya çalışılmıştır<sup>938</sup>. Her iki olaydan da Brezilya'da mahkemelerin talep ettiği verilerin verilmemesinin bir suç olarak düzenlenmiş olduğu sonucuna varılabilmektedir. Ancak bu sert yaklaşıma rağmen, Brezilya'da veri lokalizasyonu gerektiren herhangi bir açık hukuki düzenleme bulunmamaktadır<sup>939</sup>.

Kamu otoritelerinin bulut hizmeti alımlarına ilişkin hükümetçe yayınlanan tavsiye kararı niteliğindeki rehber içerisinde ise milli güvenliğe ilişkin verilerin Brezilya sınırları içerisinde tutulması yönünde bir yönlendirme bulunmaktadır<sup>940</sup>.

#### d. Suudi Arabistan

Suudi Arabistan Krallığı, Arap Yarımadası'nın büyük bölümünü kaplayan ve mutlak monarşi ile yönetilen dünyadaki tek ülkedir<sup>941</sup>. Ülke aynı zamanda dünyanın en büyük petrol ve doğalgaz üreticilerinden birisi konumundadır<sup>942</sup>.

Suudi Arabistan Ulusal Siber Güvenlik Otoritesi (NCA)<sup>943</sup>, veri lokalizasyonu konusunda tüm kamu otoritelerine ve kamunun sahip olduğu şirketlere uygulanacak, Temel Siber Güvenlik Kontrolleri adında bir düzenleme yapmış durumdadır<sup>944</sup>. Düzenleme kapsamı içine Suudi Arabistan Mali Otoritesi'nin düzenleyici ve denetleyici olarak görev yaptığı bankalar, sigorta ve reasürans şirketleri, finansman

<sup>937</sup> Rob Thubron, "Facebook's Latin America VP Arrested in Brazil after Failing to Provide WhatsApp User Data Rob", **Techspot**, 2016, (Çevrimiçi) <https://www.techspot.com/news/63970-facebook-latin-america-vp-arrested-brazil-after-%20failing.html>, 10.10.2021.

<sup>938</sup> Brad Smith, "Answering Europe's Call: Storing and Processing EU Data in the EU - EU Policy Blog", 06.05.2021, (Çevrimiçi) <https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>.

<sup>939</sup> Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", s. 222.

<sup>940</sup> Mark Lewis, **Cloud Computing 2020**, 3. bs, London UK, Tom Barnes and Law Business Research Ltd., 2019, s. 34.

<sup>941</sup> "Saudi Arabia", **Encyclopedia Britannica**, 08.01.2022, (Çevrimiçi) <https://www.britannica.com/place/Saudi-Arabia>, 09.01.2022.

<sup>942</sup> "Economy of Saudi Arabia", **Encyclopedia Britannica**, 08.01.2022, (Çevrimiçi) <https://www.britannica.com/place/Saudi-Arabia/Economy#ref259141>, 09.01.2022.

<sup>943</sup> Suudi Arabistan Ulusal Siber Güvenlik Otoritesi'nin internet sitesi için bkz. "Suudi Arabistan Ulusal Siber Güvenlik Otoritesi", (27.12.2021), (Çevrimiçi) <https://www.nca.gov.sa/>, 27.12.2021.

<sup>944</sup> "Saudi Arabia Essential Cybersecurity Controls An Overview", **Thales Security Solutions & Services**, White Paper, s. 3, (10.11.2020).



şirketleri, kredi büroları ve diğer finansal sistemde görev yapan kuruluşlar da girmektedir. Söz konusu düzenleme çerçevesinde, kapsam dahilinde olan tüm kuruluşların sahip oldukları bilgileri ve teknik varlıkları ülke toprakları içerisinde tutma saklama zorunluluğu bulunmaktadır<sup>945</sup>. Bu nedenle anılan düzenlemenin kamu ve finans sektörü için geniş bir veri lokalizasyonu yükümlülüğü getirdiği sonucuna ulaşmak mümkündür.

#### **IV. VERİ LOKALİZASYONU KURALLARININ MİLLETLERARASI ÖZEL HUKUK VE USUL HUKUKU AÇISINDAN ÖNEMİ**

Veri lokalizasyonu yükümlülüğü getiren kurallar, kamu hukuku niteliğindeki kurallardır. Yani bunlar nitelik itibarıyla kişiler arasındaki ilişkileri düzenleyen özel hukuk kuralları olarak sınıflandırılmamaktadır. Dolayısıyla veri lokalizasyonu kuralları ile kanunlar ihtilafı kuralları arasında herhangi bir direkt ilişki bulunmamaktadır. Ayrıca kanunlar ihtilafı kuralları içerisinde verilerin konumu, bir bağlama noktası olarak ele alınmamıştır. Dolayısıyla verilerin konumu, herhangi bir özel hukuk ilişkisinin tabi olacağı hukuku belirleyen bir faktör de değildir. Öte yandan belirtmek gerekir ki veri lokalizasyonu yükümlülükleri ile belirlenen verilerin konumu, aynı zamanda mülklik ilkesi çerçevesinde verilere uygulanacak hukuku da tespit etmiş olmaktadır.

Veri lokalizasyonu kuralları, verilere hangi hukukun uygulanacağını kanunlar ihtilafındaki bir bağlama kuralı gibi göstermemektedir<sup>946</sup>. Ancak veri lokalizasyonu yükümlülüğü getiren kurallar, kamu hukukunun bir parçası oldukları için doğrudan uygulanan kural niteliğindedirler. İşte bu nedenle kanunlar ihtilafı kuralları çerçevesinde yabancı hukuku uygulayan bir ülke mahkemesi, kendi kanunlar ihtilafı

---

<sup>945</sup> a.g.e., s. 4.

<sup>946</sup> Her ne kadar MÖHUK m. 35/3 ile İsviçre Federal Milletlerarası Özel Hukuk Kanunu m. 139/3, kişisel verilerin işlenmesi veya kişisel verilere ilişkin bilgi alma hakkının sınırlandırılması nedenleriyle kişilik hakkı ihlallerinden doğacak taleplere uygulanacak hukukun tespitine yönelik bir kural getirmekteyse de bu bağlama kuralı esasen taraflar arasındaki haksız fiil ilişkisine uygulanacak hukuku tespit etmektedir. Kişisel verilere uygulanacak hukuk (örneğin KVKK ya da GDPR) kanunlar ihtilafı kuralları çerçevesinde belirlenmemektedir.

kurallarının doğrudan uygulanan kurallara ilişkin normları çerçevesinde veri lokalizasyonu yükümlülüklerine muamele yapmalıdır. Ayrıca veri lokalizasyonu yükümlülüğünün niteliğine bağlı olarak söz konusu yükümlülüğün kamu düzenine ilişkin bir kural olduğu sonucuna varmak da mümkün olabilecektir. Dolayısıyla hukuk mahkemeleri önüne gelen yabancılık unsuru taşıyan bir uyumsuzlukta, veri aktarımı söz konusuysa; veri lokalizasyonuna ilişkin kurallar da yukarıda bahsedilen kavramlar çerçevesinde dikkate alınmalıdır.

Milletlerarası özel hukuk kapsamında verilerin lokalizasyonu yükümlülüklerinin iki ana inceleme alanı açısından önemi bulunmaktadır. Bunlardan ilki milletlerarası istinabedir. İkincisi ise yabancı yatırımlar ve milletlerarası ticaret alanıdır. Aşağıdaki başlıklar altında bu iki konu ile veri lokalizasyonu yükümlülüklerinin etkileşimi incelenecektir.

#### **A. Milletlerarası İstinabe ile Veri Lokalizasyonu Yükümlülüğü Kurallarının İlişkisi**

Milletlerarası istinabe, farklı devlet mahkemelerinin adli faaliyetlerini yürütebilmek adına birbirleri ile yardımlaşmaları olarak tanımlanabilmektedir. Örneğin bir Türk mahkemesinin, Almanya’da bulunan bir tanığın dinlenmesini Alman mahkemelerinden istemesi, milletlerarası istinabe süreçlerine bir örnek teşkil etmektedir. Yine bir mahkemenin yabancı bir ülkede bulunan delilleri, o ülke mahkemesinden talep etmesi de milletlerarası istinabe kapsamında değerlendirilmektedir<sup>947</sup>.

Teknolojinin yoğun bir şekilde kullanıldığı günümüz dünyasının hemen her adli olayında, dijital ortamda bulunan delillerin toplanması ihtiyacı gündeme gelmektedir<sup>948</sup>. Dijital ortamda bulunan deliller (yani veriler), esasen bahse konu dijital hizmetin sağlandığı veri merkezinde bulunmaktadır. Örneğin **Facebook**

<sup>947</sup> Brehmer, “Data Localization: The Unintended Consequences of Privacy Litigation”, s. 950.

<sup>948</sup> **Commission Staff Working Document Impact Assessment**, Brussels, European Commission, 2018, s. 5, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN>, 10.11.2020.

üzerinden gerçekleşen ve hakaret içeriği bulunan bir konuşmanın kaydı, **Facebook**'a ait olan ve Türkiye'ye hizmet sunan veri merkezi içerisinde bulunmaktadır. İşte bu veri merkezi içerisinde bulunan ve delil niteliği taşıyan verilere erişmek için, Türk mahkemelerinin milletlerarası istinabe süreçleri kapsamında verilerin bulunduğu ülke makamlarından talepte bulunması gerekmektedir. Milletlerarası istinabenin nasıl işleyeceği, talep gönderen ve talebin muhatabı olan devletler arasında bulunan milletlerarası sözleşmelere göre belirlenmektedir. Eğer taraflar arasında bir milletlerarası sözleşme bulunmuyorsa, bu durumda konu milletlerarası nezaket doktrini kapsamında ilgili devletlerin tercihlerine bırakılmaktadır<sup>949</sup>.

Günümüzde milletlerarası istinabe süreçlerinin etkin ve hızlı bir şekilde çalıştığını söylemek mümkün değildir. Genellikle milletlerarası istinabe süreçlerinden sonuç almak birkaç yılı bulabilmektedir<sup>950</sup>. Bu durum yargılama sürelerini aşırı şekilde uzatmaktadır. Ayrıca milletlerarası istinabe başvurusu sonucunda, muhatap devletten olumlu bir yanıt alma garantisi de bulunmamaktadır. Yani yıllarca bekleme sonucunda istinabe talebinin olumsuz sonuçlanması mümkündür.

Milletlerarası istinabe süreçlerine yönelik olarak mahkemelerin ciddi rahatsızlıkları olduğu gözlemlenmektedir<sup>951</sup>. Nitekim Türk mahkemeleri de yurtdışı merkezli sosyal medya şirketlerine yönelik bilgi taleplerinin önemli bir kısmına olumlu yanıt alamamaktadır<sup>952</sup>. Önceki bölümde açıklanan CLOUD Act çerçevesinde ABD'nin üçüncü taraf ülkelerle imzalamaya başladığı veri paylaşım sözleşmelerini, bu sorunları çözen yeni nesil istinabe sözleşmeleri olarak kabul etmek kanaatimizce mümkün

---

<sup>949</sup> **a.g.e.**, s. 48.

<sup>950</sup> Brehmer, "Data Localization: The Unintended Consequences of Privacy Litigation", s. 951.

<sup>951</sup> "In the United States District Court for the Eastern District of Pennsylvania Memorandum of Decision", s. 27; **Commission Staff Working Document Impact Assessment**, s. 25.

<sup>952</sup> 7253 sayılı Kanun ile yapılan değişiklik neticesinde 5651 numaralı Kanun'a eklenen ek madde 4, Türkiye'de günlük erişimi 1 milyondan fazla olan yurtdışı kaynaklı sosyal ağ sağlayıcılarına Türkiye'de yerleşik bir gerçek ya da tüzel kişi temsilci atama zorunluluğu getirmiştir. Ancak kanaatimizce bu adım, verilerin konumunu ve dolayısıyla uygulanacak hukuku değiştirmede için muhatap temsilcilere bildirim gitse dahi bu kişilerin tabi oldukları yabancı hukuk ile Türk hukuku arasındaki hukukların çatışması sorunu giderilemeyecektir. Bu nedenle de yapılacak tebligatların, talep edilen verilere erişimi kolaylaştırmayacağı düşünülmektedir. Nitekim ilgili sosyal ağ sağlayıcılarca yapılan açıklamalarda da temsilci atanmanın bilgi ve içerik kaldırma taleplerine ilişkin değerlendirme süreçlerinde herhangi bir farklılık yaratmayacağı vurgulanmıştır.

olabilecektir. Ancak bu sözleşmelerin, her ülke ile imzalanması söz konusu olmadığı gibi veri paylaşım talepleri konusunda ABD'nin de kabulünü gerektirdiği için istinabe konusunda veri lokalizasyonu yükümlülüklerinin yerini alabilecek bir çözüm teşkil edemeyecekleri düşünülmektedir.

Milletlerarası istinabe süreçlerinin yetersizliği, devletleri veri lokalizasyonu yükümlülüğü getirmeye iten sebeplerden bir tanesini oluşturmaktadır. Verilerin yurtdışında bulunması, verilere erişim açısından ilgili devletin uluslararası uygulama ve yargılama yetkilerini kullanmasını engelleyen bir durumdur. Zira uluslararası yargı ve uygulama yetkisinin ülke dışında kullanımı, yukarıda da detaylıca açıklandığı üzere, fiilen mümkün olmamaktadır. Bu nedenle de ilgili devlet mahkemeleri, kendilerine gereken delillere erişebilmek için milletlerarası istinabe süreçlerine mahkûm olmakta; bu süreçlerin de gereği gibi çalışmaması nedeniyle de görevlerini layıkıyla yapamaz hale gelmektedirler. Veri lokalizasyonu yükümlülükleri ise verilerin ülke içerisinde kalmasını sağlayarak uluslararası yargı ve uygulama yetkisinin kullanılabilmesini temin etmekte ve aynı zamanda milletlerarası istinabe süreçlerine başvurma ihtiyacını ortadan kaldırmaktadır.

Veri lokalizasyonu yükümlülükleri aynı zamanda ülke içerisinde saklanmakta olan verilere yabancı devletlerin erişimini de milletlerarası istinabe prosedürlerine bağlamaktadır. Böylelikle ev sahibi devlet, yabancı devletlerin veriye erişimleri üzerinde de kontrol sahibi olabilmektedir<sup>953</sup>.

## **B. Serbest Ticaret Anlaşmaları ve Doğrudan Yabancı Yatırımlar ile Veri Lokalizasyonu Yükümlülüğü Kurallarının İlişkisi**

Veri lokalizasyonu yükümlülükleri, aynı zamanda çeşitli ekonomik etkiler doğurmaktadır. Önceki başlıklarda detaylıca açıklanan bu etkiler, serbest ticaret anlaşmaları ve yabancı yatırımlar açısından kendilerini hukuk dünyasında da göstermektedirler. Aşağıdaki başlıklar altında öncelikle veri lokalizasyonu

---

<sup>953</sup> Önemle belirtmek gerekir ki bu kontrol, sadece hukuki erişim taleplerinin yanıtlanması noktasında mevcuttur. İstihbarat faaliyetleri kapsamında teknik yöntemlerle gerçekleştirilebilecek erişim teşebbüslerini bu ifade kapsamında değerlendirmemek gerekmektedir.

yükümlülüklerinin serbest ticaret anlaşmaları içerisinde nasıl ele alındığı konusu incelenecektir. Daha sonrasında ise veri lokalizasyonu yükümlülüklerinin doğrudan yabancı yatırımlar açısından doğurduğu sonuçlar üzerinde durulacaktır.

## 1. Serbest Ticaret Anlaşmaları ile Veri Lokalizasyonu Yükümlülükleri İlişkisi

Kişisel verilerin korunması hukuku ve uluslararası ticaret hukuku, İkinci Dünya Savaşından sonra birbirlerinden bağımsız olarak gelişen iki farklı alan olmuştur<sup>954</sup>. Ancak 1980’li yıllarla birlikte uluslararası veri aktarımı imkanlarının gelişmesi, her iki hukuk dalının birbirleri ile etkileşime girmesini sağlamıştır<sup>955</sup>. Yapay zekâ ve büyük veri gibi verilerin ekonomik değerini arttıran yeni gelişmeler, devletlerin veriler üzerindeki ilgisini iyice arttırmıştır. Bu durum da veri lokalizasyonu yükümlülüklerinin doğmasında etkin olan nedenlerden birini teşkil etmektedir.

Veri lokalizasyonu yükümlülükleri, uluslararası veri akışını yavaşlattığı ya da kestiği için uluslararası ticareti de olumsuz etkilemektedir<sup>956</sup>. Aynı zamanda uluslararası veri akışına dayalı olarak sunulabilen hizmetlerin (örneğin sosyal medya ya da bulut bilişim gibi) ticareti de veri lokalizasyonu yükümlülükleri mümkün olmayabilmektedir<sup>957</sup>. Örneğin ülkemizde veri lokalizasyonu yükümlülüğü altında bulunan kişilerin bulut bilişim hizmeti satın almaları ticari açıdan anlamsız hale gelmektedir. İşte bu sebeplerle veri lokalizasyonuna ya da uluslararası veri akışına ilişkin hükümler, artık serbest ticaret anlaşmaları müzakereleri içerisinde de ele alınmakta ve anlaşma metinlerinde kendisine yer bulabilmektedir<sup>958</sup>.

---

<sup>954</sup> Tian, “Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement”, s. 393; Burri, “Interfacing Privacy and Trade”, s. 35.

<sup>955</sup> Fraser, “Data Localisation and the Balkanisation of the Internet”, s. 368; Burri, “Interfacing Privacy and Trade”, s. 37.

<sup>956</sup> Mishra, “Data Localization Laws in a Digital World”, s. 142; “Mapping Approaches to Data and Data Flows”, s. 11; Christian Ketels, Arindam Bhattacharya, Liyana Satar, “Global Trade Goes Digital”, **BCG Henderson Institute**, (12.08.2019), (Çevrimiçi) <https://www.bcg.com/publications/2019/global-trade-goes-digital>, 19.05.2020.

<sup>957</sup> Mitchell, Mishra, “Data at the Docks: Modernizing International Trade Law for the Digital Economy”, s. 1112.

<sup>958</sup> Selby, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, s. 217; Mira Burri, “The Regulation of Data Flows through Trade Agreements”, **Georgetown Journal of International Law**, C. 48, S. 2, 2017, s. 408.

Daha önceki başlıklarda açıklanan ülkelere göre veri lokalizasyonu yükümlülüklerinden de anlaşılabilirliği üzere, ülkeler veri lokalizasyonu konusunda farklı politikalar izlemektedir. Dünyadaki teknoloji şirketlerinin büyük çoğunluğuna ev sahipliği yapan ABD, veri lokalizasyonuna karşı durmakta ve serbest ticaret anlaşmaları içerisinde serbest veri akışını güvenceye alan (yani veri lokalizasyonunu yasaklayan ya da sınırlayan) hükümlere yer vermeye çalışmaktadır<sup>959</sup>. Rusya, Çin ve diğer uzak doğu ülkeleri (Japonya hariç) veri lokalizasyonu yükümlülüklerini geniş kapsamlı olacak şekilde uygulamaya almaktadır. AB ise veri akışını sınırlayıcı hükümler ile yerel veri depolama ve işleme kapasitesini arttırmaya yönelik politikaları birleştirerek verileri kendi sınırları içerisinde tutmayı hedeflemektedir. Ancak AB, bağlayıcı veri lokalizasyonu hükümleri getirmekten kaçınmakta ve bu konuyu serbest ticaret anlaşmaları içerisinde düzenleme konusunda ihtiyatlı davranmaktadır<sup>960</sup>. Ülkelerin bu çeşitli yaklaşımları, serbest ticaret anlaşmaları çerçevesindeki duruşlarını da etkilemektedir.

Ülkemizin durumuna bakıldığında ise Rusya, Çin ve diğer uzak doğu ülkelerine benzer şekilde veri lokalizasyonu yükümlülüklerinin geniş bir şekilde benimsendiği görülmektedir. Ancak çalışmamız tarihi itibarıyla ülkemizin taraf olduğu serbest ticaret anlaşmaları içerisinde veri lokalizasyonu konusunu gündemine almış olan bir anlaşma bulunmamaktadır.

## **2. Serbest Ticaret Anlaşmaları İçerisinde Veri Lokalizasyonu Yükümlülüklerinin Ele Alınışı**

Dünya ticaretini düzenleyen kurallar, 163 devletin üye olduğu DTÖ<sup>961</sup> nezdinde uluslararası anlaşmalar yoluyla vücuda getirilmektedir. Kişisel verilerin korunması ya da veri lokalizasyonu gibi konular ise henüz DTÖ tarafından ele alınmamıştır.

---

<sup>959</sup> Burri, “Interfacing Privacy and Trade”, s. 67; Taylor, “‘Data Localization’: The Internet in the Balance”, s. 5; Mitchell, Mishra, “Data at the Docks: Modernizing International Trade Law for the Digital Economy”, s. 1078; Mira Burri, “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions”, *Journal of World Investment & Trade*, C. 22, 2021, s. 2.

<sup>960</sup> Burri, “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions”, s. 15.

<sup>961</sup> DTÖ’nün açılımı, “Dünya Ticaret Örgütü” şeklindedir. İnternet sitesi için bkz. “World Trade Organization”, (28.09.2017), [https://www.wto.org/english/tratop\\_e/region\\_e/regfac\\_e.htm](https://www.wto.org/english/tratop_e/region_e/regfac_e.htm), 28.09.2017. (Çevrimiçi)

Dolayısıyla DTÖ nezdinde imzalanan anlaşmalar, bu konuyu direkt olarak değerlendirmemektedir.

Dünya ticaretini düzenleyen GATT<sup>962</sup> ve GATS<sup>963</sup> adlı iki önemli anlaşma bulunmaktadır. GATT m. XX ile GATS m. XIV, akit devletlerin serbest ticareti engelleme amacı olmamak kaydıyla, söz konusu anlaşmalardaki yükümlülüklerini ihlal edebilecek önlemleri almalarına imkân vermiştir. Bu önlemlerin alınabilme gerekçelerinden bazıları kamu düzeninin ya da kamu ahlakının korunması, mevcut mevzuata uyum sağlanması ya da çevrenin korunması şeklindedir. Veri lokalizasyonu yükümlülüklerinin bu istisnalar kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin herhangi bir içtihat bulunmamakta olduğu için belirsizlikler mevcuttur<sup>964</sup>. Ancak bazı görüşlere göre GDPR'ın veri akışına ilişkin hükümlerinin dahi söz konusu istisnalar kapsamında değerlendirilemeyeceği ve anlaşmalara aykırılık teşkil edeceği öne sürülmektedir<sup>965</sup>. Bir diğer görüş ise veri lokalizasyonu yükümlülüklerinin GATS'ı ihlal ettiği yönündedir<sup>966</sup>. Aksi yönde bir görüş de uluslararası veri akışını engelleyen yükümlülüklerin GATS m. XIV kapsamında getirilebileceğini

---

<sup>962</sup> “The General Agreement on Tariffs and Trade”, World Trade Organization, 07.1986, (Çevrimiçi) [https://www.wto.org/english/docs\\_e/legal\\_e/gatt47\\_e.pdf](https://www.wto.org/english/docs_e/legal_e/gatt47_e.pdf), 12.12.2021.

