Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr
Cilt: 2, Sayı:2
Geliş 27.05.2020
Kabul: 29.12.2020

Parçalı Bulutlar: Cloud Act ve Etkileri

Ata Umur, Kalender
Bozoğlu-İzgi Avukatlık Ortaklığı, İstanbul, Türkiye, ata.kalender@bi.legal
ORCID: https://orcid.org/0000-0002-4396-9300

ÖZ
Uluslararası teknoloji ve yazılım şirketlerinin kişisel veriler üzerinde hâkimiyeti gün geçtikçe artmaktadır. Teknoloji devi şirketler, dünyanın her bölgesinde sayıları milyarlara varan kullanıcılarının verilerini depolamak için, bulut teknolojileri kullanmak veya verileri parçalara ayırarak farklı parçaları farklı ülkelerde yer alan veri merkezlerinde saklamak gibi yeni yöntemler kullanmaktadır. Kullanılan teknolojilerin giderek karmaşık ve muğlak bir hal almasıyla birlikte, adli makamların veriye erişim ihtiyacı da artmaktadır. Bu trendlerden ötürü oluşan, açık ve modern düzenlemelere ve uluslararası araçlara duyulan gereksinim Microsoft'un dahil olduğu ve kamuoyunda büyük yankı uyandıran bir davada gözler önüne serilmiş ve kısa süre sonra yürürlüğe giren CLOUD Act adlı Kanun Amerikan mevzuatında önemli değişikliklere yol açmıştır. Bu makale, değişen teknolojilerin beraberinde getirdiği sorunları ve CLOUD Act'in etkilerini tartışmaktadır.
Anahtar Sözcükler: Bulut, Depolama, Kişisel Veri, Teknoloji, Microsoft

Partly Cloudy: the Cloud Act and Its Effects

ABSTRACT
The hegemony of international technology and software companies on personal data intensifies each day. "Big tech" companies invent and employ new methods of data storage, such as cloud technologies or data shards that allow breaking up data and storing different shards in data centers located in different countries. While the technologies used by tech giants become more complex and ambiguous, the need for judicial authorities to access data has increased as well. The need for clear and modern legislation and international tools became apparent in a case involving Microsoft that drew significant public attention, and the CLOUD Act was promulgated shortly after, introducing important changes in American laws. This article discusses the issues created by developing technologies and the impact of the CLOUD Act.
Keywords: Cloud, Storage, Personal Data, Technology, Microsoft

Atıf Gösterme Kalender, A. U. (2020). Parçalı Bulutlar: Cloud Act ve Etkileri, *Kişisel Verileri Koruma Dergisi. 2*(2), 73-106.

GİRİŞ

Teknolojinin gelişimi 21. yüzyılda giderek hızlanmaktadır. Gelişen internet teknolojileri ve bu teknolojiler kapsamında kişisel verilerin kullanımı da gün geçtikçe yaygınlaşan bir tartışma konusu hâlini almaktadır. Kişisel veriler üzerinde hâkimiyet internet kullanıcıları için önemli bir endişeye dönüşmektedir ve kullanıcılar gün geçtikçe internet ortamında bıraktıkları ayak izine dair farkındalık kazanmaktadır. Örneğin, Google veya Instagram gibi internet hizmetleri tarafından sunulan kişiselleştirilmiş reklamlara maruz kalan kullanıcılar, telefonlarının dinlenildiğinden şüphelenmektedir (Nichols, 2018). Gün geçtikçe, Facebook veya Amazon gibi teknoloji devlerinin veri ihlalleri hakkında daha fazla haberle karşılaşılmaktadır (Grundy, 2019; Brignall, 2018). Dahası, Cambridge Analytica skandalında ortaya çıktığı gibi, internet kullanıcılarının kişisel verileri internet ortamında kendilerinin haberleri olmaksızın toplanmakta, işlenmekte ve müşteri ya da seçmen olarak tercihlerini etkilemek için kullanılmaktadır (Cadwalladr ve Graham-Harrison, 2018).