<sup>963</sup> “The General Agreement on Trade in Services”, World Trade Organization, 01.1995, (Çevrimiçi) [https://www.wto.org/english/docs\\_e/legal\\_e/26-gats\\_01\\_e.htm](https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm), 12.12.2021.

<sup>964</sup> Andrew D. Mitchell, Jarrod Hepburn, “Don’t Fence Me In: Reforming Trade And Investment Law To Better Facilitate Cross-Border Data Transfer”, **Yale Journal of Law & Technology**, C. 19, 2017, s. 206; Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation”, **U.C. Davis Law Review**, C. 51, S. 1, 2017, s. 85; Joshua D. Blume, “Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization, and Cybersecurity Laws”, **Georgetown Journal of International Law**, C. 49, S. 2, 2018, s. 840; Nivedita Sen, “Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?”, **Journal of International Economic Law**, C. 21, S. 2, 2018, s. 337; Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures”, s. 596; Neha Mishra, “Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows”, **Vanderbilt Journal of Transnational Law**, C. 52, S. 2, 2019, s. 506; Abe Yoshinori, “Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?”, s. 25.

<sup>965</sup> Burri, “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions”, s. 12; Blume, “Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization, and Cybersecurity Laws”, s. 842.

<sup>966</sup> Crosby, **Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments**, s. 10; Sen, “Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?”, s. 335.

savunmaktadır<sup>967</sup>. Ayrıca belirtmek gerekir ki aşağıda açıklanan Kapsayıcı ve İlerici Trans-Pasifik Ortaklığı Anlaşması'nın GATS'ın veri lokalizasyonu konusundaki hükümlerine göre daha makul hükümler içerdiği belirtilmesine rağmen GATS'ın bu konudaki en önemli uluslararası anlaşma olma özelliğini sürdürdüğü ifade edilmektedir<sup>968</sup>. Yine de DTÖ nezdindeki anlaşmalar çerçevesinde veri lokalizasyonu yükümlülükleri konusunun çözülmesinin mümkün olmayacağını ifade eden görüşler de bulunmaktadır<sup>969</sup>.

Serbest ticaret anlaşmaları içerisinde veri lokalizasyonu ya da verilerin serbest akışı konusundaki hükümlerde artış trendi olduğu gözlemlenmektedir<sup>970</sup>. Yapılan araştırmalara göre 2008 ile 2019 arasında imzalanan, 72 farklı ülkenin taraf olduğu toplam 29 çift ya da çok taraflı anlaşma içerisinde bu konuya ilişkin hükümlere yer verilmiştir<sup>971</sup>. Söz konusu anlaşmalar içerisinde temel olarak üç tipte maddeler bulunduğu görülmektedir<sup>972</sup>. Bunlar bağlayıcı olmayan tavsiye niteliğindeki veya gelecekte tekrar müzakere öngören maddeler, veri akışının hiçbir sınırlamaya tabi tutulmadan gerçekleşmesini öngören maddeler ve veri akışını engelleyen bazı istisnalara izin veren maddeler olarak sıralanmaktadır. Son gruptaki istisnai durumlar ise farklı muamele öngörmemek ve sadece serbest ticareti engelleme amacı taşımamak kaydıyla kamu düzenine ve kamu politikalarına yönelik meşru amaçlar olarak özetlenebilmektedir.

---

<sup>967</sup> Mitchell, Mishra, "Data at the Docks: Modernizing International Trade Law for the Digital Economy", s. 1094; Victoria Conrad, "Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data", **William and Mary Business Law Review**, C. 10, S. 1, 2018, s. 333; Burri, "Interfacing Privacy and Trade", s. 62; Wong, "Data Localization and ASEAN Economic Community", s. 162.

<sup>968</sup> Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures", s. 607.

<sup>969</sup> Burri, "Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions", s. 17; Burri, "Interfacing Privacy and Trade", s. 86; Yine de veri lokalizasyonu konusunun DTÖ gündeminde olduğuna dair bkz. Bernard Hoekman, Petros C. Mavroidis, "WTO Reform: Back to the Past to Build for the Future", **Global Policy**, No: 12, 2021, s. 6.

<sup>970</sup> "Mapping Approaches to Data and Data Flows", s. 34; Burri, "Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions", s. 3.

<sup>971</sup> Casalini, González, Nemoto, "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers", s. 25.

<sup>972</sup> Casalini, González, Nemoto, **a.g.e.**, s. 27.



Aynı araştırma çerçevesinde bağlayıcılık açısından yapılan sınıflandırmaya bakıldığında, 13 anlaşmanın konuya ilişkin bağlayıcı hükümler, 13 tanesinin tavsiye niteliğinde hükümler öngördüğü; 3 tanesinin ise konuyu gelecekteki müzakerelere bıraktığı anlaşılmaktadır<sup>973</sup>.

Bağlayıcı hükümler taşıyan anlaşmalar incelendiğinde ise ana kural olarak veri akışının serbestçe gerçekleşmesinin kabul edildiği; ancak farklı muamele öngörmek ve sadece serbest ticareti engelleme amacı taşımamak kaydıyla kamu düzeni ve kamu politikalarına yönelik meşru amaçlar çerçevesinde istisnai olarak veri akışının sınırlanabilmesi yaklaşımının benimsendiği görülmektedir<sup>974</sup>. Bu anlaşmalara örnek olarak 13 pasifik ülkesinin taraf olduğu Kapsayıcı ve İlerici Trans-Pasifik Ortaklığı Anlaşması<sup>975</sup>; ABD, Meksika ve Kanada Anlaşması<sup>976</sup> ile Birleşik Krallık ve Japonya Kapsayıcı Ekonomik Ortaklık Anlaşması'nı<sup>977</sup> örnek olarak göstermek mümkündür<sup>978</sup>. Ayrıca Birleşik Krallık ve Japonya arasında imzalanacak ticaret anlaşmasında veri lokalizasyonunun yasaklanması yönünde taraflar arasında prensipte uzlaşma sağlanmıştır<sup>979</sup>.

ABD, Meksika ve Kanada Anlaşması'nın 19.11 numaralı maddesi, uluslararası veri akışının, yukarıda açıklanan istisnalar haricinde yasaklanamayacağını açıkça ifade etmektedir. 19.12 numaralı madde ise bilgi sistemlerinin ilgili ülke sınırları içerisinde bulunmasının, o ülkede ticari faaliyet yürütmek için ön koşul olarak belirlenemeyeceği hüküm altına alınmıştır. Kapsayıcı ve İlerici Trans-Pasifik Ortaklığı Anlaşması'nın

---

<sup>973</sup> Casalini, González, Nemoto, **a.g.e.**, s. 28.

<sup>974</sup> Casalini, González, Nemoto, **a.y.**

<sup>975</sup> “Trans-Pacific Partnership Agreement (TPPA)”, 2015, (Çevrimiçi) <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text>, 12.12.2021.

<sup>976</sup> “The United States-Mexico-Canada Agreement (USMCA)”, Congressional Research Service, 2021, (Çevrimiçi) <https://sgp.fas.org/crs/row/R44981.pdf>, 14.01.2022.

<sup>977</sup> “UK-Japan Comprehensive Economic Partnership Agreement”, 2020, (Çevrimiçi) <https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020>, 12.10.2021.

<sup>978</sup> Mishra, “Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows”, s. 506; Burri, “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions”, s. 9.

<sup>979</sup> Aditi Agrawal, “UK-Japan agree to trade deal that bans data localisation”, **Medianama**, (11.09.2020), (Çevrimiçi) <https://www.medianama.com/2020/09/223-uk-japan-trade-deal-ban-data-localisation/>, 26.11.2020.

14.11 numaralı maddesi yukarıda açıklanan istisnalarla birlikte uluslararası serbest veri akışının serbest olduğunu hüküm altına almaktadır. Bu anlaşmanın 14.13 numaralı maddesi, yukarıda sayılan istisnai durumlar ile bilgi sistemlerinin ilgili ülke sınırları içerisinde bulundurulmasını, o ülkede ticari faaliyet yürütmek için ön koşul olarak arama yasağına da istisna olarak tanımlamıştır. Ancak söz konusu 14.11 ve 14.13 numaralı maddelerin nasıl uygulanacağı, henüz belirsizliğini korumaktadır<sup>980</sup>. Öte yandan bahse konu anlaşmanın, serbest veri akışının sağlanmasını; veri güvenliği ve gizliliğinden önde tuttuğuna dair görüş de bulunmaktadır<sup>981</sup>. Birleşik Krallık ve Japonya Kapsayıcı Ekonomik Ortaklık Anlaşması'nın 8.84 ve 8.85 numaralı maddeleri de yukarıda açıklananlar ile büyük ölçüde aynı hükümleri içermektedir. Öte yandan, AB'nin taraf olduğu serbest ticaret anlaşmalarına bu tür hükümler ekleme konusunda çekimser kaldığını da ifade etmek gerekmektedir<sup>982</sup>.

Uluslararası veri akışının uluslararası ticaretteki önemi arttıkça, bu konuya ilişkin hükümler öngören serbest ticaret anlaşmalarının sayısının artmasını beklemek, kanaatimizce makul olacaktır. Nitekim uluslararası ticarete ilişkin DTÖ anlaşmalarının yenilenmesine ilişkin görüşler doktrinde halihazırda ileri sürülmektedir<sup>983</sup>. Ancak henüz ülkemizin taraf olduğu serbest ticaret anlaşmaları içerisinde veri lokalizasyonu ya da serbest veri akışını düzenleyen hükümler içeren herhangi bir anlaşma bulunmamaktadır. Türkiye'de mevcut olan veri lokalizasyonu yükümlülükleri düşünüldüğünde, bu konuları içeren serbest ticaret anlaşmalarının müzakerelerinin dikkatli şekilde yürütülmesi gerekecektir. Kanaatimizce ülkemizde bulunan bazı veri lokalizasyonu yükümlülüklerini, örnek olarak verilen anlaşma hükümlerindeki istisnalara dayandırmak mümkün olabileceksede çoğu yükümlülük için aynı sonuca varmak mümkün olmayacaktır. Dolayısıyla ileride imzalanacak

---

<sup>980</sup> Hodson, "Applying WTO and FTA Disciplines to Data Localization Measures", s. 600; Abe Yoshinori, "Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?", s. 26; Burri, "Interfacing Privacy and Trade", s. 71.

<sup>981</sup> Ida Madieha Abdul Ghani Azmi, Jeong Chun Phuoc, "International Norms in Regulating Commerce: The Electronic Commerce Chapter of the Comprehensive Trans-Pacific Partnership Agreement", **International Journal of Business and Society**, 2020, s. 75.

<sup>982</sup> Burri, "Interfacing Privacy and Trade", s. 73.

<sup>983</sup> Mitchell, Mishra, "Data at the Docks: Modernizing International Trade Law for the Digital Economy", s. 1109.

serbest ticaret anlaşmaları müzakereleri sırasında ülkemizin ekonomik menfaatleri ile veri lokalizasyonu yükümlülükleri arasında bir seçim yapmak gerekebilecektir.

### **3. Veri Lokalizasyonu Yükümlülüklerinin Doğrudan Yabancı Yatırımlar Açısından Etkileri**

OECD tarafından yapılan tanıma göre<sup>984</sup> doğrudan yabancı yatırım, ev sahibi ülke içerisinde, başka bir ülkede yerleşik olan müteşebbisin uzun süreli menfaat yaratmak amacıyla gerçekleştirdiği yatırım kategorisini ifade etmektedir. Buradaki uzun süreli menfaatten kasıt, müteşebbis ile ticari işletmesi arasında uzun süreli bir ilişki kurulması ile bu işletmenin yönetiminin büyük ölçüde müteşebbis etkisi altında olmasıdır.

ICSID Konvansiyonu çerçevesinde verilen tahkim kararları çerçevesinde doğrudan yabancı yatırım kavramının ne şekilde tanımlanması gerektiğine ilişkin olarak birçok farklı görüş bulunmaktadır. Söz konusu görüşler kavramın tanımının tahkim taraflarının iradelerine bırakılması ya da hakem kararlarında belirtilen birtakım kriterlerin kullanılması gibi farklı fikirleri öne sürmektedirler<sup>985</sup>. Yine de ana hatlar itibarıyla söz konusu tanımların OECD tarafından verilen tanım ile esaslı şekilde farklılaştığını söylemek düşüncemize göre mümkün değildir.

Doğrudan yabancı yatırımlar ile veri lokalizasyonu kavramlarının ilişkisini kurabilmek için öncelikle odaklanılması gereken nokta, veri lokalizasyonu yükümlülüklerinin etkilediği hususların doğrudan yabancı yatırım teşkil edip etmediğidir. Veri lokalizasyonu yükümlülükleri, verilerin belirli bir ülke sınırları

<sup>984</sup> “Glossary of Foreign Direct Investment Terms and Definitions”, OECD, 30.04.2008, s. 7, (Çevrimiçi) <https://www.oecd.org/daf/inv/investment-policy/2487495.pdf>, 28.10.2021.

<sup>985</sup> ICSID Yatırım Tahkimi kapsamında verilen kararlardan birisi olan Salini kararı (Salini Costruttori S.p.A. and Italstrade S.p.A. v. Kingdom of Morocco, Decision on Jurisdiction, ARB/00/4, [International Centre for Settlement of Investment Disputes 23 Temmuz 2001]) ; , gereğince yatırım kavramından bahsedebilmek için; ev sahibi ülkeye sermaye anlamında önemli miktarda katkı sağlaması, yatırımın belirli bir süre boyunca yapılmış olması, yatırımcının risk taşıyor olması ve ev sahibi devletin ekonomik gelişimine katkı sunuyor olması kriterlerinin sağlanmış olması gerekmektedir (Melis Avşar, “The Concept of Investment Under The ICSID Convention”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni**, C. 37, S. 2, 2017, s. 117; Mitchell, Hepburn, “Don’t Fence Me In: Reforming Trade And Investment Law To Better Facilitate Cross-Border Data Transfer”, s. 217).

dışarısına çıkarılmasını yasaklamak veya bilgi sistemlerinin konumlarına ilişkin kurallar belirlemek suretiyle yabancı ülkede bulunan veri merkezlerinin kullanımını engellemektedir. Kanaatimizce, bir ülkeden başka bir ülkeye çevrimiçi hizmet sunma kapasitesinin oluşturulması, özellikle ICSID Konvansiyonu çerçevesinde bir doğrudan yabancı yatırım olarak kabul edilmelidir<sup>986</sup>. Ancak söz konusu kapasitenin doğrudan yabancı yatırım olarak kabul edilmesi, veri lokalizasyonu yükümlülüklerinin her durumda doğrudan yabancı yatırımlara ilişkin korumaların ihlal edildiği anlamına gelmemektedir. Kanaatimizce bu korumaların ihlal edip edilmediği, her bir olay özelinde değerlendirilmelidir.

Yabancı yatırımlar hukuku çerçevesinde doğrudan yabancı yatırımların korunması için yabancılarla yerlilerin eşit muameleyle tutulması, yabancı yatırımların kamulaştırılması konusunda çeşitli kurallar benimsenmesi ve yabancı yatırımcıların yatırımlarından elde ettikleri geliri yurtdışına aktarabilmesine izin verilmesi şeklinde ilkesel düzenlemeler yapılmıştır. Veri lokalizasyonu yükümlülüklerinin kanaatimizce söz konusu ilkelere aykırılık teşkil etmesi söz konusu değildir. Çünkü veri lokalizasyonu yükümlülükleri, bir ülke içerisinde verilerin saklanması ya da verilerin o ülkeden çıkarılmamasını emreden kurallar olarak yerli ya da yabancı tüm kişilere uygulanacak şekilde getirilmektedir. Dolayısıyla eşitlik ilkesinin zedelenmesi söz konusu olmamaktadır<sup>987</sup>. Veri lokalizasyonu yükümlülüklerinin kamulaştırma ya da dolaylı kamulaştırma<sup>988</sup> teşkil etmesi de bizim de katıldığımız görüşe göre mümkün değildir<sup>989</sup>. Zira veri lokalizasyonu yükümlülükleri vasıtasıyla yabancı yatırım sayılabilecek hususların mülkiyetine müdahale edilmesi söz konusu olmamaktadır. Öte yandan, somut olayın hal ve şartları değerlendirilerek veri lokalizasyonu yükümlülüğü olmayan bir sektörde faaliyet gösteren bir yabancı yatırımcının yatırımlarının, veri lokalizasyonu yükümlülükleri vasıtasıyla dolaylı kamulaştırmaya tabi tutulabilmesi de ihtimal dahilindedir.

---

<sup>986</sup> Uzun, “Cloud Computing as an Investment under the ICSID Convention”, s. 539.

<sup>987</sup> Mitchell, Hepburn, “Don’t Fence Me In: Reforming Trade And Investment Law To Better Facilitate Cross-Border Data Transfer”, s. 224.

<sup>988</sup> Kavramın tanımı için bkz. Zeynep Nalçacıoğlu Erden, **Milletlerarası Yatırım Hukukunda Dolaylı Kamulaştırma**, İstanbul, XII Levha Yayıncılık, 2015, s. 50.

<sup>989</sup> Mitchell, Hepburn, “Don’t Fence Me In: Reforming Trade And Investment Law To Better Facilitate Cross-Border Data Transfer”, s. 223.

Hukuki açıdan olmasa da veri lokalizasyonu yükümlülüklerinin yabancı yatırımlar için bir engel teşkil etmesi de bilinen bir gerçektir. Örneğin, veri lokalizasyonu yükümlülükleri sebebiyle dünyanın en büyük ödeme hizmeti ve elektronik para sağlayıcılarından birisi olan **PayPal**, Türkiye’deki faaliyetlerine son vermiştir<sup>990</sup>. Benzer şekilde **Google**, Rusya’daki ofisine getirilen veri lokalizasyonu yükümlülükleri nedeniyle kapatmıştır<sup>991</sup>. Yine birçok yabancı ülkede de hem yabancı yatırımcıların hem de diğer devletlerin, yerel veri lokalizasyonu yükümlülüklerinden rahatsız oldukları görülmektedir. Zira veri lokalizasyonu yükümlülüklerinin, uluslararası şirketlerin işleyişlerini bozucu etkisi bulunmaktadır. Bu bozucu etki nedeniyle faaliyetleri etkilenen şirketlerin menşei oldukları devletler de veri lokalizasyonu yükümlülüklerinden rahatsız olmaktadır.

Yabancı yatırımcılar açısından veri lokalizasyonu yükümlülüklerinin yarattığı sorunların en başında, yatırım kapsamında kurulacak şirketin ana şirket ile bağlantısının kesilmesi sorunu gelmektedir<sup>992</sup>. Yabancı yatırımcı genellikle ana şirketi ile yatırım niteliğinde olan bağlı şirketin tüm sistemlerinin entegre olarak çalışmasını ve bu şirketler arasında sürekli olarak veri akışı olmasını beklemektedir. Bu veri akışı sayesinde hem bağlı şirket denetlenebilmekte hem de bağlı şirketin verilerinin güvenliğinin sağlanabilmesi amaçlanmaktadır. Ayrıca söz konusu veri akışı, yeni bilgi sistemi altyapısı yatırımlarının yapılması ihtiyacını da azaltabilmektedir.

Sosyal medya ve bulut bilişim gibi teknoloji temelli hizmetler sunan şirketler için ise veri lokalizasyonu yükümlülükleri, yabancı ülkede bulunan veri merkezlerinin kullanılamaması anlamına gelmektedir. Bu da söz konusu şirketlerin faaliyette bulunmak istedikleri ülkede veri merkezi açmalarını gerektirmektedir. Ancak veri merkezinin açılacağı ülkeden elde edilen gelirlerin böyle bir yatırımı makul

---

<sup>990</sup> Füsün Sarp Nebil, “PayPal neden Türkiye’den çekildi?”, 2016, (Çevrimiçi) <https://t24.com.tr/yazarlar/fusun-sarp-nebil/paypal-neden-turkiyeden-cekildi,14690>, 10.11.2021.

<sup>991</sup> Catherine Boyle, “Google Closes Russia Office After Internet Crackdown”, **CNBC**, (2014), (Çevrimiçi) <https://www.cnbc.com/2014/12/12/google-closes-russia-office-after-internet-crackdown.html>, 18.03.2020.

<sup>992</sup> Swire, Kennedy-Mayo, “Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data”, s. 4.

kılmaması, o ülkede hukuk güvenliğinin olmaması ya da uluslararası ilişkiler açısından böyle bir yatırımın sakıncalı görülebilmesi gibi nedenler, veri merkezi yatırımlarını engelleyebilmektedirler. Dolayısıyla bu tür şirketler için veri lokalizasyonu yükümlülükleri, ilgili ülkedeki ticari faaliyetlerin tamamen durdurulması anlamına da gelebilmektedir.

## **V. VERİ LOKALİZASYONU KURALLARININ HUKUKLARIN ÇATIŞMASI AÇISINDAN ÖNEMİ**

Veri lokalizasyonu yükümlülükleri, devletin veri üzerindeki egemenliği ve uluslararası yetkisi açısından belirleyici bir rol oynamaktadır<sup>993</sup>. Veri üzerindeki egemenlik iddiaları ve verilere ilişkin sınır ötesi uygulama kapsamı olan hukuki düzenlemeler, dijital ortamda hukukların çatışması olgusunu meydana getiren ana unsurlardır.

Daha önceki bölümlerde de açıklandığı bir devlet egemenliğinden doğan uluslararası yetkilerini ülke içerisinde mülkilik esasına göre, ülke dışında ise sınır ötesi yetki kullanımına ilişkin kurallara göre kullanmaktadır. Veri lokalizasyonu yükümlülükleri çerçevesinde verilerin ya da bilgi sistemlerinin fiziksel konumlarına ilişkin kurallar öngörülmesi ya da verilerin ülke dışına çıkarılması imkanlarının sınırlandırılması suretiyle verilerin ilgili ülke içerisinde kalması hedeflenmektedir. Böylelikle devletin veriler üzerindeki uluslararası yetkisini, mülkilik ilkesi çerçevesinde kullanması sağlanmakta ve dolayısıyla sınır ötesi yetki kullanımının yarattığı kısıtlayıcı durumlar ortadan kaldırılmaktadır. Yine egemenliğin mülkilik ilkesi çerçevesinde, diğer devletlerin de bu verilere ilişkin müdahale kabiliyetlerinin azaltılması da kanaatimizce veri lokalizasyonu yükümlülüklerinin getirilme amaçlarından birisidir.

Veri lokalizasyonu yükümlülüklerinin kanaatimizce en önemli etkisi, devletin uluslararası yetkisini veriler üzerinde fiilen kullanabilmesine imkân sağlamasıdır. Uluslararası yargı yetkisinin ve uluslararası uygulama yetkisinin sınır ötesi kullanımı,

---

<sup>993</sup> Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 16.

fiili durumda pek mümkün olmamaktadır. Zira söz konusu yetkilerin sınır ötesi kullanımı hem fiziki güç kullanımı hem de ev sahibi devletin rızasını gerektirmektedir. Veri lokalizasyonu sayesinde veriler üzerindeki söz konusu uluslararası yetkiler, ülke içerisinde kullanılabildiği için, anılan yetkilerin etkin şekilde kullanılamamasından doğan sorunlar ortadan kalkmaktadır.

Uluslararası düzenleme yetkisi konusunda ise veri lokalizasyonu yükümlülükleri, oldukça karmaşık etkiler doğurmaktadır. İnternet üzerinden mal ve hizmet sunan kişilerin, hizmet sundukları ülkede bulunmaması halinde (örneğin, sosyal medya şirketlerinin hemen hepsi sadece ABD ve İrlanda gibi birkaç ülkeden tüm dünyaya hizmet vermektedir.), ev sahibi devletin başka bir ülkede bulunan bir kişi hakkında veri lokalizasyonu yükümlülüğü öngörmesi, esasen düzenleme yetkisinin sınır ötesi kullanımını teşkil etmektedir. Böyle durumlarda, verilerin ilgili kişinin bulunduğu ülkeden dışarı çıkarılması, o ülkenin mevzuatına aykırılık teşkil edebileceği için hukukların çatışması olgusu veri lokalizasyonu yükümlülüğünün kendisi nezdinde doğabilecektir.

Veri lokalizasyonu yükümlülüğünün yarattığı ikinci hukukların çatışması olgusu, veri lokalizasyonu çerçevesinde ülke içerisine getirilmiş olan veriler üzerinde, diğer devletlerin sınır ötesi düzenleme yetkisi kullanmalarıdır. ABD adli makamlarının sınır ötesi uygulama kapsamına sahip mevzuatları neticesinde yabancı bir ülkede bulunan verileri talep etmeleri; ancak bu ülkenin ilgili mevzuatının söz konusu verilerin yurtdışına veri gönderimini yasaklaması hali, söz konusu hukukların çatışması olgusuna bir örnek teşkil etmektedir.

Öte yandan doktrinde, uluslararası yetkinin ülke sınırları gibi bölünemeyen dijital ortamda, fiziki ortama göre farklı kurallara göre kullanılması gerektiği yönünde bir görüş de ortaya atılmıştır<sup>994</sup>. Bu görüşe göre uluslararası yetki ve kanunlar ihtilafı anlamında uygulanacak hukuk belirlenirken verilerin ya da bilgi sistemlerinin konumu

---

<sup>994</sup> Paul Schiff Berman, “Legal Jurisdiction and the Deterritorialization of Data”, **Vanderbilt Law Review En Banc**, C. 71, 2018, s. 20.

dikkate alınmamalı; ilgili şirketlerin kuruluş yeri ve boyutları belirleyici olmamalı, ancak göz önünde bulundurulmalı; belirli bir bölgeye hizmet sunma kriteri ile hizmetlerin etkisinin doğduğu yer dikkate alınmalı; kullanım koşulları sözleşmelerinde yer alan yetki ve uygulanacak hukuk hükümleri dikkate alınmamalıdır. Kanaatimizce söz konusu görüşe katılmak mümkün değildir. Zira burada kanunlar ihtilafı kuralları ile uluslararası yetkinin kullanımına ilişkin kurallar birlikte değerlendirilmiştir. Ancak bu kurallar hem kapsam hem de uygulama alanı açısından, daha önceki bölümlerde de açıklandığı üzere oldukça farklıdır<sup>995</sup>. Ayrıca önerilen kriterler de somut bir çözüm önermekten uzak olup ancak uluslararası bir anlaşma olması halinde uygulanabilecek niteliktedir. Dolayısıyla herhangi bir devletin tek başına bu kuralları uygulaması pek de mümkün olmayacaktır.

## **VI. ÜLKEMİZİN VERİ LOKALİZASYONU HAKKINDAKİ HUKUK POLİTİKASININ DEĞERLENDİRİLMESİ VE ÖNERİLER**

Veri lokalizasyonu yükümlülükleri, ülkemizde çok yaygın bir şekilde uygulama alanı bulmaktadır. Dolayısıyla kanun koyucunun güttüğü hukuk politikasının, veri lokalizasyonunu destekler durumda olduğu sonucuna varılmaktadır. Ülkemizin neden veri lokalizasyonu yaklaşımını benimsediği sorusu ile veri lokalizasyonu konusunda ülkemizin yaklaşımının nasıl olması gerektiğine ilişkin düşünceler aşağıdaki başlıklar altında paylaşılacaktır.

### **A. Türkiye’de Veri Lokalizasyonu Yükümlülükleri Getirilmesinin Amaçları**

Türkiye’de mevcut bulunan veri lokalizasyonuna ilişkin mevzuatın yürürlüğe sokulmasında temel olarak üç amacın bulunduğunu söylemek kanaatimizce mümkündür. Bu amaçlar milli güvenliğin ve kamu düzeninin sağlanması, veriye erişebilme imkânının olması ile ekonomik gelişmedir.

---

<sup>995</sup> Bkz. Yuk. s. 6 vd.



Verilerin yurtdışında bulunması, verilerin aynı zamanda Türkiye Cumhuriyeti'nin egemenlik alanının dışında olması anlamına gelmektedir. Bu nedenle devlet, veriler üzerinde egemenliğini, uluslararası yetkinin sınır ötesi kullanımına ilişkin uluslararası hukuktan kaynaklanan sınırlamalar çerçevesinde kullanabilmektedir. Uygulamada bu durum ise mevcut mevzuat çerçevesinde adli ve idari makamların yabancı ülkelerde bulunan verilere erişememesi sonucunu doğurmaktadır. Söz konusu verilerin eksikliği, adli ve idari makamların görevlerini yerine getirmelerini zorlaştırmakta ve kimi durumda da imkânsız hale getirmektedir.

Adli ve idari makamların verilere erişmesinde yaşanan sorunların doğurduğu en önemli netice, milli güvenliğin ve kamu düzeninin sağlanmasında zafiyetler meydana gelmesidir. İstihbarat faaliyetlerinin yeterince gerçekleştirilememesi, yabancıların istihbarat faaliyetleri de dahil olmak üzere veriye erişimde avantajlı konuma geçmesi ya da suç işleyen kişilerin cezalandırılmaması gibi birçok durum, verilere erişememenin neden milli güvenlik ve kamu düzeni konusunda zafiyetler doğabileceğini açıklar niteliktedir.

Veri lokalizasyonu yükümlülükleri vasıtasıyla aynı zamanda ekonomik fayda elde edilmesi de hedeflenmektedir. Yurtdışından bir takım çevrimiçi hizmetlerin satın alınması, aynı zamanda yurtdışına döviz gönderilmesi anlamına gelmektedir ki bu husus ülkemizin cari açığının büyümesine katkı sağlamaktadır. Veri lokalizasyonu yükümlülükleri, verileri barındıran ve işleyen bilgi sistemlerinin ülke içerisinde kurulmasını gerektirerek ülke içerisindeki yatırımların artmasını sağlayabilecektir.

Yukarıda sayılan amaçlara ulaşabilmek için veri lokalizasyonu yükümlülüklerinin doğru araçlardan biri olup olmadığı ile ülkemizin veri lokalizasyonuna yönelik politikasının ne olması gerektiği konusundaki görüşler aşağıdaki başlık altında açıklanacaktır.

## **B. Türkiye’de Veri Lokalizasyonu Konusunun Ele Alınışına Dair Öneriler**

Veri lokalizasyonu yükümlülüklerine ilişkin olarak, yukarıda da açıklandığı üzere dünyada çeşitli yaklaşımlar benimsenmiştir. ABD, veri lokalizasyonuna tamamen

karşı olarak uluslararası veri akışının engellenmemesi gerektiğini savunmaktadır. AB ise her ne kadar veri lokalizasyonu yükümlülüklerini direkt olarak benimsememişse de hem uluslararası veri akışını sınırlayarak hem de AB içerisindeki veri işleme imkanlarını güçlendirerek dolaylı yünden veri lokalizasyonunu sağlamaya çalışmaktadır. Asya’da ise direkt ve kapsamlı veri lokalizasyonu yükümlülüklerinin uygulandığı görülmektedir. Dünyanın hemen her yerinde devletlerin gündemine girmiş olan veri lokalizasyonu konusu, doğal olarak ülkemizde de gündemde olan bir konudur.

Çalışmamızın bu kısmına kadar da açıklandığı üzere ülkemizde veri lokalizasyonu yükümlülükleri geniş kapsamlı olarak uygulanmaktadır. Zira ülkemizin hukuk politikası, Türkiye’ye ilişkin tüm verilerin yine Türkiye sınırları içerisinde kalması yönündedir. Veri lokalizasyonu politikamız milli güvenliğin ve kamu düzeninin sağlanması, veriye erişebilme imkânının olması ile ekonomik gelişme amaçlarını gerçekleştirmek amaçlarıyla şekillenmiştir. Ancak kanaatimizce ülkemizin veri lokalizasyonu politikası gereğinden fazla sıkı olan kurallar içermektedir ve pratikteki ihtiyaçları karşılamaktan uzak kalmaktadır. Zira gereğinden fazla sıkı olan veri lokalizasyonu kuralları, özel sektörün ticari faaliyetlerini sekteye uğratmaktadır ve dijitalleşme süreçlerini yavaşlatmaktadır. Özel sektörün yaşadığı bu sorunlar hem maliyetlerinin artmasına sebep olmakta hem de tüketicilerin yabancı ülkelere kıyasla daha düşük teknoloji ürünleri daha yüksek fiyatlara kullanmasına sebebiyet vermektedir.

Öte yandan tüm dünyada söz sahibi olabilecek güçlü bir teknoloji sektörüne sahip olmadan veri lokalizasyonu politikasının da tamamen terk edilmesi, yukarıda sayılan ve meşru olan amaçlara ulaşılması ihtimalini ortadan kaldıracak için kanaatimizce yerinde bir yaklaşım da olmayacaktır. Hatta düşüncemize göre bu tür bir yaklaşımı benimsemek, ülkemizin teknoloji sektörünü tamamen korumasız bırakarak bu pazarın tamamen yabancılara terk edilmesi anlamına gelecektir.

Veri lokalizasyonu yükümlülüklerinin gereğinden fazla sıkı uygulanması da hiç uygulanmaması da olumsuz etkiler doğurduğundan dolayı, günümüz dünyası

içerisinde veri lokalizasyonu yükümlülüklerini dengeli bir şekilde uygulamak, kanaatimizce en doğru yaklaşımı teşkil etmektedir. Dengeli yaklaşımın sağlanabilmesi için de veri lokalizasyonu yükümlülükleri belirlenirken orantılılık ve hukuk güvenliği ilkelerine uygun hareket edilmesi önerilmektedir.

Veri lokalizasyonu yükümlülüğü getirilirken, ulaşılmak istenen amaç açısından veri lokalizasyonu yükümlülüğünün etkileri ve doğuracağı sonuçların değerlendirilmesi ile bu amacın etki ve sonuçları ile orantılı olup olmayacağının tespit edilmesi kanaatimizce bir gerekliliktir<sup>996</sup>. Örneğin kamu kurum ve kuruluşlarının kritik bilgileri açısından veri lokalizasyonu yükümlülükleri öngörülmesi orantılı bir yaklaşım teşkil ederken elektrikli skuterler için veri lokalizasyonu yükümlülüğü öngörmeyi orantılı bir yaklaşım olarak kabul etmek uygun olmayacaktır.

İkinci olarak veri lokalizasyonu yükümlülükleri yanında, mutlaka hukuk güvenliğini temin edici hukuk kurallarının da yürürlüğe sokulması gerektiği düşünülmektedir. Bu kurallar vasıtasıyla verilerini Türkiye içerisinde saklamak zorunda kalan kişilerin (özellikle yabancıların) verilerinin keyfi muamelelere tabi tutulmayacağına ikna olması gerekmektedir. Ancak Türk mevzuatı ile Türk idari makamlarına gerekli gördükleri her türlü bilgiyi ilgili kişilerden herhangi bir mahkeme kararı olmaksızın talep etme imkânını sağlamaktadır<sup>997</sup>. Benzer durum CMK içerisinde cumhuriyet savcıları için de söz konusudur<sup>998</sup>. Dolayısıyla Türk hukuku, adli ve idari makamların veriye erişimi konusunda keyfi uygulamalara son derece müsaittir. Üstelik adli ve idari makamların elde edeceği verilerin gizliliği ve güvenliğinin sağlanması noktasındaki hukuki düzenlemeler de eksiktir ve bu konudaki farkındalık seviyesi de oldukça düşüktür. Önceki bölümlerde açıklandığı üzere ABD’de ise verilere erişim, detaylı ve sıkı kurallara tabi tutulmakta ve çoğu durumda verilere erişim için bağımsız mahkeme

---

<sup>996</sup> Veri lokalizasyonu yükümlülüğünün orantılı olup olmadığını test etmekte kullanılabilecek kriterler için bkz. Svantesson, “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, s. 27.

<sup>997</sup> Örnek olarak 5809 sayılı Elektronik Haberleşme Kanunu m. 6/1-ı ve m. 60/12 ile 5651 sayılı kanun m. 5/4 ve m. 6/1-d’nin BTK’ya verdiği geniş yetkiler, İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi m. 17/2 ile İletişim Başkanlığı’na verilen geniş yetkiler gösterilebilecektir.

<sup>998</sup> CMK m. 332 gereği cumhuriyet savcısının, herhangi bir mahkeme kararına ihtiyaç duymadan her bilgi talep etme yetkisi bulunmaktadır.

kararı aranmaktadır. Türk hukukunun benzeri koruma sağlayamaması, veri lokalizasyonu yükümlülüklerinin doğurduğu olumsuz etkileri güçlendirmektedir.

Veri lokalizasyonu yükümlülüklerinin, veri güvenliği ve sürekliliği konularında zafiyet yaratmaması için teknolojik altyapıların güçlü olmasına ve nitelikli insan gücüne de ihtiyaç vardır. Özellikle veri merkezi kurulumu konusunda coğrafi olarak elverişli olan bölgelerde söz konusu altyapı ve insan gücünün konumlandırılması, veri lokalizasyonu yükümlülüklerinin etkin şekilde uygulanabilir hale gelmesine katkı sağlayacaktır.

Yukarıda da açıklandığı üzere Türkiye’de veri lokalizasyonu yükümlülüğü getirilmesi ile amaçlanan unsurlardan ilk ikisi veriye adli ve idari makamların erişiminin sağlanması ile milli güvenliğin ve kamu düzeninin tesis edilmesidir. Bu iki amaç birbirleri ile çok yakın ilişkilidir. Ancak bu amaçlara yönelik olarak getirilen veri lokalizasyonu yükümlülükleri, ekonomik ve sosyal açılardan zararlar doğurmaktadır. Örneğin bugün sosyal medya mecralarının veri lokalizasyonu yükümlülüklerini yerine getirmemeleri nedeniyle erişime kapatılmaları hem ekonomik hem de sosyal açıdan çok büyük olumsuz etkiler doğurabilecek niteliktedir. Dolayısıyla sadece söz konusu amaçlar göz önüne alınarak aşırı kapsayıcı veri lokalizasyonu yükümlülükleri getirilmesi fiilen mümkün olmamaktadır. O halde önerdiğimiz ilkeler vasıtasıyla sınırlandırılmış olan veri lokalizasyonu yükümlülüklerinin belirlenmesinin yanında, Vietnam modeline<sup>999</sup> uygun şekilde aşamalı veri lokalizasyonu yükümlülükleri ve ABD’nin CLOUD Act’ine benzer veriye erişim düzenlemelerinin yürürlüğe sokulması; güdülen bahse konu amaçlara ulaşmayı çok büyük oranda mümkün kılacaktır. Ayrıca yine AB ülkelerinin yaptığı gibi CLOUD Act vasıtasıyla yabancıların Türkiye’deki verilere tek taraflı olarak erişmesinin engellenmesinin de bir gereklilik olduğu; yabancıların verilere erişiminin ise yeni nesil istinabe sözleşmeleri çerçevesinde sağlanmasının da uygun olacağı düşünülmektedir.

---

<sup>999</sup> Bkz. Yuk. s. 262 vd.

Veri lokalizasyonu yükümlölükleri çerçevesinde ölkemize yatırım çekilmesi ve yerli teknoloji sektörünün geliştirilmesi fikri, ekonomistlerce tartışılması gereken bir husustur. Ancak yine de çeşitli çalışmalar neticesinde veri lokalizasyonu yükümlölüklerinin ekonomik faydadan çok zarar getirdiğı sonucuna varıldığı gözlemlenmektedir.

Son olarak ifade etmek gerekir ki veri lokalizasyonu yükümlölükleri, mülklik ilkesi çerçevesinde (sınır ötesi uluslararası yetki kullanımı kuralları çerçevesinde değil) veriler üzerinde devletin uluslararası yetkisini kullanabilmesini sağlamayı hedeflemektedir. Ancak bu yaklaşım, verileri yabancı devletlerin müdahalesinden koruma konusunda yeterli değildir zira onların sınır ötesi uluslararası yetki kullanımı kuralları çerçevesinde hala verilere etki edebilme imkânları bulunmaktadır. O halde iç hukukta yapılacak düzenlemeler yoluyla hukukların çatışması durumları yaratılarak veriler üzerinde yabancı devletlerin uluslararası yetki kullanmasının engellenmesi yönünde çalışmalar yapılması da elzemdir.

## SONUÇ

İnternet ve bilgi teknolojilerinin gelişmesi neticesinde meydana gelen ve yaygın olarak kullanılan dijital ortam, kişiler arasındaki ilişkilerin hemen hepsine etki eder hale gelmiştir. Günümüzde artık ifade özgürlüğü, ticari işlemler ve işlenen suçlar gibi birçok hukuki olayda, dijital ortamın kullanıldığı görülmektedir. Söz konusu gelişmeler, dijital ortama ilişkin devletlerin hukuki düzenlemeler yapma ihtiyacını arttırmıştır. İnternetin, ülke sınırlarından etkilenmeyen yapısı nedeniyle devletler dijital ortam üzerinde egemenlik ve uluslararası yetkilerini kullanmakta zorluk yaşamaktadırlar. İşte bu zorluklar hem sınır ötesi uygulama kapsamına sahip kanunların hem de veri lokalizasyonu yükümlülükleri getiren hukuki düzenlemelerin yaygınlaşmasına sebebiyet vermektedir.

Çalışmamızın ilk bölümünde, uluslararası hukuk açısından bir devletin sınır ötesi uygulama kapsamına sahip hukuki düzenlemeler yapıp yapamayacağı konusu değerlendirilmiştir. Sınır ötesi uygulama kapsamı, bir hukuki düzenlemenin; ilgili düzenlemeyi yürürlüğe sokan devletin ülkesinin dışında da bağlayıcı olması anlamına gelmektedir. Uluslararası hukuktaki mülkilik ilkesi ile müsamahakâr ilkeler çerçevesinde, uluslararası hukukun sınır ötesi uygulama kapsamına sahip hukuki düzenlemelerin çıkarılmasına izin verdiği sonucuna ulaşmak mümkündür. Ancak önemle belirtmek gerekir ki söz konusu sonuç, bağlayıcı uluslararası hukuk kurallarına değil, uluslararası hukuk teamüllerine dayanmaktadır. Sınır ötesi uygulama kapsamına sahip kanunların yabancı ülkede kamu gücüne dayalı olarak uygulanması ise ev sahibi devletin rızası olmaması halinde kesinlikle yasaklanmış durumdadır.

Devletlerin uluslararası düzenleme yetkisini mülkilik ilkesi çerçevesinde ya da müsamahakâr ilkelere uygun olarak sınır ötesi kapsamda kullanmaları uluslararası hukuka uygun kabul edilmektedir. Ancak bu kriterleri kullanarak düzenleme yetkisinin aynı olgu hakkında birden fazla devlet tarafından kullanılması mümkündür. Her bir devletin kendi menfaatlerine uygun şekilde düzenleme yetkisini kullanacağı göz önüne alındığında, devletlerin bireyler üzerinde farklı yükümlülükler öngörme ihtimali yüksektir. Bu yükümlülükler kimi durumlarda birbirleri ile çelişmezken kimi

durumlarda ise çelişkili olabilecektir. İşte bu şekilde birbirleriyle çelişen yükümlülükleri adlandırmak amacıyla “hukukların çatışması” (**Conflict of Legal Orders**) kavramı tarafımızca ortaya atılmıştır. Hukukların çatışması kavramı, mülkilik ilkesi ya da müsamahakâr ilkelere uygun olarak sınır ötesi kapsamda devletlerin düzenleyici yetki kullanmaları neticesinde kişiler üzerinde birbirleriyle çelişen hukuki yükümlülükler doğması şeklinde tanımlanabilecektir. Hukukların çatışması kavramı sadece özel hukuk alanları ile sınırlı değildir; kamu hukuku nitelikli kurallar açısından da meydana gelebilmektedir. Hatta ağırlıklı olarak hukukların çatışmasının kamu hukuku içerisinde oluşacağını söylemek de kanaatimizce mümkündür. Hukukların çatışması kavramının bir diğer özelliği de sadece mahkeme önüne gelen uyuşmazlıklarda meydana gelen bir vakıa olmamasıdır. Hatta tam tersine mahkemelerin önüne gelmeyen ve devlet ile kişiler arasında etki doğuran hukuk kurallarının uygulanması sırasında hukukların çatışmasının daha yoğun olarak meydana geldiğini söylemek mümkündür.