Öte yandan, özel şirketlerin ve kişilerin yığınla topladığı ve ticari aktivitelerinde kullanmaya elverişli bir cephaneye çevirdiği verilerin önemi artık devletler için de ortadadır. Gün geçtikçe kişisel verilerin yasal kullanımına ilişkin yasalar, yönetmelikler ve uluslararası anlaşmaların sayısı artmaktadır. Yazılım şirketleri gibi, günümüzde devletler ve devlet kurumları da veri toplamaya ve işlemeye ihtiyaç duymaktadır (Beattie, 2019). Öyle ki kimileri, sıradaki soğuk savaşın kişisel veriler üzerinden verildiğini söyleyecek kadar ileri gitmektedir (Pendergast, 2018). Kişisel verilerin gizliliği hem ticari kaygılar hem de kamu güvenliği perspektifinden sıcak bir tartışma konusu olarak gündemde bulunmaktadır.

"Bulut bilişim" olarak bilinen teknolojiler ise ister bireysel kullanıcılara ister kurumsal müşterilere veri depolama, sunucu ve veri tabanlarına erişim gibi bilgi işlem hizmetlerini internet üzerinden edinme imkânı tanımaktadır. Özellikle şirketler için bu tür altyapılar için harcanan sermayeden tasarruf etme fırsatı yarattığından, bulut bilişim günümüzde hızla yaygınlaşmıştır. Bununla birlikte, bu çalışmanın ilgili kısımlarında daha detaylı olarak açıklanacağı üzere, bu "bulut" sistemlerinde tutulan verilerin dünyanın çeşitli yerlerinde bulunan veri tabanları ve veri depolama merkezlerine erişim sağlayarak saklanması ise bu verilerin adli makamlarca edinilmesini güçleştirebilmektedir.

İşte bu arka plan ışığında, "CLOUD Act" olarak kısaltılan, Türkçe adıyla "Yurtdışındaki Verilerin Yasal Kullanımı Kanunu" internet kullanıcılarının verilerine ilişkin önemli bir düzenleme olarak gündeme gelmektedir. CLOUD Act, Amerika Birleşik Devletleri'nin 45. Başkanı Donald J. Trump tarafından imzalanarak 23 Mart 2018 tarihinde yürürlüğe girmiştir ("Clarifying Lawful Overseas Use of Data Act", H.R. 4943). CLOUD Act ile elektronik ortamda bulunan verilerin gizliliğini düzenleyen ve Amerika Birleşik Devletleri veri gizliliği mevzuatının önemli bir parçası olan, 1986 tarihli Elektronik İletişimin Gizliliği Kanunu (Electronic Communications Privacy Act) İkinci Bölümü'nde yer alan Depolanan İletişimler Kanunu (Stored Communications Act) tadil edilmiştir. 1986 tarihli bu Kanunun günümüzde uygulanmasında güçlükler yaşanmaya başlanmış, gelişen teknoloji ile hukuki çerçeve arasında uyumsuzluklar ortaya çıkmıştır. Bununla birlikte CLOUD Act'in yürürlüğe girme sebebini ve özellikle de bu yasama sürecinin yürütülmesindeki aceleyi, Microsoft'un dâhil olduğu bir davayla ilişkilendirmemek mümkün değildir.

CLOUD Act, bu çalışmanın devamında ele alınacağı üzere, Amerika Birleşik Devletleri (ABD) Yüksek Mahkemesi nezdinde görülen yüksek profilli ve veri gizliliği bakımından hem ABD mevzuatı hem de diğer ülkeler için önem arz eden bir davayı konusuz bırakmıştır. Olayda, Federal Araştırma Bürosu (FBI) tarafından yürütülen bir soruşturma kapsamında Microsoft'tan bir kullanıcının e-posta yazışmaları talep edilmiştir. Microsoft bu talebe cevaben verilerin İrlanda'da bulunduğunu ve ABD ile İrlanda arasındaki adli yardım mekanizması yürütülerek İrlanda hukukuna uygun bir şekilde talep edilmedikçe İrlanda'da bulunan verilerin FBI'a açıklanmasının mümkün olmadığını öne sürmüştür.

Dava, yargı sürecinin sonunda Yüce Divan'ın önüne gelmiş, kamuoyundan oldukça ilgi toplamıştır. CLOUD Act'in hem bu olay ve benzerlerinde ortaya çıkan hukuki tartışmaları çözüme kavuşturmak hem de elektronik ortamda bulunan verilere kamu soruşturmaları kapsamında erişime ilişkin güncel ihtiyaçları karşılayamayan Amerikan mevzuatını yeniden ele almak amacı taşıdığı söylenebilir.