Hukukların çatışması kavramının yukarıda sayılan özellikleri, aslında milletlerarası özel hukukun, yabancılık unsuru içeren yukarıdaki durumları çözmekte etkisiz kalmasını da açıklamaktadır. Zira milletlerarası özel hukukun cevabını aradığı soru olan yabancılık unsuru bulunan uyuşmazlıklarda hangi hukukun uygulanması konusu, dijital ortamın yaygınlaşması ile birlikte artan hukukların çatışması sorunu ile aynı konu değildir. Düşüncemize göre milletlerarası özel hukuk, hukukların çatışması kavramını çözmeye en yakın hukuk dalıdır. Bu nedenle milletlerarası özel hukuk doktrinine getirilecek yeni bakış açıları, bu alanın önemini çok daha arttırabilecektir.

Dijital ortamı düzenleyen sınır ötesi uygulama kapsamlı kanunların tüm dünyada yaygınlaştığı gözlemlenmektedir. Bu tür kanunların amacı, ev sahibi ülkeyi etkileyen; ancak yurtdışında bulunan verilere dair kurallar getirmektedir. Bu kapsamda KVKK ve GDPR, Türkiye ve AB dışında işlenen kişisel veriler hakkında da eğer bu veriler ilgili ülkelerle bağlantılıysa, birçok kural öngörmektedir. ABD tarafından yürürlüğe konulan CLOUD Act ile değiştirilmiş olan SCA, ABD mahkemelerine ABD dışında olan veriler hakkında bağlayıcı mahkeme kararı verme yetkisi sunmaktadır. Yine CLOUD Act ile birlikte öngörülen yeni tip adli istinabe sözleşmeleri, mevcut adli

istinabe sözleşmelerinin yavaş ve etkisizliğini kabul ederek konuyu çözümlemeyi hedeflemektedir.

Kanaatimizce söz konusu sınır ötesi uygulama kapsamına sahip kanunların yürürlüğe konulması, uluslararası hukukun mevcut durumunun ihlali anlamına gelmemektedir. Ancak bu kanunların etki ettikleri ülkede bulunan yerel kanunlar neticesinde yaratacağı hukukların çatışması olgusunun çözümlenmesi, esasen uluslararası hukukun konusu değildir. Çalışmamız içerisinde detaylıca incelenen ve analiz edilen bu sınır ötesi uygulama kapsamlı kanunlar içerisinde sadece SCA, hukukların çatışması ihtimali öngörmüş ve bu konuya ilişkin düzenlemeler yapmış durumdadır. Ancak bu düzenlemelerin de genellikle ABD lehine sonuçlar doğurmayı hedeflediği düşünülmektedir.

Çalışmamızın temel amacı, dijital ortamı düzenleyen kanunların yarattığı hukukların çatışması sorununa yönelik olarak ülkemizde kullanılabilecek çözüm önerileri sunmaktır. Bu kapsamda her bölüm sonunda, ilgili konuya ilişkin detaylı fikir ve çözüm önerileri paylaşılmış durumdadır. Tüm bu önerilerin ortak noktası ise KVKK'nın sınır ötesi uygulama kapsamını netleştirmesi ile SCA benzeri bir kanun ile Türk mahkemelerine sınır ötesi bağlayıcı yetki verilmesi gibi önlemlerle, yabancı hukukların yaptığı sınır ötesi uygulamaların aynılarının yapılması şeklindedir. Ayrıca Türk vatandaşlarına ve şirketlerine ait verilerin korunması için de yabancı makamların bilgi taleplerine Türk mahkemelerinin onayı olmaksızın cevap verilmesini yasaklayan düzenlemelerin yürürlüğe sokulması ile yabancı devletlerin sınır ötesi uygulama kapsamına sahip kanunları çerçevesinde Türk vatandaşlarına ve şirketlerine uygulanabilecek yaptırımlara dair koruma sağlanması gibi öneriler de sunulmuştur. Sunulan öneriler, bir taraftan hukukların çatışması olgusundan etkilenen özel hukuk kişilerini korumaya yönelikken diğer taraftan da hukukların çatışması durumlarını yabancılarla arttırmayı hedefleyerek sorunların çözümüne yönelik uluslararası uzlaşma ortamı yaratmayı amaçlamaktadır. Düşüncemize göre, hukukların çatışması durumlarının devletler arasında çözümlenebilmesinin yegâne yolu, ilgili devlet menfaatlerini bu yönde adım atılmasını gerektirir hale getirmektir. Bu da mevcut



statüden menfaat elde eden ya da menfaatleri etkileyen devletlerin, hukukların çatışması durumları ile menfaat kaybına uğramaları halinde mümkün olabilecektir.

Çalışmamızın son bölümünde değinilen veri lokalizasyonu kavramı ise, adeta sınır ötesi uygulama kapsamına sahip kanunların alternatifi olarak karşımıza çıkmaktadır. Sınır ötesi uygulama kapsamına sahip kanunlar, yabancı ülkelerde bulunan verilerin; bahse konu kanunu çıkaran ülke düzenlemelerine tabi olmasını uluslararası düzenleme yetkisine dayanarak sağlamaya çalışmaktadır. Veri lokalizasyonu yükümlülükleri ise verilerin bulunacağı coğrafi konumu belirleyerek veriler üzerinde uygulanacak kanunları, mülkilik ilkesine göre belirlemeyi hedeflemektedirler. Veri lokalizasyonu yükümlülükleri tüm dünyada ve ülkemizde oldukça popülerdir. Ancak veri lokalizasyonu yükümlülükleri, tek başlarına yabancı kanunların sınır ötesi uygulama kapsamı vasıtasıyla söz konusu verilere etki etmelerine engel teşkil etmemektedir. Örneğin bir ABD menşeli şirketin, Türkiye’de veri merkezi açması halinde; o veri merkezinde bulunan her türlü veri yine SCA kapsamında ABD makamları tarafından erişilebilir olacaktır. O halde veri lokalizasyonu kavramı, verilerin yurtdışına aktarılmasını engelleyen diğer hukuki düzenlemelerle de desteklenmelidir. Öte yandan ifade etmek gerekir ki veri lokalizasyonu yükümlülüklerinin teknolojik gelişme ve yeterlilik ile ekonomi açısından da olumlu ve olumsuz etkileri bulunmaktadır. Bu nedenle veri lokalizasyonu yükümlülükleri getirilirken orantılı davranılması son derece önemlidir.

Son olarak ifade etmek gerekir ki devletler arasında dijital ortamdaki egemenlik açısından yıllardır bir mücadele sürmektedir. Bu mücadele, etkilerini sadece sınır ötesi uygulama kapsamına sahip kanunlarla ya da veri lokalizasyonu yükümlülükleri ile göstermemektedir. Devletler sıklıkla kendilerine göre yabancı olan ülkelerin teknolojilerini yasaklamakta<sup>1000</sup> veya yabancı şirketlerin faaliyetlerine müdahalelerde

---

<sup>1000</sup> “German Schools Ban Microsoft Office 365 amid Privacy Concerns (Updated)”, **TNW**, 15.07.2019, (Çevrimiçi) [https://thenextweb.com/news/german-schools-ban-microsoft-office-365-amid-privacy-concerns?\\_\\_twitter\\_impression=true](https://thenextweb.com/news/german-schools-ban-microsoft-office-365-amid-privacy-concerns?__twitter_impression=true), 11.11.2021; Daniel Cooper, “China Bans All Government Departments from Using US-Made Technology”, **Engadget**, 09.12.2019, (Çevrimiçi) [https://www.engadget.com/2019-12-09-china-bans-all-government-departments-from-using-us-made-technol.html?utm\\_campaign=homepage&utm\\_medium=internal&utm\\_source=dl&guccounter=1](https://www.engadget.com/2019-12-09-china-bans-all-government-departments-from-using-us-made-technol.html?utm_campaign=homepage&utm_medium=internal&utm_source=dl&guccounter=1), 11.11.2021.

bulunmaktadır<sup>1001</sup>. Dijital ortamın hızlı yapısı karşısında, çalışmamız kapsamında sunulan önerilerin kısa zamanda geçerliliklerini yitireceğine şüphe yoktur. O nedenle dijital ortama ilişkin her türlü gelişmenin sürekli olarak yakından takip edilmesinin ve yabancı mevzuatın tercümelere yerine ülkemizin ihtiyaçlarına ve durumuna uygun yerli mevzuatın üretilmesinin yerinde olacağı düşünülmektedir.



---

<sup>1001</sup> Emma Roth, “TikTok and Oracle Teamed up after All, but Concerns about Data Privacy Remain”, **TheVerge**, 19.06.2022, (Çevrimiçi) <https://www.theverge.com/2022/6/19/23174775/tiktok-oracle-team-up-concerns-data-privacy-remain>, 11.11.2022; Monica Miller, “Tech War: Biden Moves to Halt US Exports to Huawei, Reports Say”, **BBC**, 31.01.2023, (Çevrimiçi) <https://www.bbc.com/news/business-64461877>, 02.02.2023.

## KAYNAKÇA

- Abe, Yoshinori: “Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?”, **Policy Research Institute, Ministry of Finance, Japan, Public Policy Review**, S. 5, 2021.
- Agrawal, Aditi: “UK-Japan agree to trade deal that bans data localisation”, **Medianama**, (11.09.2020), (Çevrimiçi) <https://www.medianama.com/2020/09/223-uk-japan-trade-deal-ban-data-localisation/>, 26.11.2020.
- Akehurst, Michael: “Jurisdiction in International Law”, **British Year Book of International Law**, C. 46, 1972.
- Akıncı, Ziya: **Milletlerarası Özel Hukuk**, 1. bs, İstanbul, Vedat Kitapçılık, 2020.
- Altıntaş, Hilal: “Bankacılık Krizleri, Nedenleri ve Ekonomik Maliyetleri”, **Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, S. 22, 2004.
- Ankeny, Cody: “The Costs of Data Localization”, **Information Technology Industry Council**, (17.08.2016), (Çevrimiçi) <https://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization>, 04.04.2020.
- Aşıkoğlu, Şehriban  
İpek, Fatih Burak  
Uzun: “Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri”, **Prof. Dr. Türkan Rado’nun Anısına Armağan**, 1.bs, İstanbul, On İki Levha Yayıncılık 2020.
- Avşar, Melis: “The Concept of Investment Under The ICSID Convention”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni**, C. 37, S. 2, 2017, s. 95-140.
- Aybay, Rona: **Genel Kamu Hukuku**, 3. bs, İstanbul, DER Kitabevi, 2020.
- Aybay, Rona, Esra  
Dardağan: **Yasaların Çatışması**, 2. bs, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2008.
- Aydoğmuş Gisoldi,  
Ayşe Yasemin: **Milletlerarası Özel Hukukta Kişisel Verilerin Korunması**, 1. bs, İstanbul, On İki Levha Yayıncılık, 2022.

- Ayers, Cynthia E.: **Rethinking Sovereignty in the Context of Cyberspace**, Pennsylvania US, The United States Army War College, 2016.
- Aygün, Mesut: “ABD Kanunlar İhtilafı Hukukuna Kuramsal ve Metodolojik Bir Bakış: Çeşitli Teori ve Metotlar, II. Restatement ve Sözleşmeye Uygulanacak Hukuk”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. 20, S. 2, 2016, s. 129-170.
- Azmi, Ida Madieha Abdul Ghani, Jeong Chun Phuoc: “International Norms in Regulating Ecommerce: The Electronic Commerce Chapter of the Comprehensive Trans-Pacific Partnership Agreement”, **International Journal of Business and Society**, 2020.
- Azzi, Adele: “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, C. 9, S. 2, 2018, s. 126-137.
- Bailey, Rishab: “The issues around data localisation”, **The Hindu**, (25.02.2020), (Çevrimiçi) <https://www.thehindu.com/opinion/op-ed/the-issues-around-data-localisation/article30906488.ece>, 04.08.2020.
- Bailey, Rishab, Smriti Parsheera: “Data Localisation in India: Questioning the Means and Ends”, **National Institute of Public Finance and Policy**, Working Paper No:242, 2018.
- Basu, Arindrajit: “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam”, **The Diplomat**, (10.01.2020), (Çevrimiçi) <https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/>, 15.05.2020.
- Basu, Arindrajit, Elonnai Hickok, Aditya Singh Chawla: “The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India”, **The Centre for Internet & Society**, 2019.
- Batthey, Alexander Dugas Jr.: “A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act Notes & Comments”, **Rutgers Computer and Technology Law Journal**, C. 42, S. 2, 2016, s. 262-298.
- Bauer, Matthias, Martina F. “Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States”, European Centre for International Political Economy,

- Ferracane, Hosuk Lee-Makiyama: 2016, (Çevrimiçi) <https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>, 05.04.2022.
- Bauer, Matthias, Martina F. Ferracane, Erik Van der Marel: “Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization”, **Centre for International Governance Innovation and Chatham House**, Paper Series No. 30, 2016, 20.
- Baylson, Michael M., Sandra A. Jeskie: “Overseas Obligations: An Update on Cross-Border Discovery”, **Judicature**, C. 103, S. 1, 2019, s. 54-63.
- Beale, Joseph Henry: **A Treatise on the Conflict of Laws or Private International Law**, C. 1, Cambridge, Harvard University Press, 1916.
- Beletski, Roman: “Critical assessment of the extraterritoriality of the EU General Data Protection Regulation”, 2019, (Çevrimiçi) <https://helda.helsinki.fi/server/api/core/bitstreams/6bbda301-005d-4973-8986-8859e6334770/content> 18.10.2021.
- Benhamou, Yaniv: “GDPR on the Swiss Territory Cooperation with European Authorities and Enforcement of Monetary Fines”, **Jusletter-it**, 2018, (Çevrimiçi) [https://www.researchgate.net/profile/Yaniv-Benhamou/publication/326253605\\_GDPR\\_on\\_the\\_swiss\\_territory\\_Cooperation\\_with\\_European\\_authorities\\_and\\_enforcement\\_of\\_monetary\\_fines/links/5d80ecd2a6fdcc12cb96f134/GDPR-on-the-swiss-territory-Cooperation-with-European-authorities-and-enforcement-of-monetary-fines.pdf](https://www.researchgate.net/profile/Yaniv-Benhamou/publication/326253605_GDPR_on_the_swiss_territory_Cooperation_with_European_authorities_and_enforcement_of_monetary_fines/links/5d80ecd2a6fdcc12cb96f134/GDPR-on-the-swiss-territory-Cooperation-with-European-authorities-and-enforcement-of-monetary-fines.pdf), 11.20.2021.
- Bennett, Colin, Smith Oduro-Marfo: “Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?”, **UbiComp '18: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers**, 2018, 880-890.
- Benton, Diana: “Seeking Warrants for Unknown Locations: The Mismatch between Digital Pegs and Territorial Holes”, **Emory Law Journal**, C. 68, S. 1, 2018, s. 183-220.
- Berman, Paul Schiff: “Legal Jurisdiction and the Deterritorialization of Data”, **Vanderbilt Law Review En Banc**, C. 71, 2018, s. 11-32.

- Berry, Renee, Matthew Reisman: "Policy Challenges of Cross-Border Cloud Computing", **Journal of International Commerce & Economics**, C. 4, S. 2, 2012, s. 1-38.
- Bilgic, Secil: "Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act", **Harvard Journal of Law & Technology**, C. 32, S. 1, 2018, s. 321-355.
- Blackman, Jonathan I., Jared Gerber: "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", **Clearly Gottlieb**, 2018, (Çevrimiçi) <https://www.clearlygottlieb.com/-/media/files/alert-memos-2018/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications.pdf>, 18.08.2019.
- Blanke, Jordan M.: "Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act", **Global Privacy Law Review**, C. 1, S. 2, 2020, s. 81-92.
- Blume, Joshua D.: "Reading the Trade Tea Leaves: A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization, and Cybersecurity Laws", **Georgetown Journal of International Law**, C. 49, S. 2, 2018, s. 801-844.
- Bohaker, Heidi, Lisa Austin, Andrew Clement, Stephanie Perrin: **Seeing Through the Cloud**, Canada, Creative Commons, 2015.
- Boyd, Stephen E.: "Certification from U.S. Department of Justice - Office of Legislative Affairs to Senate Judiciary Committee and the Senate Foreign Relations Committee", 04.12.2019, (Çevrimiçi) <https://www.justice.gov/dag/page/file/1231381/download>, 06.06.2021.
- Boyle, Catherine: "Google Closes Russia Office After Internet Crackdown", **CNBC**, (2014), (Çevrimiçi) <https://www.cnn.com/2014/12/12/google-closes-russia-office-after-internet-crackdown.html>, 18.03.2020.
- Brannon, Ike, Hart Schwartz: "The New Perils of Data Localization Rules", **Regulation**, C. 41, S. 2, 2018, s. 12-13.

- Brehmer, H. Jacqueline: “Data Localization: The Unintended Consequences of Privacy Litigation”, **American University Law Review**, C. 67, S. 3, 2018, s. 927-970.
- Briggs, Adrian: **The Conflict of Laws**, 3. bs, Oxford, United Kingdom, Oxford University Press, 2013.
- Brilmayer, Lea, Jack Goldsmith, Erin O’Hara O’Connor: **Conflict of Laws Cases and Materials**, 7. bs, New York, Wolters Kluwer Law & Business, 2015.
- Brkan, Maja: “Data Protection and Conflict-of-Laws: A Challenging Relationship”, **European Data Protection Law Review (EDPL)**, C. 2, S. 3, 2016, s. 324-341.
- Brkan, Maja: “The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?”, **Maastricht Journal of European and Comparative Law**, C. 23, S. 5, 2016, s. 812-841.
- Brown, Shaun: “Data Localization: An Exercise in Futility?”, IAPP Canada Privacy Symposium, 23.05.2019, (Çevrimiçi) <https://nnovation.com/wp-content/uploads/2019/05/SBrown-Data-Localization-May2019.pdf>, 11.09.2020.
- Brownlie, Ian: **Principles of Public International Law**, 7. bs, New York, Oxford University Press, 2008.
- Buchan, Russell: **Cyber Espionage And International Law**, 1. bs, Oxford UK, Hart Publishing, 2019.
- Burman, Anirudh, Upasana Sharma: “How Would Data Localization Benefit India?”, 14.04.2021, (Çevrimiçi) <https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291>, 09.09.2021.
- Burri, Mira: “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions”, **Journal of World Investment & Trade**, C. 22, 2021, s. 17.
- Burri, Mira: “Interfacing Privacy and Trade”, **Case Western Reserve Journal of International Law**, C. 53, S. 1, 2021.
- Burri, Mira: “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation”, **U.C. Davis Law Review**, C. 51, S. 1, 2017, s. 65-132.

- Burri, Mira: “The Regulation of Data Flows through Trade Agreements”, **Georgetown Journal of International Law**, C. 48, S. 2, 2017, s. 407-448.
- Burri, Mira, Rahel Schär: “The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy”, **Journal of Information Policy**, C. Vol. 6, 2016, s. 479-511.
- Busser, Els De: “The Digital Unfitness of Mutual Legal Assistance”, **Security and Human Rights**, C. 28, S. 1-4, 2017, s. 161-179.
- Calster, Geert van: **European Private International Law**, 2. bs, Oxford UK, Hart Publishing and Bloomsbury Publishing, 2016.
- Cantekin, Kayahan: “Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?”, **1st Edition of the Seminars of the PhD School in Public, International and European Union law of “Università degli Studi di Milano”**, 2018, 79-95.
- Carlson, Greta, Jonathan McKinney, Elizabeth Slezak, Esther-Sarah Wilmot: “General Data Protection Regulation and California Consumer Privacy Act: Background Symposium: Compliance in International Corporate Legal Practices”, **Currents: Journal of International Economic Law**, C. 24, S. 1, 2020, s. 62-69.
- Carmen, Rolando V. del, Craig Hemmens: **Criminal Procedure Law and Practice**, 10. bs, Boston, Cengage Learning, 2017.
- Casalini, Francesca, Javier López González, Taku Nemoto: “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers”, **OECD Trade Policy Papers**, 2021.
- Caşın, Mesut Hakkı: **Modern Uluslararası Hukukun Temel Esasları**, 1. bs, İstanbul, Yeditepe Üniversitesi Yayınları, 2019.
- Cate, Fred H., James X. Dempsey: **Systematic Government Access to Private-Sector Data Bulk Collection**, New York, NY, USA, Oxford University Press, 2017.
- Cerulus, Laurens: “Europe’s litmus test over cloud computing push”, **Politico**, (28.07.2020), (Çevrimiçi)



<https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/>, 28.09.2020.

- Chander, Anupam, Uyên P. Lê: “Data Nationalism”, **Emory Law Journal**, C. 64, S. 3, 2015, s. 679-739.
- Cheatham, Elliott E.: “Stone on Conflict of Laws”, **Columbia Law Review**, C. 46, 1946, s. 719-733.
- Cherry, Miriam A.: “A Global System of Work, a Global System of Regulation: Crowdwork and Conflicts of Law”, **Tulane Law Review**, C. 94, S. 2, 2019, s. 183-246.
- Childress III, Donald Earl: “Comity as Conflict: Resituating International Comity as Conflict of Laws”, **U.C. Davis Law Review**, C. 44, S. 1, 2010, s. 11-80.
- Christakis, Theodore: “21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)”, **European Law Blog**, (17.10.2019), (Çevrimiçi) <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>, 15.04.2020.
- Christakis, Theodore: **Lawful Access To Data: The Us V. Microsoft Case, Sovereignty In The Cyber-Space And European Data Protection**, CEIS and The Chertoff Group, 2017.
- Christakis, Theodore: “Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 27.05.2019, (Çevrimiçi) <https://papers.ssrn.com/abstract=3397047>, 27.09.2020.
- Christiano, Fabio: “Palestine: Whose Cyber Security without Cyber Sovereignty?”, Routledge Companion to Global Cyber-Security Strategy, 2020, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3700850](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700850), 01.02.2021.
- Clemons, Eric: “The Federal Government’s Attempt to Force Microsoft to Violate Irish Territoriality”, 2017, (Çevrimiçi), <http://scholarspace.manoa.hawaii.edu/handle/10125/41768>, 12.06.2019.
- Cochrane, Tim: “Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory

- Powers”, **Duke Journal of Comparative & International Law**, C. 32:153, 2021, s. 153-210.
- Cole, Mark D.,  
Quintel Teresa: “Transborder Access to e-Evidence by Law Enforcement Agencies”, University of Luxembourg Law Working Paper No. 2018-010, 2018, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3278780](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278780), 05.07.2019.
- Conrad, Victoria: “Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data”, **William and Mary Business Law Review**, C. 10, S. 1, 2018, s. 295-336.
- Cook, Chris: “Cross-Border Data Access and Active CyberDefense: Assessing Legislative Options for a New International Cybersecurity Rulebook”, **Stanford Law & Policy Review**, C. 29, S. 2, 2018, s. 205-236.
- Cooper, Daniel: “China Bans All Government Departments from Using US-Made Technology”, **Engadget**, 09.12.2019, (Çevrimiçi) [https://www.engadget.com/2019-12-09-china-bans-all-government-departments-from-using-us-made-technol.html?utm\\_campaign=homepage&utm\\_medium=internal&utm\\_source=dl&guccounter=1](https://www.engadget.com/2019-12-09-china-bans-all-government-departments-from-using-us-made-technol.html?utm_campaign=homepage&utm_medium=internal&utm_source=dl&guccounter=1), 11.11.2021.
- Cors, Dylan: “National Security Data Access and Global Legitimacy”, **United States Attorneys’ Bulletin**, C. 67, S. 4, 2019, s. 257-286.
- Cory, Nigel: “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?”, **Information Technology & Innovation Foundation**, 2017, (Çevrimiçi) [http://www2.itif.org/2017-cross-border-data-flows.pdf?\\_ga=2.200100782.1604662306.1615630888-1194186901.1615630888](http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.200100782.1604662306.1615630888-1194186901.1615630888), 04.09.2020.
- Cosby, Teresa  
Nesbitt: “The Expectation of Privacy: An Unreasonable Standard in an Era of Rapid Innovations in Technology”, **Charleston Law Review**, C. 12, S. 3, 2017, s. 337-352.
- Creemers, Rogier,  
Graham Webster: “Translation: Personal Information Protection Law of the People’s Republic of China”, 20.08.2021, (Çevrimiçi) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>, 12.10.2021.
- Crosby, Daniel: **Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments**, Switzerland,

International Centre for Trade and Sustainable Development (ICTSD), 2016.

Çekin, Mesut  
Serdar:

**Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku**, 2. bs, İstanbul, On İki Levha Yayıncılık, 2019.

Çelikel, Aysel, B.  
Bahadır Erdem:

**Milletlerarası Özel Hukuk**, 17. bs, İstanbul, Beta Basım A.Ş., 2021.

Dal, Ufuk:

“Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti”, **Kişisel Verileri Koruma Dergisi**, C. 1, S. 1, 2019, s. 21-33.

Daley, M. James,  
Jason Priebe,  
Patrick Zeller:

“The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery”, **Sedona Conference Journal**, C. 16, 2015, s. 201-256.

Daskal, Jennifer:

“Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0”, **Stanford Law Review**, C. 71, 2018.

Daskal, Jennifer:

“Privacy and Security Across Borders”, **Yale Law Journal Forum**, 2019, 1029-1051.

Daskal, Jennifer:

“The Un-Territoriality of Data”, **Yale Law Journal**, C. 125, S. 2, 2015, s. 326-399.

Daskal, Jennifer,  
Justin Sherman:

“Data Nationalism on the Rise”, **Data Catalyst**, 2020, (Çevrimiçi) <https://datacatalyst.org/wp-content/uploads/2020/06/Data-Nationalism-on-the-Rise.pdf>, 27.11.2020.

Daskal, Jennifer,  
Peter Swire:

“The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards”, **Lawfare**, (14.03.2020), (Çevrimiçi) <https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards>, 14.03.2020.

Davies, Jamie:

“US Government to consider strict data localisation laws”, **Telecoms.com**, (19.11.2019), (Çevrimiçi) <https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/>, 22.05.2020.

De Hert, Paul,  
Cihan Parlar,

“Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium

- Johannes Thumfart: to Microsoft Ireland”, **New Journal of European Criminal Law**, C. 9, S. 3, 2018, s. 326-352.
- De Hert, Paul, Johannes Thumfart: “The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 08.07.2018, (Çevrimiçi) <https://papers.ssrn.com/abstract=3228388>, 15.06.2019.
- De Hert, Paul, Johannes Thumfart: “The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies”, **Brussels Privacy Hub, Working Paper**, C. 4, S. 11, 2018, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3228388](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228388), 15.12.2020.
- De Souza Abreu, Jacqueline: “Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience”, **Revista de Informação Legislativa: RIL**, C. 55, S. 220, 2018, s. 233-257.
- Dean, William Tucker Jr.: “The Conflict of Conflict of Laws”, **Stanford Law Review**, C. 3, S. 3, 1951, s. 388-412.
- Dedezade, Esat: “Microsoft to Deliver Cloud Services From New Datacentres in Germany in 2019 to Meet Evolving Customer Needs”, 31.08.2018, (Çevrimiçi) <https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/>, 06.06.2022.
- Delerue, François: **Cyber Operations And International Law**, 1. bs, Cambridge UK, Cambridge University Press, 2020.
- Deradjat, ABNR-Agus Ahadi: “Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems | Lexology”, (19.08.2020), (Çevrimiçi) <https://www.lexology.com/library/detail.aspx?g=cd6e5251-6dd7-4b46-b6be-759c78c9bf7b>, 19.08.2020.
- Dixon, Martin, Robert McCorquodale, Sarah Williams: **Cases & Materials on International Law**, 6. bs, New York, Oxford University Press, 2016.

- Dodge, William S.: “International Comity In American Law”, **Columbia Law Review**, C. 115, S. 8, 2015, s. 2072-2142.
- Dodge, William S.: “Jurisdictional Reasonableness under Customary International Law: The Approach of the Restatement (Fourth) of United States Foreign Relations Law”, t.y.
- Doğan, İlyas: **Devletler Hukuku**, 4. bs, Ankara, Astana Yayınları, 2020.
- Doğan, Vahit: **Milletlerarası Özel Hukuk**, 8. bs, Ankara, Savaş Yayınevi, 2022.
- Du Plessis, Paul, Andrew Borkowski: **Borkowski’s Textbook on Roman Law**, 5. bs, New York, Oxford University Press, 2015.
- Duggal, Pavan: “Data Localization: A Review of Proposed Data Localization Legislation in India, With Learnings for The United States”, **Data Catalyst**, 2019, (Çevrimiçi) <https://datacatalyst.org/wp-content/uploads/2019/12/Data-Localization-Pavan-Duggal.pdf>, 04.10.2020.
- Dunham, Mitchol: “Arbitrary and Outdated: Reforming the Stored Communications Act”, 2018, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3258774](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258774), 19.03.2020.
- Dülger, Murat Volkan: “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, C.1 S.2 2019, s.71-174.
- Eichensehr, Kristen E.: “Data Extraterritoriality”, **Texas Law Review**, C. 95, 2017, s. 145-160.
- Eichensehr, Kristen E.: “The Cyber-Law of Nations”, **The Georgetown Law Journal**, C. 103, 2015, s. 317-380.
- Fabbrini, Federico, Edoardo Celeste: “The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders”, **German Law Journal**, C. 21, S. S1, 2020, s. 55-65.
- Fang, Binxing: **Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace**, Beijing, China, Springer International Publishing and Science Press Beijing, 2018.

- Focarelli, Carlo: **International Law**, Cheltenham, UK, Edward Elgar Publishing, 2019.
- Franzese, Patrick W.: “Sovereignty in Cyberspace: Can it exist?”, **Air Force Law Review**, C. 64, (Çevrimiçi), <https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist>, 26.12.2020.
- Fraser, Erica: “Data Localisation and the Balkanisation of the Internet”, **SCRIPTed: A Journal of Law, Technology and Society**, C. 13, S. 3, 2016, s. 359-373.
- Garnefsky, Andre: **Public Policy in Soviet Private International Law**, 2. bs, Netherlands, Springer Science Business Media, 1970.
- Garrie, Daniel, Irene Byhovsky: “Privacy and Data Protection in Russia Country Briefings”, **Journal of Law & Cyber Warfare**, C. 5, S. 2, 2017, s. 235-255.
- Gasser, Urs: “Cloud Innovation and the Law: Issues, Approaches, and Interplay”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 17.03.2014, (Çevrimiçi) <https://papers.ssrn.com/abstract=2410271>, 10.07.2017.
- Gavouneli, Maria: **Functional Jurisdiction in the Law of the Sea**, Leiden, Hollanda, Martinus Nijhoff Publishers, 2007.
- Geist, Michael: “What the USMCA means for Data Localization Rules and Local Businesses in Canada”, **Bot Populi**, 2019.
- Gillaspie, Adam: “Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law Comments”, **University of Kansas Law Review**, C. 66, S. 2, 2017, s. 459-484.
- Gimelstein, Shelli: “A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy”, **University of Illinois Journal of Law, Technology & Policy**, C. 2018, S. 1, 2018, s. 1-32.
- Glahn, Gerhard Von, James Larry Taulbee: **Law Among Nations An Introduction to Public International Law**, 11. bs, New York, NY, USA, Routledge Taylor & Francis Group, 2017.
- Godel, Moritz, Joshi Alexander, Robert Bond, Jose: **Facilitating Cross Border Data Flow in the Digital Single Market**, European Commission, Directorate-General of Communications Networks, Content & Technology, 2016.

Manuel Cabello,  
Daniel Fernandez:

Göçmen Uyarer,  
Sinem: “6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 5237 sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması”, 2019, (Çevrimiçi) <https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>, 24.05.2020.

Göger, Erdoğan: **Devletler Hususi Hukuku**, 4. bs, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1977.

Gözler, Kemal: **Anayasa Hukukunun Genel Esasları**, 13. bs, Bursa, Ekin Basım Yayın Dağıtım, 2021.

Gözler, Kemal: **Devletin Genel Teorisi**, 9. bs, Bursa, Ekin Basım Yayın Dağıtım, 2018.

Graber, Katherine: “Where in the World Is Your Data: Who Can Access It?”, **Federal Communications Law Journal**, C. 70, S. 1, 2018, s. 157-178.

Greenleaf, Graham: “Global Data Privacy Laws 2019: 132 National Laws & Many Bills”, **Privacy Laws & Business International Report**, C. 157, 2019.

Greenwald, Glenn,  
Ewen MacAskill: “NSA Prism Program Taps into User Data of Apple, Google and Others”, **The Guardian**, 2013, (Çevrimiçi) <https://www.pulitzer.org/files/2014/public-service/guardianus/02guardianus2014.pdf>, 17.10.2021.

Greze, Benjamin: “The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives”, **International Data Privacy Law**, C. 9, S. 2, 2019, s. 109-128.

Grusic, Ugljesa  
vd.: **Cheshire, North & Fawcett Private International Law**, ed. Paul Torremans, 15. bs, Oxford, Oxford University Press, 2017.

Gstrein, Oskar  
Josef, Andrej  
Zwitter: “Extraterritorial Application of the GDPR”, **Internet Policy Review** 2021, C. 10, S. 3, 2021, (Çevrimiçi) <https://research.rug.nl/en/publications/extraterritorial-application-of-the-gdpr-promoting-european-value>, 18.01.2023.

Heinegg, Wolff  
Heintschel von: “Legal Implications of Territorial Sovereignty in Cyberspace”, **NATO CCD COE Publications**, 2012, 7-19.

- Hemmings, Justin, Sreenidhi Srinivasan, Peter Swire: “Defining the Scope of ‘Possession, Custody, or Control’ for Privacy Issues and the Cloud Act”, **Journal of National Security Law and Policy**, C. Forthcoming 2020, 2019, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3469808](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469808), 16.03.2021 .
- Henriksen, Anders: **International Law**, 1. bs, New York, Oxford University Press, 2017.
- Hert, Paul De, Michal Czerniawski: “Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context”, **International Data Privacy Law**, C. 6, S. 3, 2016, s. 230-243.
- Heward- Mills, Dyann, Helga Turku: “California and the European Union Take the Lead in Data Protection”, **Hastings International and Comparative Law Review**, C. 43, S. 2, 2020, s. 319-338.
- Hill, Jonah Force: “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, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2430275](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275), 14.03.2021.
- Hixson, Kathleen: “Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States”, **Fordham International Law Journal**, C. 12, S. 1, 1988, s. 127-152.
- Hodson, Susannah: “Applying WTO and FTA Disciplines to Data Localization Measures”, **World Trade Review**, C. 18, S. 4, 2019, s. 579-607.
- Hoekman, Bernard, Petros C. Mavroidis: “WTO Reform: Back to the Past to Build for the Future”, **Global Policy**, No: 12, 2021.
- Hon, W. Kuan, Christopher Millard, Jatinder Singh, Ian Walden: “Policy, Legal and Regulatory Implications of a Europe-Only Cloud”, **International Journal of Law and Information Technology**, C. 24, S. 3, 2016, s. 251-278.
- Hong, Yanqing: “The Cross-Border Data Flows Security Assessment”, Working Paper, 2017, 13.
- Hong, Yanqing: “The Cross-Border Data Flows Security Assessment: An Important Part of Protecting China’s Basic Strategic



- Resources”, Working Paper, Yale Law School Paul Tsai China Center, 20.06.2017, (Çevrimiçi) <http://apide.org/apru-asia-eu-dialogue/readings/CrossBorderDataFlows.pdf>, 27.07.2020.
- Hong, Yu, Gerald Thomas Goodnight: “How to Think about Cyber Sovereignty: The Case of China”, **Chinese Journal of Communication**, 2020, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=346793](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=346793), 01.01.2021.
- Houser, Kimberly A., W. Gregory Voss: “GDPR: The End of Google and Facebook Or a New Paradigm in Data Privacy”, **Richmond Journal of Law & Technology**, C. 25, S. 1, 2018, s. 1-109.
- Huang, Jeanne: “Chinese private international law and online data protection”, **Journal of Private International Law**, C. 15, S. 1, 2019, s. 186-209.
- Huo, Zhengxin: “Highlights of China’s New Private International Law Act: From the Perspective of Comparative Law”, 2011, (Çevrimiçi) [https://ssl.editionsthemis.com/uploaded/revue/article/5973\\_45-3%20Huo.pdf](https://ssl.editionsthemis.com/uploaded/revue/article/5973_45-3%20Huo.pdf), 18.03.2020.
- Ingram, Jefferson L.: **Criminal Procedure: Theory and Practice**, 3. bs, Routledge, 2022.
- Innis, Mark, Adhika Wiyoso: “General Data Localization Requirements in Indonesia”, Jakarta, Baker McKenzie, 07.2018, (Çevrimiçi) [https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al\\_generaldatalocalizationrequirements\\_july2018.pdf?la=en](https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf?la=en), 18.08.2020.
- Isaacson, Cory: “Database Sharding: The Key to Database Scalability”, **Database Trends and Applications**, 14.08.2009, (Çevrimiçi) <https://www.dbta.com/Editorial/Trends-and-Applications/Database-Sharding--The-Key-to-Database-Scalability-55615.aspx>, 03.09.2021.
- Jennifer Huddleston, Jacqueline Varas: “Impact of Data Localization Requirements on Commerce and Innovation”, **American Action Forum**, 16.06.2020, (Çevrimiçi) <https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/>, 14.02.2021.

- Jensen, Eric Talbot: “Cyber Sovereignty: The Way Ahead”, **Texas International Law Journal**, C. 50, S. 2, 2015, s. 276-304.
- Johnston, David: **The Cambridge Companion to Roman Law**, 1. bs, New York, NY, USA, Cambridge University Press, 2015.
- Jones, Doone, Kim-Kwang Raymond Choo: “Should There Be a New Body of Law for Cyber Space?”, **22nd European Conference on Information Systems**, Tel Aviv, 2014, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2431614](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2431614), 24.12.2020.
- Justin Ling: “National | CBA National - Canadian Legal Affairs: The Battle Over Data Localization”, (2019), (Çevrimiçi) <https://www.nationalmagazine.ca/en-ca/articles/law/opinion/2019/the-battle-over-data-localization>, 22.10.2020.
- Kalender, Ata Umur: “Parçalı Bulutlar: Cloud Act ve Etkileri”, **Kişisel Verileri Koruma Dergisi**, C. 2, 2020, s. 74-107.
- Kemp, Richard: “Cloud Computing and Data Sovereignty”, 2016, (Çevrimiçi) <https://kempitlaw.com/insights/cloud-computing-and-data-sovereignty/>, 12.06.2019.
- Kent, Gail: “The Mutual Legal Assistance Problem Explained”, **Stanford Law School**, 23.02.2015, (Çevrimiçi) <https://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>, 06.05.2022.
- Kerr, Orin S.: “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It”, **The George Washington Law Review**, C. 72, 2003, s. 1208-1243.
- Kerr, Orin S.: “Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn’t”, **Northeastern University Law Review**, C. 97, S. 2, 2003, s. 607-674.
- Ketels, Christian, Arindam Bhattacharya, Liyana Satar: “Global Trade Goes Digital”, **BCG Henderson Institute**, (12.08.2019), (Çevrimiçi) <https://www.bcg.com/publications/2019/global-trade-goes-digital>, 19.05.2020.
- Kindt, E. J.: “Why Research May No Longer Be the Same: About the Territorial Scope of the New Data Protection Regulation”, **Computer Law & Security Review**, C. 32, S. 5, 2016, s. 729-748.

- Kirschenbaum, Andrew: “Beyond Microsoft: A Legislative Solution to the SCA’s Extraterritoriality Problem”, **Fordham Law Review**, C. 86, S. 4, 2018, s. 1923-1962.
- Klar, Manuel: “Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies”, **Hastings Science and Technology Law Journal**, C. 11, S. 2, 2020, s. 101-154.
- Korff, Douwe: “The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 19.08.2019, doi:10.2139/ssrn.3439293.
- Koschaker, Paul: **Modern Hususi Hukuka Giriş Olarak Roma Hususi Hukukunun Ana Hatları**, çev. Kudret Ayiter, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1971.
- Kruger, Ralph R., David J. Bercuson, William Lewis, Norman L. Nicholson, Roger D. Hall: “Canada”, **Encyclopedia Britannica**, 27.07.2022, (Çevrimiçi) <https://www.britannica.com/place/Canada>, 30.07.2022.
- Kuner, Christopher, (ed.), Lee A. Bygrave, Christopher Docksey, Laura Drechsler: **The EU General Data Protection Regulation (GDPR): A Commentary**, Oxford, New York, Oxford University Press, 2020.
- Kuner, Christopher: “Data Nationalism and Its Discontents”, **Emory Law Journal**, C. 64, 2015, s. 2089-2098.
- Kuner, Christopher: “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law”, **International Data Privacy Law**, C. 5, S. 4, 2015, s. 235-245.
- Kuner, Christopher: “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, **German Law Journal**, C. 18, S. 4, 2017, s. 881-918.

- Kuner, Christopher: “The Extraterritoriality of Data Privacy Laws—an Explosive Issue yet to Detonate”, **International Data Privacy Law**, C. 3, S. 3, 2013, s. 147-148.
- Kuner, Christopher: “The Internet and the Global Reach of EU Law”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 01.02.2017, doi:10.2139/ssrn.2890930.
- Kuyper, Pieter Jan: “The European Community and the US Pipeline Embargo: Comments on Comments”, **German Yearbook of International Law**, C. 27, 1984, (Çevrimiçi) <https://heinonline.org/HOL/Page?handle=hein.journals/gyl27&id=72&div=&collection=>, 10.04.2021.
- Küçük, Adnan: “Egemenlik (Hakimiyet), Halk Egemenliği ve Milli Egemenlik Anlayışında Esaslı Dönüşüm”, **Uyuşmazlık Mahkemesi Dergisi**, S. 6, 2016, s. 311-361.
- Küzeci, Elif: **Kişisel Verilerin Korunması**, 4. bs, İstanbul, On İki Levha Yayıncılık, 2021.
- Kyriakides, Eleni: “The CLOUD Act, E-Evidence, and Individual Rights”, **European Data Protection Law Review (EDPL)**, C. 5, S. 1, 2019, s. 99-106.
- Lambert, Paul: **Understanding the New European Data Protection Rules**, NW, CRC Press Taylor & Francis Group, 2018.
- Lee, Kyu Yub, Moon hee Cho, Jungu Kang, Minji Kang: “Welfare Effects of the EU GDPR and Data Localization Measures”, **World Economy Brief**, C. 9, S. 7, 2019, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3407208](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407208), 04.08.2020.
- Lee, Sangwoo: “A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing”, 2018, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3442428](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442428), 27.09.2020.
- Lewis, Mark: **Cloud Computing 2020**, 3. bs, London UK, Tom Barnes and Law Business Research Ltd., 2019.
- Lieven, Dominic, Martin McCauley: “Ethnic Relations and Russia’s ‘near-Abroad’”, **Encyclopedia Britannica**, 18.12.2021, (Çevrimiçi) <https://www.britannica.com/place/Russia>, 18.12.2021.

- Lin, Wei Chen: “Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third Party Doctrine, the Cloud and Encryption”, **DePaul Law Review**, C. 65, S. 3, 2016, s. 1093-1138.
- Linthicum, David: “How Cloud Computing Impacts Technology Evolution”, **InfoWorld**, 01.10.2021, (Çevrimiçi) <https://www.infoworld.com/article/3635092/how-cloud-computing-impacts-technology-evolution.html>, 01.11.2021.
- Liu, Jinhe: “China’s Data Localization”, **Chinese Journal of Communication**, C. 13, S. 1, 2020, s. 84-103.
- Lohman, Walter, Riley Walters: “Understanding the Chinese Challenge to the United States”, **The Heritage Foundation**, (2020), (Çevrimiçi) <https://www.heritage.org/asia/commentary/understanding-the-chinese-challenge-the-united-states>, 22.10.2021.
- Lowenfeld, Andreas F.: “Harold Maier, Comity and the Foreign Relations Restatement”, **Vanderbilt Journal of Transnational Law**, C. 36, S. 5, 2006, s. 1415-1426.
- Lynskey, Orla: “Extraterritorial Impact in Data Protection Law through an EU Law Lens”, Brexit Institute Working Paper Series, 2020, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3674413](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3674413), 25.09.2020.
- Lynskey, Orla: **The foundations of EU data protection law**, 1. bs, United Kingdom, Oxford University Press, 2015.
- Madiega, Tambiama: “Digital Sovereignty for Europe”, European Parliamentary Research Service, 2020, (Çevrimiçi) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf), 18.03.2021.
- Maillart, Jean-Baptiste: “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”, **Springer**, 2018, (Çevrimiçi) <https://link.springer.com/content/pdf/10.1007%2Fs12027-018-0527-2.pdf>, 05.07.2019.
- Mann, Francis: “The Doctrine of Jurisdiction in International Law”, **Recueil des Cours de l’Académie de droit international**, C. I, S. 111, 1964.
- Mao, Yahya Mohamed: “Microsoft Announces the End of the Germany Cloud”, 12.10.2018, (Çevrimiçi) <https://hackernoon.com/microsoft->

announces-the-end-of-the-germany-cloud-431bbe407b94,  
06.07.2022.