CLOUD Act, uluslararası alanda faaliyet gösteren Amerikan şirketlerinin kontrolü altında bulunan elektronik haberleşme kaynaklı verilerin kamu soruşturmalarında talep (celp) edilmesini düzenlemektedir. CLOUD Act, Türkiye de dâhil olmak üzere dünyanın çeşitli ülkelerinde etki uyandırması muhtemel bir düzenleme olarak görülmektedir; kaldı ki Microsoft davasında da Avrupa Komisyonu, AB Veri Koruma ve Gizlilik Akademisyenleri Topluluğu, Basın Özgürlüğü Raportörleri Komitesi, Avrupa Şirket Avukatları Derneği, Uluslararası ve Sınırötesi Hukuk Akademisyenleri Topluluğu, Fransa, Almanya, İrlanda ve Polonya'dan endüstriyel dernekler, Yeni Zelanda Veri Koruma Otoritesi ve Birleşik Krallık devleti gibi dünyanın birçok yerinden devlet kurumları, mesleki örgütler ve akademisyenlerin ABD Yüksek Mahkemesi'ne sunduğu görüşler (*amici curiae brief*) burada incelenen hukuki meselenin uluslararası doğasını sergilemektedir.

İletişim ve ticaretin gün geçtikçe küresel, uluslararası ve dijital bir hâl aldığı dünyamızda, suçların ve soruşturmaların da birden fazla ülke hukukunu ilgilendirmesi kaçınılmaz olduğundan, CLOUD Act'in temas ettiği hukuki meselelerin çeşitli diğer ülkelerde de gündeme gelmesi an meselesi olarak görülmektedir. Bu kapsamda, bir devletler topluluğu olarak Avrupa Birliği'nin ve pek tabii diğer ülkelerin de ceza soruşturmalarında yurt dışında depolanan dijital verilerin celp edilebilirliğine ilişkin, uluslararası etkiler doğurabilecek düzenlemeler getirebileceği öngörülmektedir (Davis ve Gressel, 2018).

Bu çalışma kapsamında, CLOUD Act'in yürürlüğe girmesini gerektiren gelişmeler, CLOUD Act'in getirdiği değişiklikler ve veri gizliliğine ilişkin Türkiye'de yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği'nde yürürlükte olan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR) ile CLOUD Act arasında ortaya çıkabilecek çelişkiler incelenecektir. İlk olarak, CLOUD Act'e giden yolda Amerikan mevzuatının nasıl geliştiği, okur tarafından hukuki meselenin tüm boyutlarıyla anlaşılması amacıyla ele alınacaktır.

ABD'DE ELEKTRONİK VERİLERİN GİZLİLİĞİNE DAİR İÇTİHAT VE MEVZUATIN GELİŞİMİ

Anayasa, gizlilik beklentisi, U.S. v. Miller davası ve "Üçüncü Taraf Doktrini"

Yakın dönem Amerikan hukuk tarihinde kişisel verilerin gizliliği açısından mihenk taşı olarak görülen U.S. v. Miller davasında, 1976 yılında Amerikan Federal Temyiz Mahkemesi, şahısların üçüncü kişilere isteyerek aktardığı bilgiler üzerinde bir gizlilik beklentisi (reasonable expectation of privacy) içinde olamayacaklarını hüküm altına almış ve Üçüncü Taraf Doktrini olarak anılan bu içtihat, yasal otoritelerin herhangi bir mahkeme kararı olmaksızın internet veya e-posta hizmeti sunucularının hâkimiyetinde bulunan verilere erişiminin önünü açmıştır (United States v. Miller, 425 U.S. 435, 1976).

U.S. v. Miller davasında sanık Miller, Citizens & Southern National Bank of Warner Robins ve the Bank of Byron adlı iki banka tarafından tutulan çek, mevduat makbuzu ve benzeri belgelerin soruşturmayı yürüten savcılık tarafından bir müzekkere ile bankalardan istenmesi ve soruşturma kapsamında delil olarak değerlendirilmesinin yasadışı olduğunu ve bu belgelerin yalnızca bir

mahkeme emriyle talep edilebileceğini öne sürmüştür. Sanık Miller'ın bu savunması bölge mahkemesi (District Court) tarafından reddedilmiş, banka kayıtları dosyada Miller aleyhine isnatları ispat etmek için kullanılmıştır (United States v. Miller, 425 U.S. 435, 1976).