- Marel, Erik Van der: “Data localisation in the EU: the threat from inside”, **Encompass**, (12.2016), (Çevrimiçi) <https://encompass-europe.com/comment/data-localisation-in-the-eu-the-threat-from-inside>, 04.11.2020.
- Maxwell, Winston, Mark W. Brennan, Arpan A. Sura: “Demystifying the U.S. CLOUD Act: Assessing the law’s compatibility with international norms and the GDPR”, **Hogan Lovells**, 2019, (Çevrimiçi) [https://www.hoganlovells.com/~media/hoganlovells/pdf/2019/2019\\_01\\_15\\_whitepaper\\_demystifying\\_the\\_us\\_cloud\\_act.pdf](https://www.hoganlovells.com/~media/hoganlovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf), 14.03.2020.
- McCubbin, Sabrina: “Summary: The Supreme Court Rules in Carpenter v. United States”, **Lawfare**, 22.06.2018, (Çevrimiçi) <https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states>, 25.06.2020.
- McDougal, Luther L.: “‘Private’ International Law: Ius Gentium versus Choice of Law Rules or Approaches”, **The American Journal of Comparative Law**, C. 38, S. 3, 1990, s. 521-537.
- Meessen, Karl M.: “Conflict of Jurisdiction under the New Restatement”, **Law and Contemporary Problems**, C. 50, S. 3, 1987, s. 47-69.
- Mell, Peter, Timothy Grance: “The NIST Definition of Cloud Computing”, Recommendations of the National Institute of Standards and Technology, The National Institute of Standards and Technology, 2011, (Çevrimiçi) <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, 12.02.2017.
- Meltzer, Joshua P., Peter Lovelock: “Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia”, **Brookings**, (20.03.2018), (Çevrimiçi) <https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/>, 16.05.2020.
- Menthe, Darrel: “Jurisdiction in Cyberspace: A Theory of International Spaces”, **Michigan Telecommunications and Technology Law Review**, C. 4, S. 1, 1998, s. 69-103.
- Mihaylova, Iva: “Could the Recently Enacted Data Localization Requirements in Russia Backfire?”, U. of St. Gallen Law &

- Economics Working Paper No. 2015-07, 2015, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=262953](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=262953)  
 3, 13.03.2021.
- Millard,  
 Christopher: “Forced Localization of Cloud Services: Is Privacy the Real Driver?”, **IEEE Cloud Computing**, C. 2, S. 2, 2015, s. 10-14.
- Miller, Monica: “Tech War: Biden Moves to Halt US Exports to Huawei, Reports Say”, **BBC**, 31.01.2023, (Çevrimiçi)  
<https://www.bbc.com/news/business-64461877>, 02.02.2023.
- Mills, Alex: “The Private History of International Law”, **International and Comparative Law Quarterly**, C. 55, S. 1, 2006, s. 1-50.
- Mishra, Neha: “Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows”, **Vanderbilt Journal of Transnational Law**, C. 52, S. 2, 2019, s. 463-510.
- Mishra, Neha: “Data Localization Laws in a Digital World”, **The Public Sphere**, 2016, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=284802](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=284802)  
 2, 04.11.2020.
- Mitchell, Andrew  
 D., Jarrod  
 Hepburn: “Don’t Fence Me In: Reforming Trade And Investment Law To Better Facilitate Cross-Border Data Transfer”, **Yale Journal of Law & Technology**, C. 19, 2017, s. 182-237.
- Mitchell, Andrew  
 D., Neha Mishra: “Data at the Docks: Modernizing International Trade Law for the Digital Economy”, **Vanderbilt Journal of Transnational Law**, C. 20, S. 4, 2018, s. 1073-1134.
- Moniz, Graça  
 Canto: “Finally: A Coherent Framework for the Extraterritorial Scope of EU Data Protection Law - the End of the Linguistic Conundrum of Article 3(2) of the GDPR”, **UNIO – EU Law Journal**, C. 4, S. 2, 2018, s. 105-116.
- Moody, Glyn: “Microsoft Building Data Centers in Germany That US Government Can’t Touch”, **Ars Technica**, 11.12.2015, (Çevrimiçi)  
<https://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>, 09.07.2021.
- Mowbray,  
 Miranda: “The Fog over the Grimpen Mire: Cloud Computing and the Law”, **SCRIPTed: A Journal of Law, Technology and Society**, C. 6, S. 1, 2009, s. 132-146.

- Mueller, Milton: “Sovereignty and Cyberspace: Institutions and Internet Governance”, (Çevrimiçi) <https://www.intgovforum.org/multilingual/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>, 29.11.2020.
- Mulligan, Stephen P.: “Cross-Border Data Sharing Under the CLOUD Act”, **Congressional Research Service**, No: 7-5700, 2018, (Çevrimiçi) <http://www.crossborderdataforum.org/wp-content/uploads/2018/07/CRS-Cross-Border-Data-Sharing-Under-the-CLOUD-Act.pdf>, 05.07.2019.
- Musil, Steven: “Amazon Cloud Outage Downs Netflix, Quora”, **CNET**, 2011, (Çevrimiçi) <https://www.cnet.com/tech/services-and-software/amazon-cloud-outage-downs-netflix-quora/>, 17.03.2022.
- Nalçacıoğlu Erden, Zeynep: **Milletlerarası Yatırım Hukukunda Dolaylı Kamulaştırma**, İstanbul, XII Levha Yayıncılık, 2015.
- Nomer, Ergin: **Devletler Hususi Hukuku**, 22. bs, İstanbul, Beta Basım A.Ş., 2017.
- Nomer, Ergin: “Devletler Hususi Hukukunda Milletlerarası Yetki Mefhumi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 40, S. 1-4, 2011, s. 393-426.
- Nugraha, Yudhistira, Kautsarina, Ashwin Sastrosubroto: “Towards Data Sovereignty in Cyberspace”, **Third International Conference of Information and Communication Technology**, 2015, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2610314](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610314), 27.12.2020.
- Nussbaum, Arthur: “Rise and Decline of the Law-of-Nations Doctrine in the Conflict of Laws”, **Columbia Law Review**, C. 42, S. 2, 1942, s. 189-206.
- Öztürk, Mustafa, Akgün Bilgin: **Cezai ve Sınırşan Örgütlü Suçlarda Mücadelede - ABD ve Türkiye Arasında Karşılıklı Adli Yardımlaşma Rehberi**, 1. bs, İstanbul, Aristo Yayınevi, 2021.
- Pamir, Aybars: “Kapitülasyon Kavramı ve Osmanlı Devleti’ne Etkileri”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 51, S. 2, 2002, s. 79-119.
- Panday, Jyoti, Jeremy Malcolm: “The Political Economy of Data Localization”, **The Open Journal of Sociopolitical Studies**, Symposium 4, 2018, s. 511-527, (Çevrimiçi) <http://siba->



ese.unisalento.it/index.php/paco/article/viewFile/19553/166  
35, 12.03.2021.

- Pardede, Daniel,  
Adhika Wiyoso: “GR 82 No More! Now It Is GR 71!: New Regulation on Electronic System and Transactions”, Jakarta, Baker McKenzie, 10.2019, (Çevrimiçi)  
[https://f.datasrvr.com/fr1/319/37527/Corporate\\_Commercial\\_-\\_GR\\_82\\_no\\_more\\_Now\\_it\\_is\\_GR\\_71\\_\(Oct\\_2019\)\\_-\\_Final.pdf](https://f.datasrvr.com/fr1/319/37527/Corporate_Commercial_-_GR_82_no_more_Now_it_is_GR_71_(Oct_2019)_-_Final.pdf), 18.08.2020.
- Pazarcı, Hüseyin: **Uluslararası Hukuk**, 19. bs, Ankara, Turhan Kitabevi, 2020.
- Peace, Krista: “Where in the World Is My Data Today? The U.S. - U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigation”, **North Carolina Journal of International Law**, C. 47, 2022, s. 417-432.
- Pecoraro, Andrew J.: “Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act”, **Creighton Law Review**, C. 51, S. 1, 2017, s. 75-118.
- Peters, Robert J.,  
Alicia D. Loy,  
Matthew Osteen,  
Joseph Remy,  
Justin  
Fitzsimmons: “Not an Ocean Away, Only a Moment Away: A Prosecutor’s Primer for Obtaining Remotely Stored Data for Obtaining Remotely Stored Data”, **Mitchell Hamline Law Review**, C. 47, S. 3, 2021, s. 1073-1128.
- Pijpers, Peter  
B.M.J., Bart van  
den Bosch: “The ‘Virtual Eichmann’: on Sovereignty in Cyberspace”, **Amsterdam Law School Research Paper**, No: 2020-65, 2020, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=374684](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=374684)  
3, 01.01.2021.
- Pirker, Benedikt: “Territorial Sovereignty and Integrity and the Challenges of Cyberspace”, **Right and Obligations of States in Cyberspace Part 2**, he Peacetime Regime for State Activities in Cyberspace - International Law, Foreign Affairs and Cyber-Diplomacy, Tallinn, 2013, s. 189-216, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=301133](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=301133)  
7, 17.12.2020.
- Plessis, Paul J.  
Du, Clifford Ando,  
Kaius Tuori: **The Oxford Handbook of Roman Law And Society**, Great Britain, Oxford University Press, 2016.

- Pullen, Philip J.: “Nail in the MLAT Coffin: Examining Alternatives Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing”, **North Carolina Journal of International Law**, C. 44, S. 1, 2018, s. 1-16.
- Reydams, Luc: **Universal Jurisdiction International and Municipal Legal Perspectives**, New York, Oxford University Press, 2006.
- Richards, Neil: “The Third Party Doctrine and the Future of the Cloud”, **Washington University Law Review**, C. 94, S. 6, 2017, s. 1441-1492.
- Riedenberg, Joel R.: “Resolving Conflicting International Data Privacy Rules in Cyberspace”, **Stanford Law Review**, C. 52, S. 5, 2000, s. 1315-1372.
- Robinson, William Jeremy: “Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act”, **The Georgetown Law Journal**, C. 98, 2010, s. 1195-1239.
- Rojszczak, Marcin: “CLOUD act agreements from an EU perspective”, **Computer Law & Security Review**, C. 38, 2020, (Çevrimiçi)  
<https://www.sciencedirect.com/science/article/pii/S0267364920300479>, 27.09.2020.
- Roth, Emma: “TikTok and Oracle Teamed up after All, but Concerns about Data Privacy Remain”, **TheVerge**, 19.06.2022, (Çevrimiçi)  
<https://www.theverge.com/2022/6/19/23174775/tiktok-oracle-team-up-concerns-data-privacy-remain>, 11.11.2022.
- Rusbridger, Alan: “The Snowden Leaks and the Public”, **The New York Review**, 2013, (Çevrimiçi)  
<https://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/>, 20.01.2021.
- Rustad, Michael L., Thomas H. Koenig: “Towards a Global Data Privacy Standard”, **Florida Law Review**, C. 71, S. 2, 2019, s. 365-454.
- Rutherford, Miranda: “The CLOUD Act: Creating Executive Branch Monopoly Over Cross-Border Data Access”, 2019, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3508942](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3508942), 15.03.2020.
- Ryan, Patrick S., Sarah Falvey, Ronak Merchant: “When the Cloud Goes Local: The Global Problem with Data Localization”, **IEEE Computer Society**, 2013, 54-59.

- Ryngaert, Cedric: **Jurisdiction in International Law**, 2. bs, New York, Oxford University Press, 2015.
- Ryngaert, Cedric, Mistale Taylor: "Symposium on The GDPR And International Law The GDPR as Global Data Protection Regulation?", **AJIL Unbound**, C. 114, 2020, s. 5-9.
- Sacks, Samm, Justin Sherman: "The Global Data War Heats Up", **The Atlantic**, (26.06.2019), (Çevrimiçi) <https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/>, 21.05.2020.
- Sargsyan, Tatevik: "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security", **International Journal of Communication**, C. 10, 2016, s. 2221-2237.
- Sarp Nebil, Füsün: "PayPal neden Türkiye'den çekildi?", 2016, (Çevrimiçi) <https://t24.com.tr/yazarlar/fusun-sarp-nebil/paypal-neden-turkiyeden-cekildi,14690>, 10.11.2021.
- Savelyev, Alexander: "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?", **Computer Law & Security Review**, C. 32, S. 1, 2016, s. 128-145.
- Savigny, Friedrich K. von: **Private International Law and the Retrospective Operation of Statutes\_ A Treatise on the Conflict of Laws, and the Limits of their Operation in Respect of Place and Time**, 2. bs, Edinburgh, T&T Clark Law Publishers, 1880.
- Schiller, A. Arthur: **Texts and Commentary for the Study of Roman Law: Mechanisms of Development**, C. I, New York, Columbia University School of Law, 1936.
- Schmitt Michael N., Liis Vihul, (ed.): **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, 1. bs, United Kingdom, Cambridge University Press, 2017.
- Schultheis, Ned: "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry", **Brooklyn Journal of Corporate, Financial & Commercial Law**, C. 9, S. 2, 2015, s. 661-694.
- Schultz, Thomas: "Private Legal Systems: What Cyberspace Might Teach Legal Theorists", **Private Legal Systems**, 10 YALE J.L. & TECH. 151, 2007, s. 153-193, (Çevrimiçi)

<https://yjolt.org/sites/default/files/schultz-10-yjolt-151.pdf>,  
28.03.2019.

Schultz, Thomas,  
Niccolo Ridi: “Comity in US Courts”, **Northeastern University Law Review**, C. 10, S. 1, 2018, s. 280-365.

Schwartz, Paul M.: “Legal Access To The Global Cloud”, **Columbia Law Review**, C. 118, S. 6, 2018, s. 1681-1762.

Schwartz, Paul M.: “Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies”, **Bloomberg BNA Privacy and Security Law Report**, 2016, (Çevrimiçi)  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2862648](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862648), 14.05.2019.

Schwartz, Paul,  
Peifer: “Data Localization Under the CLOUD Act and the GDPR”, **Computer Law Review International**, S. 1, 2019, (Çevrimiçi)  
<https://paulschwartz.net/wp-content/uploads/2020/08/Schwartz-Peifer-Data-Localization-CRi-2019-1.pdf>, 27.09.2020.

Schwarz, Andreas: **Roma Hukuku Dersleri**, C. I, çev. Türkan Rado, 7. bs, İstanbul, Doğan Kardeş Basımevi, 1965.

Scott, Joanne: “Extraterritoriality and Territorial Extension in EU Law”, **American Journal of Comparative Law**, C. 62, S. 1, 2014, s. 87-126.

Selby, John: “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?”, **International Journal of Law and Technology**, C. 25, 2017, s. 213-232.

Sen, Nivedita: “Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?”, **Journal of International Economic Law**, C. 21, S. 2, 2018, s. 323-348.

Serwin, Andrew  
B., M. Leeann  
Habte, Jerry D.  
Brown: “Privacy in an Interconnected World”, **GP Solo**, C. 28, 2011, (Çevrimiçi)  
<https://www.foley.com/-/media/files/insights/publications/2011/06/privacy-in-an-interconnected-world/files/privacy-in-an-interconnected-world/fileattachment/privacy1106.pdf>, 09.03.2023.

Shaw, Malcolm N.: **International Law**, 8. bs, United Kingdom Padstow, Cornwall, Cambridge University Press, 2017.

- Sherman, Justin, Samuel Bendett: “Russia’s ‘Data Localization’ Efforts May Guide Other Governments”, **Defense One**, (04.09.2020), (Çevrimiçi) <https://www.defenseone.com/ideas/2020/01/russias-data-localization-push-may-guide-other-governments/162380/>, 04.09.2020.
- Sherman, Justin, Holden Triplett: “Why Russia, China, and Other Countries Are Demanding Big Tech Companies Build Local Offices”, **Future Tense**, (2022), (Çevrimiçi) <https://slate.com/technology/2022/02/data-localization-laws-china-russia-authoritarian.html>, 18.04.2022.
- Shyngyssov, Aset, Bakhytzhan Kadyroz, Zhamilya Bilisbekova: “Data Localization Laws: Overview (Kazakhstan)”, 2019, (Çevrimiçi) <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2019/datalocalizationlawsoverviewkazakhstan.pdf>, 22.10.2020.
- Sinha, Amber, Elonnai Hickok, Udbhav Tiwari, Arindrajit Basu: “Cross Border Data-Sharing and India A Study in Processes, Content and Capacity”, **The Centre for Internet & Society**, (Çevrimiçi) <https://cis-india.org/internet-governance/files/mlat-report>, 19.05.2020.
- Sitinjak, Posman Krismanto, Riva’atul Adaniah Wahab: “Policy Analysis of Data Localization in Digital Market Integration in Southeast Asian Region”, **Jurnal Masyarakat Telematika dan Informasi**, C. 10, S. 1, 2019, s. 41-50.
- Smith, Brad: “Answering Europe’s Call: Storing and Processing EU Data in the EU - EU Policy Blog”, 06.05.2021, (Çevrimiçi) <https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/>.
- Söğütlü, Özlem: **Roma Özel Hukuku**, 1. bs, Ankara, Seçkin Yayıncılık, 2020.
- Stepanova, Olga, Patricia Jechel: “The Privacy, Data Protection and Cybersecurity Law Review: Germany”, **The Law Reviews**, 2022, (Çevrimiçi) [https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,\(BDSG\)%20entered%20into%20force](https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Germany%20has%20been%20and%20still,(BDSG)%20entered%20into%20force), 28.10.2022.
- Stigall, Dan E.: “International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law”, **Hastings International and Comparative Law Review**, C. 35, S. 2, 2012, s. 324-382.

- Svantesson, Dan Jerker B., Felicity Gerry: “Access to extraterritorial evidence: The Microsoft cloud case and beyond”, **Computer Law & Security Review**, C. 31, S. 4, 2015, s. 478-489.
- Svantesson, Dan Jerker B.: “Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines”, OECD Digital Economy Papers, No. 301, 2020, (Çevrimiçi) [https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges\\_7fbaed62-en](https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en), 28.12.2020.
- Svantesson, Dan Jerker B.: “Article 4(1)(a) ‘establishment of the controller’ in EU data privacy law—time to rein in this expanding concept?”, **International Data Privacy Law**, C. 6, S. 3, 2016, s. 210-221.
- Svantesson, Dan Jerker B.: “Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation”, **International Data Privacy Law**, C. 5, S. 4, 2015, s. 226-234.
- Svantesson, Dan Jerker B.: “The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses”, **Stanford Journal of International Law**, C. 50, S. 1, 2014, s. 53-102.
- Swire, Peter, DeBrae Kennedy-Mayo: “Comments to EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data”, 2020, (Çevrimiçi) [https://edpb.europa.eu/sites/default/files/webform/public\\_consultation\\_reply/comments\\_to\\_edpb\\_recommendations\\_by\\_swire\\_and\\_mayo\\_2020.pdf](https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/comments_to_edpb_recommendations_by_swire_and_mayo_2020.pdf), 18.03.2021.
- Şanlı, Cemal, Emre Esen, İnci Ataman-Figaneşe: **Milletlerarası Özel Hukuk**, 10. bs, İstanbul, Beta Basım A.Ş., 2023.
- Şimşek, Kemal: **Yabancıların Türkiye’de Yargılanması ve Uluslararası Adli Yardımlaşma**, Adalet Yayınevi, 2014.
- Tahiroğlu, Bülent, Belgin Erdoğan: **Roma Hukuku Dersleri**, 14. bs, İstanbul, DER Kitabevi, 2020.
- Taylor, Mistale: “The EU’s Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect”, **International Data Privacy Law**, C. 5, S. 4, 2015, s. 246-256.

- Taylor, Richard D.: “‘Data Localization’: The Internet in the Balance”, **Telecommunications Policy**, C. 44, S. 8, 2020.
- Tekinalp, Gülören: **Milletlerarası Özel Hukuk Bağlama ve Usul Hukuku Kuralları**, 13. bs, İstanbul, Vedat Kitapçılık, 2020.
- Temme, Laura: “The Fourth Amendment - Unreasonable Search and Seizure”, **FindLaw**, 2019, (Çevrimiçi) <https://constitution.findlaw.com/amendment4.html>, 04.08.2019.
- Tene, Omer: “Microsoft v. USA: Location of Data and the Law of the Horse”, **IEEE Security Privacy**, C. 14, S. 6, 2016, s. 81-85.
- Tene, Omer: “Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation”, **Future of Privacy Forum**, 2013, (Çevrimiçi) [https://wiki.laquadrature.net/images/5/59/Future\\_of\\_Privacy\\_Forum\\_White\\_Paper\\_on\\_Jurisdiction.pdf](https://wiki.laquadrature.net/images/5/59/Future_of_Privacy_Forum_White_Paper_on_Jurisdiction.pdf), 22.09.2020.
- Teziç, Erdoğan: **Anayasa Hukuku (Genel Esaslar)**, 24. bs, İstanbul, Beta Basım A.Ş., 2020.
- Thapar, Romila, Joseph E. Schwartzberg, A.L. Srivastava: “India”, **Encyclopedia Britannica**, 27.07.2022, (Çevrimiçi) <https://www.britannica.com/place/India>, 30.07.2022.
- Thompson II, Richard M., Jared P. Cole: “Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)”, **Congressional Research Service**, 2015, (Çevrimiçi) <https://sgp.fas.org/crs/misc/R44036.pdf>, 03.8.2023.
- Thrubron, Rob: “Facebook’s Latin America VP Arrested in Brazil after Failing to Provide WhatsApp User Data Rob”, **Techspot**, 2016, (Çevrimiçi) <https://www.techspot.com/news/63970-facebook-latin-america-vp-arrested-brazil-after-%20failing.html>, 10.10.2021.
- Tian, George Yijun: “Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement: Join or Withdraw”, **Wisconsin International Law Journal**, C. 34, S. 2, 2016, s. 367-408.
- Toker, Ali Gümrah: **Milletlerarası Özel Hukukta İstinabe**, 1. bs, Adalet Yayınevi, 2015.

- Toy, Alan, Gehan Gunasekara: “Is There a Better Option than the Data Transfer Model to Protect Data Privacy”, **University of New South Wales Law Journal**, C. 42, S. 2, 2019, s. 719-746.
- Trachtman, Joel: “Cyberspace, Sovereignty, Jurisdiction, and Modernism”, **Indiana Journal of Global Legal Studies**, C. 5, S. 2, 1998, s. 561-581.
- Tu, Guangjian: **Private International Law in China**, Singapore, Springer International Publishing, 2016.
- Umur, Ziya: **Roma Hukuku Ders Notları**, 3. bs, İstanbul, Beta Basım A.Ş., 2010.
- Ursul, Mallory: “The States’ Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause Notes”, **Suffolk University Law Review**, C. 52, S. 4, 2019, s. 577-602.
- Ustaran Eduardo, (ed.): **European Data Protection Law and Practice**, Portsmouth NH USA, International Association of Privacy Professionals, 2018.
- Uzun, Fatih Burak: “Cloud Computing as an Investment under the ICSID Convention”, **Public and Private International Law Bulletin**, C. 38, S. 2, 2019, s. 519-545.
- Ünal, Şeref: **Uluslararası Hukuk**, 1. bs, Ankara, Yetkin Basım, 2005.
- Ünver, Akın, Grace Kim: “Cross-Border Data Transfers and Data Localization”, Edam Cyber Policy Paper Series 2016/3, 2016, (Çevrimiçi) [https://edam.org.tr/wp-content/uploads/2017/03/data\\_transfers\\_en.pdf](https://edam.org.tr/wp-content/uploads/2017/03/data_transfers_en.pdf), 04.09.2020.
- Van Alsenoy, Brendan: **Reconciling the (Extra)Territorial Reach of the GDPR with Public International Law**, Maklu, 2017.
- Vermeulen, Gert, Eva Lievens: **Data Protection and Privacy under Pressure**, Antwerp Belgium, Maklu, 2017.
- Vish: “How Much Data Is Created Every Day in 2021? [You’ll Be Shocked!]”, **TechJury**, 24.06.2020, (Çevrimiçi) <https://techjury.net/blog/how-much-data-is-created-every-day/>, 12.05.2021.
- Voigt, Paul, Axel Von dem Bussche: **The EU General Data Protection Regulation A Practical Guide**, Switzerland, Springer International Publishing, 2017.



- Voss, W. Gregory: “Cross-Border Data Flows, the GDPR, and Data Governance”, **Washington International Law Journal**, C. 29, S. 3, 2019, s. 485-532.
- Voss, W. Gregory, Kimberly A. Houser: “Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies”, **American Business Law Journal**, C. 56, S. 2, 2019, s. 287-344.
- Warken, Claudia, Lodewijk Van Zwieten, Dan Jerker B. Svantesson: “Re-Thinking the Categorisation of Data in the Context of Law Enforcement Cross-Border Access to Evidence”, **International Review of Law, Computers & Technology**, 2019, (Çevrimiçi) <https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1600871>, 07.05.2019.
- Watts, Sean, Theodore T. Richard: “Baseline Territorial Sovereignty and Cyberspace”, **Lewis & Clark Law Review**, C. 22, S. 3, 2018, s. 803-872.
- Webster, Graham, Scarlet Kim: “The Data Arms Race Is No Excuse for Abandoning Privacy”, **Foreign Policy**, (14.08.2018), (Çevrimiçi) <https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/>, 20.05.2020.
- Wheeler Cook, Walter: “The Application of the Criminal Law of a Country to Acts Committed by Foreigners Outside the Jurisdiction”, **West Virginia Law Review**, C. 40, S. 4, 1934, s. 303-329.
- Wimmer, Kurt: “Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers First Amendment Symposium”, **Syracuse Law Review**, C. 68, S. 3, 2018, s. 547-578.
- Wimmer, Kurt: “The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?”, **Communications Lawyer**, 2017, 16-21.
- Wong, Benjamin: “Data Localization and ASEAN Economic Community”, **Asian Journal of International Law**, C. 10, S. 1, 2020, s. 158-180.
- Woods, Andrew Keane: “Litigating Data Sovereignty”, **Yale Law Journal**, C. 128, S. 2, 2018, s. 328-407.
- Yılmaz, Altuğ: “Anglo - Amerikan Aleminin İlk Önemli Devletler Hususi Hukukçusu Joseph Story”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 24 S. 1-4, 1959 s.63-75.

- Yoon, Julia: “South Korean Data Localization: Shaped by Conflict”, **Henry M. Jackson School of International Studies**, (28.02.2018), (Çevrimiçi) <https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/>, 14.04.2020.
- Zeno-Zencovich, Vincenzo: “Around the CJEU Schrems Decision: Digital Sovereignty and International Governance of Telecommunication Networks”, 2016, (Çevrimiçi) [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2788789](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2788789), 15.12.2020.
- Zhang, Qi, Lu Cheng, Raouf Boutaba: “Cloud Computing: State-of-the-Art and Research Challenges”, **Journal of Internet Services and Applications**, C. 1, S. 1, 2010, s. 7-18.
- “2016 - 2019 Ulusal Siber Güvenlik Stratejisi”, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (13.02.2021), (Çevrimiçi) <https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>, 13.02.2021.
- 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019), (Çevrimiçi) <https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf>, 26.09.2021.
- “2021 Country Reports on Human Rights Practices: United Kingdom”, U.S. Department of State, 12.04.2022, (Çevrimiçi) <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/united-kingdom/>, 05.10.2022.
- 5411 Sayılı Bankacılık Kanunu (2005), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5>, 17.10.2021.
- “5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu”, 01.03.2006, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5464&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.
- “5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun”, 16.08.2021, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5>.

5684 Sayılı Sigortacılık Kanunu (2007), (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5684&MevzuatTur=1&MevzuatTertip=5>, 22.12.2021.

5718 Sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun (2007), (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5718&MevzuatTur=1&MevzuatTertip=5>, 16.03.2021.

“5809 Sayılı Elektronik Haberleşme Kanunu”, 10.11.2008, (Çevrimiçi)  
<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf>, 30.06.2021.

“6361 Sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu”, 13.12.2012, (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6361&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

“6362 Sayılı Sermaye Piyasası Kanunu”, 30.12.2012, (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6362&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

“6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun”, 27.06.2013, (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6493&MevzuatTur=1&MevzuatTertip=5>, 18.10.2021.

“6639 Sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun”, (27.03.2015), (Çevrimiçi)  
<https://www.resmigazete.gov.tr/eskiler/2015/04/20150415-1.htm>, 10.05.2021.

“6698 Sayılı Kişisel Verilerin Korunması Kanunu”, 07.04.2016, (Çevrimiçi)  
[mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5](https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5).

7194 sayılı Dijital Hizmet Vergisi ile Bazı Kanunlarda ve 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun (2019), (Çevrimiçi)  
<https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=7194&MevzuatTur=1&MevzuatTertip=5>, 11.11.2020.

“Availability Zone Service and Regional Support”, 01.10.2023, (Çevrimiçi) <https://learn.microsoft.com/en-us/azure/reliability/availability-zones-service-support>, 11.01.2023.

“AWS Global Infrastructure”, 01.10.2023, (Çevrimiçi) [https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h\\_ls](https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls), 11.01.2023.

“Banka Kartları ve Kredi Kartları Hakkında Yönetmelik”, 10.03.2007, (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=11180&MevzuatTur=7&MevzuatTertip=5>, 18.10.2021.

“Bankacılık Düzenleme ve Denetleme Kurumu”, (03.11.2021), (Çevrimiçi) <https://www.bddk.org.tr/>, 03.11.2021.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (2020), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=34360&MevzuatTur=7&MevzuatTertip=5>, 26.05.2020.

Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik (2014), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19864&MevzuatTur=7&MevzuatTertip=5>, 17.10.2021.

Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ (2013), (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2013/12/20131204-9.htm>, 18.10.2021.

Bilgi Sistemleri Yönetimi Tebliği (VII-128.9) (2018), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=24296&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

“Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2018/DK-YED/27”, 22.01.2018, (Çevrimiçi) <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>, 05.06.2021.

“Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2019/DK-TED/053”, 12.02.2019, (Çevrimiçi)  
<https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf>, 05.06.2021.

“Bilgi Teknolojileri ve İletişim Kurulu Kararı, Karar No: 2020/DK-İD/274”, 29.09.2020, (Çevrimiçi)  
<https://www.resmigazete.gov.tr/eskiler/2020/10/20201002-5.pdf>, 20.10.2021.

“Bilgi ve İletişim Güvenliği Rehberi”, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 07.2020, (Çevrimiçi)  
[https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg\\_rehber.pdf](https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf), 27.06.2021.

Bill of Rights - Fifth Amendment [Grand Jury, Double Jeopardy, Self-Incrimination, Due Process] (1791), (Çevrimiçi)  
[https://www.law.cornell.edu/constitution/fifth\\_amendment](https://www.law.cornell.edu/constitution/fifth_amendment).

Bill of Rights - First Amendment [Religion, Speech, Press, Assembly, Petition] (1791), (Çevrimiçi)  
[https://www.law.cornell.edu/constitution/first\\_amendment](https://www.law.cornell.edu/constitution/first_amendment).

Bill of Rights - Fourth Amendment [Search and Seizure] (1791), (Çevrimiçi)  
[https://www.law.cornell.edu/constitution/fourth\\_amendment](https://www.law.cornell.edu/constitution/fourth_amendment).

Bill of Rights - Ninth Amendment [Non-Enumerated Rights] (1791), (Çevrimiçi)  
[https://www.law.cornell.edu/constitution/ninth\\_amendment](https://www.law.cornell.edu/constitution/ninth_amendment).

Bill of Rights - Third Amendment [Quartering of Troops] (1791), (Çevrimiçi)  
[https://www.law.cornell.edu/constitution/third\\_amendment](https://www.law.cornell.edu/constitution/third_amendment).

Blackmer v. United States, 200, 201 (U.S. Supreme Court 1932).

“Brazil”, **Encyclopedia Britannica**, 20.12.2021, (Çevrimiçi)  
<https://www.britannica.com/place/Brazil>, 20.12.2021.

Brigham City v. Stuart, 05-502 (U.S. Supreme Court 22 Mayıs 2006).

“BTK”, (03.11.2021), (Çevrimiçi) <https://www.btk.gov.tr/>, 03.11.2021.

“Bulut Bilişim Güvenlik ve Kullanım Standardı”, Türk Standartları Enstitüsü, 07.03.2014, (Çevrimiçi) <https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf>, 10.03.2022.

“Canada: Cross-border transfers and data localisation after the USMCA | Insights | DataGuidance”, **OneTrust Data Guidance**, (06.2020), (Çevrimiçi) <https://www.dataguidance.com/opinion/canada-cross-border-transfers-and-data-localisation>, 11.09.2020.

Carpenter v. United States, C. 585, C. 585 U.S. Reports (ABD Yüksek Mahkemesi 2018).

Case Concerning Barcelona Traction, Light and Power Company Limited (Belgium vs. Spain), 1962 (International Court of Justice 05 Şubat 1970).

“Cathay Pasific Airway Limited hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/144 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 16.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5480/2019-144>, 18.03.2020.

“CBDDO”, (03.11.2021), (Çevrimiçi) <https://cbddo.gov.tr/>, 03.11.2021.

“Charter of Fundamental Rights of the European Union”, Official Journal of the European Union, 26.10.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>, 15.08.2021.

Chicago Convention on International Civil Aviation (1977), (Çevrimiçi) <https://www.icao.int/publications/pages/doc7300.aspx>, 20.01.2021.

“Choosing a Cloud Platform”, **Amazon Web Services**, 26.07.2018, (Çevrimiçi) <https://perma.cc/97WA-QTFM>, 30.05.2021.

Clarifying Lawful Overseas Use of Data Act, H.R. 4943 (2018).

**Commission Staff Working Document Impact Assessment**, Brussels, European Commission, 2018 (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN>, 10.11.2020.

“Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”, European Commission, 19.02.2020, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&qid=1634039084372&from=EN>, 17.07.2021.

Connally v. Georgia, 429 U.S. 245 (1977) (U.S. Supreme Court 10 Ocak 1977).

“Consultation Paper on Regulatory Framework for Over-the-top (OTT) Services”, New Delhi, Telecom Regulatory Authority of India, 18.11.2018, (Çevrimiçi) [https://www.trai.gov.in/sites/default/files/CPOTT12112018\\_0.pdf](https://www.trai.gov.in/sites/default/files/CPOTT12112018_0.pdf), 11.10.2022.

“Convention No. 185 of the Council of Europe on Cybercrime (Budapest Convention)”, 23.11.2001, (Çevrimiçi) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, 26.08.2020.

Conventions on the Law of the Sea (1958), (Çevrimiçi) <https://legal.un.org/avl/ha/gclos/gclos.html>, 11.01.2021.

Coolidge v. New Hampshire, 403 U.S. 443 (1971) (U.S. Supreme Court 21 Haziran 1971).

“Country Reports on Human Rights Practices”, 12.04.2022, (Çevrimiçi) <https://www.state.gov/reports-bureau-of-democracy-human-rights-and-labor/country-reports-on-human-rights-practices/>, 10.05.2022.

Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 (1996), (Çevrimiçi) <https://www.congress.gov/bill/104th-congress/house-bill/927/text>, 29.03.2021.

Cybersecurity Law of the People’s Republic of China (2017), (Çevrimiçi) <https://www.newamerica.org/cybersecurity->

initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, 25.07.2020.

“Cyberspace Administration of China”, (03.11.2021), (Çevrimiçi) <http://www.cac.gov.cn/>, 03.11.2021.

“Çerez Uygulamaları Hakkında Rehber”, **Kişisel Verileri Koruma Kurumu**, 2022, (Çevrimiçi) <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf>, 11.11.2022.

“Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows”, World Economic Forum, 2020, (Çevrimiçi) [http://www3.weforum.org/docs/WEF\\_Paths\\_Towards\\_Free\\_and\\_Trusted\\_Data%20Flows\\_2020.pdf](http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf), 09.12.2021.

“Data Localisation Requirements Narrowed in Vietnam’s Cybersecurity Law”, **The Business Times**, (15.10.2019), (Çevrimiçi) <https://www.businesstimes.com.sg/asean-business/opinion/data-localisation-requirements-narrowed-in-vietnams-cybersecurity-law>, 15.05.2020.

“Data Protection and Privacy Legislation Worldwide”, **UNCTAD**, (01.11.2021), (Çevrimiçi) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>, 01.11.2021.

“Data Protection Laws of The World Angola vs Brazil”, **DLA Piper**, 2017, 14.

“Declaration Building the next generation cloud for businesses and the public sector in the EU”, the Informal Video Conference of the Ministers responsible for Telecommunications/Digital Policy, 15.10.2020, (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>, 18.03.2021.

“Department of Defense Strategy for Operating in Cyberspace”, ABD Savunma Bakanlığı, 2011, (Çevrimiçi) <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>, 20.01.2021.

“Digital Sovereignty for Europe”, European Parliamentary Research Service, 2020, (Çevrimiçi)



[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf), 18.03.2021.

“Documents Show NSA and GCHQ Spied on Partner Turkey”, (17.05.2021), (Çevrimiçi)  
<https://www.spiegel.de/international/world/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html>, 17.05.2021.

**DOD Dictionary of Military and Associated Terms**,  
<https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>, USA Department of Defense, 2021.

“Dubsmash Inc. hakkında Kişisel Verileri Koruma Kurulunun 17/07/2019 Tarihli ve 2019/222 Sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 17.07.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5523/-Dubsmash-Inc-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-17-07-2019-Tarihli-ve-2019-222-Sayili-Karari-Ozeti>, 18.03.2020.

“Economy of Saudi Arabia”, **Encyclopedia Britannica**, 08.01.2022, (Çevrimiçi)  
<https://www.britannica.com/place/Saudi-Arabia/Economy#ref259141>, 09.01.2022.

Editor, CSRC Content: “Cyberspace - Glossary | CSRC”, (14.04.2021), (Çevrimiçi)  
<https://csrc.nist.gov/glossary/term/cyberspace>, 14.04.2021.

EDPS: “Opinion of the European Data Protection Supervisor on the data protection reform package”, Görüş, Brüksel, EDPS, 07.03.2012, (Çevrimiçi)  
[https://edps.europa.eu/sites/edp/files/publication/12-03-07\\_edps\\_reform\\_package\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf).

EEOC v. Arabian American Oil Co., 89-1838, 89-1845 (U.S. Supreme Court 1991).

“Elektrikli Skuter Yönetmeliği”, Resmi Gazete, 14.04.2021, (Çevrimiçi)  
<https://www.resmigazete.gov.tr/eskiler/2021/04/20210414-3.htm>, 23.05.2021.

Elektronik Defter Genel Tebliği (Sıra No:1) (17.07.2020), (Çevrimiçi)  
<https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=15570&mevzuatTur=Tebliğ&mevzuatTertip=5>, 17.07.2020.

“EP Draft Report LIBE 2012”, European Parliament, 2012, (Çevrimiçi)

[https://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/pr/922/922387/922387en.pdf](https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf), 14.12.2021.

“EP Resolution GDPR 2014”, European Parliament, 12.03.2014, (Çevrimiçi)

[https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_EN.html), 14.12.2021.

“Establishing a Trusted Cloud Europe”, **Publications Office of the European Union**, 2014, 28.

“EU Position in World Trade - Trade - European Commission”, 09.02.2019, (Çevrimiçi)

<https://ec.europa.eu/trade/policy/eu-position-in-world-trade/>, 12.10.2021.

Europäische Union, Europarat, (ed.): **Handbook on European Data Protection Law**, 2018 edition., Luxembourg, Publications Office of the European Union, 2018.

European Commission: “How Will the EU’s Data Protection Reform Make International Cooperation Easier?”, Görüş, 01.2016, (Çevrimiçi) <https://op.europa.eu/en/publication-detail/-/publication/43a3511e-f681-11e7-b8f5-01aa75ed71a1/language-en/format-PDF>, 29.05.2020.

“European Convention on Human Rights”, Council of Europe, 03.09.1953, (Çevrimiçi)

[https://www.echr.coe.int/documents/convention\\_eng.pdf](https://www.echr.coe.int/documents/convention_eng.pdf), 15.08.2021.

“European Digital Infrastructure and Data Sovereignty - A Policy Perspective”, EIT Digital, 2020, (Çevrimiçi)

<https://www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/full-report/EIT-Digital-Data-Sovereignty-Full-Report.pdf>, 12.02.2022.

Ex parte Jackson, C. 96, C. 96 U.S. Reports 727 (ABD Yüksek Mahkemesi 1877).

Export Control Reform Act of 2018 (2018), (Çevrimiçi)

<https://www.congress.gov/bill/115th-congress/house-bill/5040>, 29.03.2021.

“Facebook hakkında Kişisel Verileri Koruma Kurulunun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 11.04.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5481/2019-104>, 18.03.2020.

“Facebook hakkında Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 18.09.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5534/2019-269>, 18.03.2020.

Federal Communications Act, 73-416 (1934), (Çevrimiçi) <https://transition.fcc.gov/Reports/1934new.pdf>, 17.11.2022.

Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ (2019), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=31395&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

“G20 Osaka Leaders’ Declaration”, 2019, (Çevrimiçi) [https://www.consilium.europa.eu/media/40124/final\\_g20\\_osaka\\_leaders\\_declaration.pdf](https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf), 20.07.2020.

“G20 Riyadh Summit Leaders’ Declaration”, 2020, (Çevrimiçi) <https://www.oecd.org/g20/g20-riyadh-summit.pdf>, 20.01.2021.

“G20 Rome Leaders’ Declaration”, 2021, (Çevrimiçi) <https://www.governo.it/sites/governo.it/files/G20ROMELEADERSDECLARATION.pdf>, 13.02.2022.

“German Schools Ban Microsoft Office 365 amid Privacy Concerns (Updated)”, TNW, 15.07.2019, (Çevrimiçi) [https://thenextweb.com/news/german-schools-ban-microsoft-office-365-amid-privacy-concerns?\\_\\_twitter\\_impression=true](https://thenextweb.com/news/german-schools-ban-microsoft-office-365-amid-privacy-concerns?__twitter_impression=true), 11.11.2021.

“Glossary of Foreign Direct Investment Terms and Definitions”, OECD, 30.04.2008, (Çevrimiçi) <https://www.oecd.org/daf/inv/investment-policy/2487495.pdf>, 28.10.2021.

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12 (European Court of Justice 13 Mayıs 2014).

“Government Relaxes Data Localisation Requirement”, Assegaf Hamzah & Partners, 25.10.2019, (Çevrimiçi) <https://id.rajahtannasia.com/media/3544/ahpclientupdate-25october2019.pdf>, 21.07.2020.

Griswold v. Connecticut, C. 381, C. 381 U.S. Reports 479 (U.S. Supreme Court 1965).

“Groups Urge Congress to Oppose US-UK Cloud Act Agreement”, **Human Rights Watch**, (29.10.2019), (Çevrimiçi) <https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement>, 14.03.2020.

“Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1”, European Data Protection Board, 12.11.2019, (Çevrimiçi) [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_after\\_public\\_consultation\\_en\\_1.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf).

Hartford Fire Insurance Co. et al. v. California et al., 91-111 (U.S. Supreme Court 28 Haziran 1993).

Hilton v. Guyot, 159 U.S. 113 (1895), C. 159, C. 159 U.S. Reports 113 (U.S. Supreme Court 1895).

Hoffa v. United States, C. 385, C. 385 U.S. Reports 293 (U.S. Supreme Court 1966).

“How Much Data Is Generated Each Day?”, **World Economic Forum**, (12.05.2021), (Çevrimiçi) <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/>, 12.05.2021.

“<https://kvkk.gov.tr/Icerik/5533/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Zynga-Game-Ireland-Limited>”, Kişisel Verileri Koruma Kurumu, 26.09.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5533/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Zynga-Game-Ireland-Limited>, 18.03.2021.

In re Search Warrant No. 16-960-M-01 to Google ve In re Search Warrant No. 16-1061-M to Google, Case 2:16-mj-01061-TJR (The United States District Court for the Eastern District of Pennsylvania 03 Şubat 2017).

“In the United States District Court for the Eastern District of Pennsylvania Memorandum of Decision”, 2017, (Çevrimiçi) <https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf>, 10.11.2021.

“Indonesia”, **Encyclopedia Britannica**, 05.01.2022, (Çevrimiçi) <https://www.britannica.com/place/Indonesia>, 06.01.2022.

“Indonesia Relaxes Data Storage Rules to Allow Placement Abroad”, **Reuters**, (24.10.2019), (Çevrimiçi) <https://www.reuters.com/article/us-indonesia-tech-data-idUSKBN1X31P5>, 19.08.2020.

“İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun”, (29.07.2020), (Çevrimiçi) <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>.

Island of Palmas Case (or Miangas), United States v Netherlands, C. Reports of International Arbitral Awards (Permanent Court of Arbitration 1928).

Johnson v. United States, C. 333, C. 333 U.S. Reports 10 (U.S. Supreme Court 1947).

“Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton”, **The United States Department of Justice**, 07.10.2019, (Çevrimiçi) <https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us>, 10.10.2021.

“Joint Statement by the United States and the United Kingdom on Data Access Agreement”, **The United States Department of Justice**, 21.07.2022, (Çevrimiçi) <https://www.justice.gov/opa/pr/joint-statement-united-states-and-united-kingdom-data-access-agreement>, 08.09.2022.