Sonraki aşamada, Temyiz Mahkemesi (Court of Appeals) Miller'ın savunmasının haklı olduğuna hüküm getirmiş ve önceki kararı bozmuştur. Bozma kararının gerekçesinde temyiz mahkemesi, U.S. v. Boyd davasında, bir kişiye ait özel belgelerin bir soruşturmada zorla celp edilemeyeceği, böyle bir celbin vatandaşların şahsen, evlerinde, evraklarında ve eşyalarında, makul olmayan arama ve el koymalara ilişkin bir koruma getiren Anayasa'nın Dördüncü Ek Maddesi'ne aykırı olacağına dair oluşan (ve bir benzeri Türk ceza hukukunda "kişinin kendini suçlamaya zorlanamaması ilkesi" olarak görülen) içtihada atıf yapmıştır (Boyd v. United States, 116 U.S. 616, 1886).

Yüksek Mahkeme, Temyiz Mahkemesinin kararını tekrar bozmuş ve ihtilaf konusu banka kayıtlarının Miller'ın şahsi belgeleri olarak değerlendirilemeyeceğini, bunların bankaların ticari kayıtları olduğunu, herhangi bir gizli bilgi teşkil etmeyeceğini, bu sebeple Anayasa'nın Dördüncü Ek Maddesi kapsamında yer almadığını ve ilk derece mahkemesinin delilleri kullanmasının önünde bir engel olmadığını saptamıştır (United States v. Miller, 425 U.S. 435, 1976).

Yüksek Mahkeme, bu kararında, Miller'a ilişkin banka kayıtlarının "şahsi belgeler olmadığını", Boyd içtihadının aksine Miller'ın "bu belgeler üzerinde mülkiyet veya zilyetlik iddiasında olamayacağını", "bankaların kıymetli evrakların düzenlenmesinde ve bunlara ilişkin işlemlerde, konu dışı üçüncü kişiler olmadığını, aksine bu işlemlere taraf olduğunu" ve "bu belgelerin bankaların ticari kayıtları olduğunu" tespit etmiştir. Sonuç olarak, herhangi bir anayasal koruma (Dördüncü Ek Madde koruması) altında olmayan bilgi ve belgelerin savcılık müzekkeresi ile istenebileceği ve soruşturma ile kovuşturmalarda delil olarak kullanabileceği, Yüksek Mahkeme tarafından hüküm altına alınmıştır (United States v. Miller, 425 U.S. 435, 1976).

Bahsedilen bu tartışmalar ışığında oluşan "Üçüncü Taraf Doktrini", gönüllü olarak üçüncü kişilere sağlanan verilerin mahkeme kararı gerekmeksizin celp edilebilmesine imkân tanımaktadır. Bu yaklaşım, kişilerin çevrimiçi ortamlarda, bilgisayarları, telefonları ya da diğer elektronik aygıtları vasıtasıyla oluşturdukları ve paylaştıkları verilerin tümünü ceza soruşturmalarında kullanılabilir hâle getirmiştir. Zira herhangi bir çevrimiçi yazılım kullanan kişi, kaçınılmaz olarak verilerini üçüncü kişilere aktarmaktadır. Örneğin, bir mesajlaşma uygulamasını kullanarak bir arkadaşına herhangi bir mesaj gönderen kişi, bu veriyi internet hizmeti sağlayıcısıyla ya da yazılım şirketiyle paylaşmaktadır. Üçüncü Taraf Doktrininin ortaya çıktığı 1970'li yıllarda ABD'de yürürlükte olan Amerikan hukukuna göre, kişisel veriye erişimi bulunan internet hizmeti sağlayıcıları bu verileri mahkeme kararı olmaksızın yasal otoritelere, savcılıklara ve istihbarat ajanslarına aktarabilecekken, 1980'li yıllarda internetin yayılması ile bu hizmet sağlayıcıların verileri gizli tutma yükümlülükleri ve kullanıcıların gizlilik hakları önemli ölçüde artmıştır.