“Joint US-EU Statement on Electronic Evidence Sharing Negotiations”, **The United States Department of Justice**, 26.09.2019, (Çevrimiçi)

<https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations>, 10.10.2021.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Acer Sales International SA”, Kişisel Verileri Koruma Kurumu, 18.03.2021, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/6908/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Acer-Sales-International-SA>, 10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Air India Limited”, Kişisel Verileri Koruma Kurumu, 01.04.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6942/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Air-India-Limited>, 10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) - ANIMOTO Inc. (Animoto)”, Kişisel Verileri Koruma Kurumu, 24.01.2019, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/5349/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi->, 18.03.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Cathay Pacific Airways Limited”, Kişisel Verileri Koruma Kurumu, 30.10.2018, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/5297/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi->, 18.03.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – EasyJet Plc”, Kişisel Verileri Koruma Kurumu, 28.05.2020, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/6744/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-EasyJet-Plc>, 18.03.2021.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Fluke Corporation ve Fluke Electronics Corporation”, Kişisel Verileri Koruma Kurumu, 16.07.2020, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/6775/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Fluke-Corporation-ve-Fluke-Electronics-Corporation>, 22.10.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – GoDaddy.com, LLC”, Kişisel Verileri Koruma Kurumu, 23.12.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7127/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-GoDaddy-com-LLC-GoDaddy->, 10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Hanon Automotive Climate Sys. Manufacturing Industrial and

Commercial Co.”, Kişisel Verileri Koruma Kurumu, 27.10.2020, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/6829/Hanon-Automotive-Climate-Sys-Manufacturing-Industrial-and-Commercial-Co->,  
10.02.2021.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Industries S.p.A.”, Kişisel Verileri Koruma Kurumu, 27.01.2022, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7165/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Industries-S-p-A->,  
22.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Marriott International, Inc.”, Kişisel Verileri Koruma Kurumu, 05.12.2018, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/5322/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi->, 18.03.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Motor Trend Group LLC”, Kişisel Verileri Koruma Kurumu, 03.08.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/7024/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Motor-Trend-Group-LLC->,  
10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Panasonic Business Support Europe GmbH”, Kişisel Verileri Koruma Kurumu, 07.10.2021, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/7060/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Panasonic-Business-Support-Europe-GmbH->,  
10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Pied Piper Fansub (piedpiperfb.com)”, Kişisel Verileri Koruma Kurumu, 18.08.2021, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/7040/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pied-Piper-Fansub-piedpiperfb-com->,  
10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – Subway International B.V.”, Kişisel Verileri Koruma Kurumu, 18.08.2021, (Çevrimiçi)  
<https://kvkk.gov.tr/Icerik/7039/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Subway-International-B-V->, 10.02.2022.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) - Ticketmaster UK”, Kişisel Verileri Koruma Kurumu, 29.06.2018,

(Çevrimiçi) <https://kvkk.gov.tr/Icerik/5244/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi->, 18.03.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – UiPath SRL”, Kişisel Verileri Koruma Kurumu, 22.12.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6848/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-UiPath-SRL>, 10.02.2021.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi, 2019) – Microsoft Corporation”, Kişisel Verileri Koruma Kurumu, 10.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5451/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation>, 18.03.2020.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi, 2020) – Microsoft Corporation”, Kişisel Verileri Koruma Kurumu, 04.02.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6670/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Microsoft-Corporation>, 18.03.2021.

“Kamuoyu Duyurusu (Veri İhlali Bildirimi) – ClearVoiceResearch.com, LLC”, Kişisel Verileri Koruma Kurumu, 04.05.2021, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6964/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-ClearVoiceResearch-com-LLC>, 10.02.2022.

Katz v. United States, C. 389, C. 389 U.S. Reports 347 (U.S. Supreme Court 1967).

“Kazakhstan”, **Encyclopedia Britannica**, 16.12.2021, (Çevrimiçi) <https://www.britannica.com/place/Kazakhstan>, 17.12.2021.

Kazakistan Cumhuriyeti Kişisel Veri ve Kişisel Verinin Korunması Kanunu (09.09.2020), (Çevrimiçi) <https://adilet.zan.kz/eng/docs/Z1500000418>, 09.09.2020.

“Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 Tarih Ve 2019/10 Sayılı Kararına İlişkin Duyuru”, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>, 01.05.2022.

“Kişisel Verileri Koruma Kurumu Veri İhlali Bildirimleri”, Kişisel Verileri Koruma Kurumu, (Çevrimiçi) <https://kvkk.gov.tr/veri-ihlali-bildirimi/?&page=14>, 10.11.2021.



“Kişisel Verilerin Korunması Kurumu”, **KVKK**, (03.11.2021), (Çevrimiçi) <https://www.kvkk.gov.tr/>, 03.11.2021.

Law on Cybersecurity, C. 24, C. 24 § (2018), (Çevrimiçi) <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>, 17.03.2020.

Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) (U.S. Supreme Court 11 Haziran 1979).

Lotus Case, France v. Turkey (Permanent Court of International Justice 1927).

Lozan Antlaşması (1923).

“Mapping Approaches to Data and Data Flows”, Suudi Arabistan, OECD, 2020, (Çevrimiçi) <https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf>, 18.03.2021.

“Marriott International Inc. hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Karar Özeti”, Kişisel Verileri Koruma Kurumu, 16.05.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5479/2019-143>, 18.03.2020.

Maryland v. Garrison, C. 480, C. 480 U.S. Reports 79 (U.S. Supreme Court 1986).

“Microsoft Azure Germany”, **Microsoft**, 26.07.2018, (Çevrimiçi) <https://perma.cc/A3K9-HYM8>, 30.05.2021.

“Microsoft Cloud Germany”, **Microsoft**, 2016, (Çevrimiçi) <https://go.microsoft.com/fwlink/?LinkId=839380&clcid=0x409>.

Microsoft Corp v. United States, 14-2985 (United States Court of Appeals for the Second Circuit 14 Temmuz 2016).

Microsoft Corp v. United States (Supreme Court of the United States 17 Nisan 2018).

Morrison v. National Australia Bank Ltd. (No. 08-1191) (U.S. Supreme Court 24 Haziran 2010).

“NATO Warsaw Summit Communiqué”, 2016, (Çevrimiçi) [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](http://www.nato.int/cps/en/natohq/official_texts_133169.htm), 11.04.2021.

“Netflix on AWS”, Amazon Web Services (04.03.2022), (Çevrimiçi) <https://aws.amazon.com/tr/solutions/case-studies/netflix/>, 04.03.2022.

“OECD Glossary of Statistical Terms”, OECD, 2004.

Olmstead v. United States, C. 277, C. 277 U.S. Reports 438 (U.S. Supreme Court 1928).

Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ (18.10.2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19817&MevzuatTur=9&MevzuatTertip=5>, 18.10.2021.

Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39081&MevzuatTur=9&MevzuatTertip=5>, 15.01.2022.

“Permanent Court of International Justice | International Court of Justice”, (26.03.2021), (Çevrimiçi) <https://www.icj-cij.org/en/pcij>, 26.03.2021.

Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09) (Grand Chamber 07 Aralık 2010).

Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2012/0011 (2012), (Çevrimiçi) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF>, 11.01.2021.

Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Çevrimiçi)

[http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf), 20.08.2017.

“Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union”, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>, 08.08.2021.

Regulation of the Government of the Republic of Indonesia number 82 of 2010 concerning Electronic System and Transaction Operation, (Çevrimiçi) <https://media2.mofo.com/documents/indonesia+government+regulation+no.+82+of+2012.pdf>, 22.08.2020.

“Report No.99-541”, U.S. Code Congressional and Administrative News (U.S.C.C.A.N.), 1986, (Çevrimiçi) <https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senatorept-99-541-1986.pdf>, 11.11.2022.

“Report of the Meeting Held on 2 March 2018, Note by the Secretariat, S/C/M/134”, World Trade Organization, 05.04.2018, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M134.pdf&Open=True>, 29.07.2020.

“Report of the Meeting Held on 6 October 2017, Note by the Secretariat, S/C/M/133”, World Trade Organization, 06.11.2017, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M133.pdf&Open=True>, 29.07.2020.

“Report of the Meeting Held on 12 October 2018, Note by the Secretariat, S/C/M/136”, World Trade Organization, 26.11.2018, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M136.pdf&Open=True>, 28.07.2020.

“Report of the Meeting Held on 13 December 2019, Note by the Secretariat, S/C/M/141”, World Trade Organization, 13.12.2019, (Çevrimiçi) <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M141.pdf&Open=True>, 29.07.2020.

“Report of the Meeting Held on 24 April 2019, Note by the Secretariat, S/C/M/138”, World Trade Organization,

24.04.2019, (Çevrimiçi)  
<https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M138.pdf&Open=True>, 29.07.2020.

“Report of the Meeting Held on 24 January 2019, Note by the Secretariat, S/C/M/137”, World Trade Organization, 24.01.2019, (Çevrimiçi)  
<https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M137.pdf&Open=True>, 29.07.2020.

“Report of the Meeting Held on 30 May 2018, Note by the Secretariat, S/C/M/135”, World Trade Organization, 11.07.2018, (Çevrimiçi)  
<https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filenam e=q:/S/C/M135.pdf&Open=True>, 29.07.2020.

**Restatement of the Law Third, the Foreign Relations Law of the United States**, C. 1, 1. bs, Washington D. C., The American Law Institute, 1986.

Riley v. California, C. 1, C. 1 U.S. Reports (U.S. Supreme Court 2014).

“Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century”, Brussels, European Commission, 25.01.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en>, 09.12.2020.

Salini Costruttori S.p.A. and Italstrade S.p.A. v. Kingdom of Morocco, Decision on Jurisdiction, ARB/00/4 (International Centre for Settlement of Investment Disputes 23 Temmuz 2001).

“Saudi Arabia”, **Encyclopedia Britannica**, 08.01.2022, (Çevrimiçi) <https://www.britannica.com/place/Saudi-Arabia>, 09.01.2022.

“Saudi Arabia Essential Cybersecurity Controls An Overview”, **Thales Security Solutions & Services**, White Paper, 8 (10.11.2020).

Schmerber v. California, 658 (U.S. Supreme Court 20 Haziran 1966).

Schrems II, C-311/18 (Avrupa Birliği Adalet Divanı 16 Temmuz 2020).

“SEDDK”, (03.11.2021), (Çevrimiçi) <https://seddk.gov.tr/>, 03.11.2021.

“Sermaye Piyasası Kurulu Bülteni”, Sermaye Piyasası Kurulu, 08.03.2018, (Çevrimiçi) <https://spk.gov.tr/Bulten/Goster?year=2018&no=10&year=2018&no=10>, 05.05.2021.

“Shaping Europe’s Digital Future - Free Flow of Non-Personal Data”, **European Commission**, (19.12.2021), (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>, 19.12.2021.

Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39171&MevzuatTur=7&MevzuatTertip=5>, 17.10.2021.

Sigortacılık ve Özel Emeklilik Sektörlerinde İç Sistemlere Dair Yönetmelik (2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=39063&MevzuatTur=7&MevzuatTertip=5>, 29.01.2022.

Smith v. Maryland, C. 442, C. 442 U.S. Reports 735 (U.S. Supreme Court 1979).

“Snowden Doc Search”, (17.05.2021), (Çevrimiçi) <https://search.edwardsnowden.com/>, 17.05.2021.

“South Korea”, **Encyclopedia Britannica**, 06.01.2022, (Çevrimiçi) <https://www.britannica.com/place/South-Korea>, 07.01.2022.

“Speech - The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens’ Rights”, **European Commission**, 2014.

“SPK”, (03.11.2021), (Çevrimiçi) <https://www.spk.gov.tr/>, 03.11.2021.

Stored Wire and Electronic Communications and Transactional Records Access Act, C. Chapter 121 §§ 2701–2712, C. Chapter 121 §§ 2701–2712 18 U.S. Code § (1986), (Çevrimiçi)

<https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>, 11.12.2020.

“Suudi Arabistan Ulusal Siber Güvenlik Otoritesi”, (27.12.2021), (Çevrimiçi) <https://www.nca.gov.sa/>, 27.12.2021.

Swiss Federal Act on Private International Law (1989), (Çevrimiçi) [https://www.fedlex.admin.ch/eli/cc/1988/1776\\_1776\\_1776/en](https://www.fedlex.admin.ch/eli/cc/1988/1776_1776_1776/en), 12.12.2021.

“TCMB”, (03.11.2021), (Çevrimiçi) <https://www.tcmb.gov.tr/>, 03.11.2021.

The Antarctic Treaty (1959), (Çevrimiçi) [https://documents.ats.aq/atcm42/ww/ATCM42\\_ww011\\_e.pdf](https://documents.ats.aq/atcm42/ww/ATCM42_ww011_e.pdf), 26.08.2020.

“The Defence Cyber Strategy”, Hollanda Savunma Bakanlığı, 2012, (Çevrimiçi) [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/Netherlands\\_2012\\_NDL-Cyber\\_StrategyEng.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf), 10.03.2021.

The Editors of Encyclopedia: “Congress of the United States”, **Encyclopedia Britannica**, 13.12.2022, (Çevrimiçi) <https://www.britannica.com/topic/Congress-of-the-United-States>, 17.07.2021.

The Editors of Encyclopedia: “Peace of Westphalia”, **Encyclopedia Britannica**, 17.10.2022, (Çevrimiçi) <https://www.britannica.com/event/Peace-of-Westphalia>, 15.11.2022.

The Foreign Corrupt Practices Act of 1977 (29.03.2021), (Çevrimiçi) <https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2012/11/14/fcpa-english.pdf>, 29.03.2021.

“The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or A Patchwork of Requirements?”, 22.06.2021, (Çevrimiçi) <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/>.

“The General Agreement on Tariffs and Trade”, World Trade Organization, 07.1986, (Çevrimiçi) [https://www.wto.org/english/docs\\_e/legal\\_e/gatt47\\_e.pdf](https://www.wto.org/english/docs_e/legal_e/gatt47_e.pdf), 12.12.2021.

“The General Agreement on Trade in Services”, World Trade Organization, 01.1995, (Çevrimiçi) [https://www.wto.org/english/docs\\_e/legal\\_e/26-gats\\_01\\_e.htm](https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm), 12.12.2021.

“The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam”, (19.08.2020), (Çevrimiçi) <https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/>, 19.08.2020.

“The Treaty on the Functioning of the European Union”, Official Journal of the European Union, 26.10.2012, (Çevrimiçi) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>, 15.08.2021.

“The United States-Mexico-Canada Agreement (USMCA)”, Congressional Research Service, 2021, (Çevrimiçi) <https://sgp.fas.org/crs/row/R44981.pdf>, 14.01.2022.

“Towards a next generation cloud for Europe | Shaping Europe’s digital future”, European Commission (10.11.2021), (Çevrimiçi) <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>, 10.11.2021.

Transcript of Oral Argument at 27:02, Smith v. Maryland, 442 U.S. 735 (1979), 1979, (Çevrimiçi) [https://apps.oyez.org/player/#/burger6/oral\\_argument\\_audio/16917](https://apps.oyez.org/player/#/burger6/oral_argument_audio/16917), 15.11.2022.

“Trans-Pacific Partnership Agreement (TPPA)”, 2015, (Çevrimiçi) <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text>, 12.12.2021.

“Transparency Report: Search Removals Under European Privacy Law”, Google (27.08.2016), (Çevrimiçi) <https://transparencyreport.google.com/eu-privacy/overview>, 27.08.2016.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967), (Çevrimiçi) <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>, 28.01.2021.

“Türkiye Bankalar Birliği Risk Merkezi”, (11.01.2022), (Çevrimiçi) <https://www.riskmerkezi.org/tr>, 11.01.2022.

“UK-Japan Comprehensive Economic Partnership Agreement”, 2020, (Çevrimiçi) <https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020>, 12.10.2021.

“Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023”, T.C. Ulaştırma ve Altyapı Bakanlığı (05.06.2022), (Çevrimiçi) <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plan-2020-2023.pdf>, 05.06.2022.

“Understanding Data Localization Laws”, **Big Bang 360**, (04.09.2020), (Çevrimiçi) <https://bigbang360.com/data-localization-laws/>, 04.09.2020.

United Nations Convention on the Law of the Sea (1982), (Çevrimiçi) [https://www.un.org/Depts/los/convention\\_agreements/convention\\_overview\\_convention.htm](https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm), 11.01.2021.

United States Bill of Rights (1791), (Çevrimiçi) <https://www.law.cornell.edu/constitution/billofrights>, 10.10.2022.

United States of America, Appellee, v. Jean Philomena Pizzarusso, 155/31392 (United States Court of Appeals, Second Circuit 1968).

United States v. Flores, 567 (U.S. Supreme Court 1937).

United States v. Graham, No. 12-4825, No. 12-4659 (United States Courts of Appeals. United States Court of Appeals (4th Circuit) 31 Mayıs 2016).

United States v. Jones, C. 565, C. 565 U.S. Reports 400 (U.S. Supreme Court 2012).



United States v. Miller, C. 425, C. 425 U.S. Reports 435 (U.S. Supreme Court 1976).

United States v. Ortiz, 422 U.S. 891 (1975) (U.S. Supreme Court 30 Haziran 1975).

United States v. Warshak, 08–3997, 08–4085, 08–4087, 08–4212, 08–4429, 09–3176 (United States Court of Appeals, Sixth Circuit 14 Aralık 2010).

United States v. White, C. 401, C. 401 U.S. Reports 745 (U.S. Supreme Court 1971).

“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”, Authenticated U.S. Government Information, 26.10.2001, (Çevrimiçi) <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>, 26.10.2021.

“Ülkemizde temsilciliği bulunan bir yabancı bankanın KVKK kapsamında veri sorumlusu sayılıp sayılmayacağı ve Veri Sorumluları Siciline kayıt yükümlülüğü hakkındaki görüş talebi ile ilgili olarak Kişisel Verileri Koruma Kurulunun 2020/471 Sayılı Kararı”, Kişisel Verileri Koruma Kurumu, 23.06.2020, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/6772/2020-471>, 10.02.2021.

Vale v. Louisiana, 727 (U.S. Supreme Court 22 Haziran 1970).

Vergi Usul Kanunu Genel Tebliği (Sıra No:509) (18.07.2021), (Çevrimiçi) <https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=33905&mevzuatTur=Tebliğ&mevzuatTertip=5>, 18.07.2021.

“Veri Sorumluları Sicili Hakkında Yönetmelik”, Kişisel Verileri Koruma Kurumu, 30.12.2017, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5442/VERI-SORUMLULARI-SICILI-HAKKINDA-YONETMELIK>, 10.02.2021.

“Veri Sorumluları Siciline Kayıt Tarihlerinin Uzatılması İle İlgili Kişisel Verileri Koruma Kurulunun 11/03/2021 Tarihli ve 2021/238 Sayılı Kararı”, **Kişisel Verilerin Korunması Kurulu**, 2021.

“Vietnam After the War”, **Asia Pacific Foundation of Canada**, (10.10.2021).

“Vietnam”, **Encyclopedia Britannica**, 26.08.2021, (Çevrimiçi) <https://www.britannica.com/place/Vietnam>, 10.09.2021.

Warden v. Hayden, 480 (U.S. Supreme Court 29 Mayıs 1967).

Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. (CJEU 01 Ekim 2015).

“What Is Gaia-X?”, (Çevrimiçi) <https://www.data-infrastructure.eu/GAIA/Navigation/EN/Home/home.html>, 17.10.2021.

“WhatsApp Uygulaması Hakkında Yürütülen Resen İncelemeye İlişkin Kamuoyu Duyurusu”, 03.09.2021, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/7045/WHATSAPP-UYGULAMASI-HAKKINDA-YURUTULEN-RESEN-INCELEMEYE-ILISKIN-KAMUOYU-DUYURUSU>, 04.11.2021.

“World Trade Organization”, (28.09.2017), (Çevrimiçi) [https://www.wto.org/english/tratop\\_e/region\\_e/regfac\\_e.htm](https://www.wto.org/english/tratop_e/region_e/regfac_e.htm), 28.09.2017.

“Yurtdışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru”, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU>, 28.05.2020.

“Yurtdışında yerleşik Tüzel kişilerin Türkiye’deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulu 2019/225 Sayılı Kararı”, Kişisel Verileri Koruma Kurumu, KVKK, 23.07.2019, (Çevrimiçi) <https://kvkk.gov.tr/Icerik/5545/2019-225>, 18.03.2020.

## ÖZGEÇMİŞ

Fatih Burak Uzun Bursa Ulubatlı Hasan Anadolu Lisesi’nde orta öğretimi tamamlamıştır. İstanbul Üniversitesi Hukuk Fakültesi’nden 2012 yılında mezun olmuş ve akabinde 2014 yılında Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Tezli Yüksek Lisans Programı’ndan mezun olmuştur. “*Milletlerarası Özel Hukukta Gerçek Kişilerin Hak ve Fiil Ehliyeti*” başlıklı yüksek lisans tezi oybirliği ile kabul edilmiştir. Yazar 2015 yılında İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Doktora Programı’na devam etmektedir.

Yazarın İstanbul Barosu Dergisi’nin Mart – Nisan 2014 sayısında yayımlanmış “*Avrupa İnsan Hakları Mahkemesi Kararları Doğrultusunda Devletin Yaşam Hakkına Müdahalesi*” adlı bir makalesi bulunmaktadır. 2015 yılında yazarın “*The Digitalization of Companies in Turkey*” başlıklı çok yazarlı makalesi Turkish Commercial Law Review adlı dergide yayımlanmıştır. Yazarın, 2017 yılında “*Gerçek Kişilerin Hak Ehliyeti ve Hak Ehliyetine Uygulanacak Hukukun Tespiti*” başlıklı makalesi Hacettepe Hukuk Fakültesi Dergisi’nde yayımlanmıştır. İlaveten yazarın, 2019 yılında “*Cloud Computing as an Investment under the ICSID Convention*” başlıklı makalesi İstanbul Üniversitesi’nin Public and Private International Law Bulletin adlı dergisinde; 2020 yılında ise “*Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri*” başlıklı çok yazarlı makalesi Prof. Dr. Türkan Rado Anısına Armağan’da yayımlamıştır.

2013 yılında avukatlık stajının tamamlayan yazar, 2014 ile 2017 yılları arasında BTS Avukatlık Ortaklığı’nda avukat olarak çalışmıştır. 2017 ve 2018 arasında Türk Ekonomi Bankası’nda hukuk müşaviri olarak çalışan yazar, 2018 ile 2021 yılları arasında Microsoft Türkiye’de hukuk müşavirliği görevini yürütmüştür. 2022 yılında ise Uzun & Keskin Hukuk Bürosu’nu kuran yazar, halen serbest avukat olarak faaliyetlerine devam etmektedir.

Yazar iyi derecede İngilizce bilmektedir. Yazar evli olup bir çocuk babasıdır.