Depolanan İletişimler Kanunu ("Stored Communications Act")

1791 yılında yürürlüğe giren Amerikan Anayasası'nın Dördüncü Ek Maddesi, vatandaşların şahsen, evlerinde, evraklarında ve eşyalarında, makul olmayan arama ve el koymalara karşı güvende olma haklarının bulunduğunu hüküm altına almakta, fakat internet üzerinden paylaşılan verilere ilişkin bir kural getirmemektedir. 1980'li yılların ortalarında, Amerikan Kongresi, Amerikan vatandaşları ve işletmelerinin veri aktarımlarının elektronik ortama taşındığını, fakat sesli iletişim ve posta gibi iletişim metotlarının gizliliğinin Amerikan Anayasası ve mevzuatı tarafından korunmasına karşın elektronik iletişimlerin gizliliğinin herhangi bir yasal düzenleme ile korunmadığını tespit etmiştir.

Bu gerekçeye dayanarak, 1986 yılında Depolanan İletişimler Kanunu (Stored Communications Act), Elektronik İletişimin Gizliliği Kanunu'nun (Electronic Communications Privacy Act) bir parçası olarak yürürlüğe girmiştir. CLOUD Act'in tadil ettiği düzenleme, Elektronik İletişimin Gizliliği Kanunu'nun bir parçası olan Depolanan İletişimler Kanunu'dur.

1976 senesinde sonuçlanan ve Üçüncü Taraf Doktrini'ne yol açan Miller davasından 10 yıl sonra, Amerikan Kongresi, Depolanan İletişimler Kanunu'nu yürürlüğe koymuştur. Depolanan İletişimler Kanunu, Dördüncü Ek Madde ile kişilere tanınan gizlilik hakkının çevrimiçi verilere nasıl uygulanacağına dair tartışmaların yoğunlaştığı bir dönemde yürürlüğe girmiştir. Amerikan Senatosu'nun incelemeleri, Dördüncü Ek Madde hükümlerinin, kişilerin internet hizmeti sunucularına aktardığı verilere uygulanıp uygulanmayacağının belirsiz olduğu ve elektronik iletişimlerin gizliliğine dair yeterli korumaların bulunmadığı sonucuna varmıştır (Medina, 2013). Kanunun yayımlandığı tarihte elektronik iletişim günümüzde olduğu kadar yaygın olmasa da, kişilerin internet ortamında paylaştığı verilerin kaçınılmaz olarak üçüncü kişiler tarafından çevrimiçi ortamda saklandığı, üçüncü kişilere gönüllü olarak açıklandığından ötürü de içtihada göre korunmadığı, hatta mevzuatın o günkü hâliyle, mahkeme emrine ihtiyaç duyulmaksızın kolluk kuvvetleri tarafından talep edilebileceği ve delil olarak kullanılabileceği açıklığa kavuşmuştur (ABD Temsilciler Meclisi, 1986).

Bu sebeple, Depolanan İletişimler Kanunu 1986 yılında kanunlaşmıştır. Böylece, Depolanan İletişimler Kanunu ile "elektronik iletişim hizmeti sağlayıcıları" ve "uzaktan işlem hizmeti sağlayıcıları" olarak tanımlanan türden hizmet sağlayıcıların müşteri ve üyelerinin elektronik ortamda yer alan verilerinin gizliliğine ilişkin bir düzenleme getirilmiştir. Bu kanunun kapsamında, elektronik iletişim hizmeti, "*kullanıcılarına kablolu veya elektronik yollarla ileti gönderme veya alma imkânı sunan hizmetler"* olarak tanımlanmış, elektronik depolama ise *"elektronik aktarım ile gönderilen kablolu veya elektronik iletilerin geçici ve vasıta olarak depolanması"* olarak tanımlanmıştır. Uzaktan işlem hizmeti, *"elektronik iletişim hizmetleri yoluyla halka bilgisayarda depolama veya işlem hizmetleri sunmak"* olarak; elektronik iletişim sistemi ise *"kablo, radyo, elektromanyetik, fotooptik veya fotoelektronik yollarla elektronik iletilerin aktarımı ve bunların elektronik olarak depolanması için kullanılan bilgisayar imkanları ya da ilgili elektronik ekipman"* olarak tanımlanmıştır (Kerr, 2004).

Depolanan İletişimler Kanunu, internet ortamında veya elektronik ortamlarda yer alan her türlü veriyi kapsayan bütünsel bir kanun değildir. Kanun yalnızca metin içinde tanımlandığı şekliyle elektronik iletişim hizmeti sunucuları ve uzaktan işlem hizmeti sağlayıcılarının müşteri ve üyelerinin elektronik yollarla aktardığı verileri kapsamaktadır (Kerr, 2004). Aynı zamanda, ilgili elektronik iletişimin taraflarınca tutulan kayıtların talep edilmesini kapsamaz. Amerikan devlet makamları tarafından Depolanan İletişimler Kanunu altında elektronik iletişimlerin açıklanması talepleri, hizmet sağlayıcıların müşterilerine değil, bizzat hizmet sağlayıcılara iletilir (Thompson II ve Cole, 2015).

Depolanan İletişimler Kanunu ile temelde iki önemli düzenleme getirilmiştir. Bunlardan birincisi, verilerin Amerikan devleti kurumları tarafından elektronik hizmet sağlayıcıları ve uzaktan işlem hizmeti sağlayıcılarından talep edilebilmesine sınırlamalar getirilmesidir. İkinci önemli düzenleme ise, Depolanan İletişimler Kanunu'nun, hizmet sağlayıcıların verileri gönüllü olarak ifşa etmesine dair getirdiği sınırlamalardır (18 U.S. Code § 2702 (b), (c); Thompson II ve Cole, 2015).

Depolanan İletişimler Kanunu Kapsamında Gönüllü İfşa

Depolanan İletişimler Kanunu'nun 1986 yılında yasalaşmasının amaçlarından biri, yukarıda ifade edildiği gibi Üçüncü Taraf Doktrini ve Anayasa Dördüncü Ek Maddesi altında yeterli korumaya sahip olmayan kullanıcıların gizlilik haklarını güçlendirmektir. Bu kapsamda, kullanıcıların hizmet

sağlayıcılarına açıkladığı veya aktardığı verilerin üçüncü kişilere gönüllü olarak açıklanması, istisnai hâller dışında yasaklanmaktadır (Kerr, 2017).

Depolanan İletişimler Kanunu altında, hizmet sağlayıcı müşterilerinin iletişimlerinin ve müşteri kayıtlarının gönüllü açıklanması için çeşitli istisnalar bulunur. İlgili düzenleme yalnızca kamuya hizmet sunan elektronik iletişim hizmeti sağlayıcıları ve uzaktan işlem hizmeti sağlayıcıları için uygulanır; kamuya hizmet sağlamayan şirketler bu düzenleme kapsamında herhangi bir kısıtlamaya tabi değildir ve Depolanan İletişim Kanunu'nu ihlal etmeksizin kullanıcılarının verilerini açıklayabilirler. Hatta kamuya hizmet sunan sağlayıcılar da içerik-dışı (*non-content*) verileri (örneğin müşterilerinin sunulan hizmetleri ne biçimde kullandığı gibi) üçüncü kişilere sınırlama olmadan açıklayabilirler.

Fakat Microsoft, Google gibi kamuya hizmet sunan sağlayıcılar istisnai hâller dışında hizmetlere dair içerik verilerini açıklayamaz, içerik-dışı verileri devlet kurumlarına ifşa edemezler. Kamuya hizmet sunan sağlayıcılar tarafından devlet kurumuna yapılacak gönüllü ifşalar ilgili kişinin rızası olmadıkça, yalnızca (a) içeriğin hizmet sağlayıcı tarafından yanlışlıkla ele geçirildiği ve bir suça ilişkin olduğu görüldüğü hâllerde, (b) iyi niyetle bir kişinin ölüm veya ciddi fiziksel zarara maruz kalabileceği bir acil durum iletişimin gecikme olmaksızın ifşasını gerektirdiğinde ve (c) çocuklara ilişkin kimi suçlarda yapılabilir (18 U.S. Code § 2702 (b)).

Depolanan İletişimler Kanunu Kapsamında Zorunlu İfşa

Depolanan İletişimler Kanunu, devlet kurumları tarafından çeşitli iletişimlerin celp edilmesi için standartlar düzenlemektedir. Zorunlu ifşaya ilişkin düzenlemeler, hem içeriklerin hem de içerik-dışı verilerin (bağlantı kayıtları gibi) açıklanmasını kapsar. Bununla birlikte "temel kullanıcı bilgileri" olarak anılan ve daha az gizli nitelikteki kimi içerik-dışı veriler (isim, adres, hizmet süresi, telefon numarası, ödeme yöntemleri gibi) basit bir celp ile edinilebildiğinden aşağıdaki süreçlere konu olmamaktadır.

Elektronik iletişim hizmeti sağlayıcılarının 180 gün veya daha uzun bir süre ile depoladığı elektronik iletişimler veya uzaktan işlem hizmeti sağlayıcılarının depoladığı iletişimler üç farklı şekilde celp edilebilmektedir. 180 günden daha kısa bir süre ile depolanan, yani daha güncel iletiler ise sadece en ağır usul takip edilerek celp edilmektedir (Kerr, 2004).

Depolanan İletişimler Kanunu kapsamında elektronik iletişimler Federal Ceza Muhakemesi Kurallarına uygun olmak koşuluyla, üç farklı usul ile celp edilebilir. Bunlar, "arama kararı" (search warrant), "mahkeme celbi" (subpoena) ya da "mahkeme kararları" (court order – 2703(d) mahkeme emri olarak da bilinir) olarak adlandırılır. Arama kararı, bu sayılanlar arasında en ağır prosedürel gerekliliklere sahip olan usuldür (Kerr, 2004). Depolanan İletişimler Kanunu kapsamında Microsoft davasında uygulanan prosedür ve bunun etrafındaki tartışmalar için fikir vermek adına bu usuller, çalışma kapsamında kısaca açıklanacaktır.

Arama kararı, mahkeme celbi ve mahkeme kararları, farklı bilgileri kapsamakla birlikte, farklı hukuki şartlara tabidir. Mahkeme celbi (subpoena) en hafif gereksinimlere sahiptir ve kullanıcı bilgileri gibi gizlilik düzeyi düşük bilgiler için celplerin kullanımı yeterlidir. Mahkeme celbi, yalnızca temel kullanıcı bilgilerinin talep edildiği hâllerde kullanıcıya tebligatta bulunulmasını gerektirmemektedir. Temel kullanıcı bilgileri kapsamında, hizmet sağlayıcıların müşterilerine ilişkin isim, adres, telefon bağlantısı kayıtları, hizmet tarihçesi, telefon numarası veya diğer müşteri numaraları ve hizmet için yapılan ödemelere ilişkin bilgiler (kredi kartı veya banka hesap bilgileri dâhil olmak üzere) yer almaktadır (Kerr, 2004). Mahkeme celpleri yanında kullanıcıya bu verilerin hizmet sağlayıcıdan talep edildiğine ilişkin tebliğde bulunulursa, açılmış e-postalar, kalıcı olarak depolanan dosyalar veya

kullanıcının erişim sağlamadığı (açmadığı) ve 180 günden fazla süreyle tutulan e-postalar gibi bilgiler edinilebilmektedir (Kerr, 2004).

2703(d) mahkeme kararı olarak bilinen mahkeme kararları tüm içerik-dışı bilgilerin (kullanıcı bilgileri, içerik olmayan kayıtlar, erişim bilgileri gibi) celp edilmesini sağlamaktadır. İlgili kullanıcıya bu karara ilişkin önceden bildirimde bulunulursa, içerik-dışı bilgilerin yanı sıra açılmış e-postalar, kalıcı olarak depolanan dosyalar veya 180 günden uzun süre tutulan, açılmamış e-postaların da hizmet sağlayıcıdan talep edilebilmesi mümkündür. Mahkeme kararları celp edilen bilginin bir ceza soruşturmasıyla ilgili ve soruşturma için önemli olduğuna dair makul bir inanç oluşmasına yol açacak spesifik ve kolayca anlaşılabilir gerekçeler bulunmasını gerektirir (Kerr, 2004). Bu gerekçeler gösterilirse hâkim gerekli kararı verecek ve karar soruşturma kapsamında hizmet sağlayıcıya iletilecektir (18 U.S. Code § 2703(d)).

Depolanan İletişimler Kanunu kapsamında, 180 günden kısa süreyle tutulan ve henüz kullanıcı tarafından erişilmemiş e-postalar en yüksek korumaya tabidir. Bunlar, yalnızca arama kararları ile edinilebilir; zira arama kararları bir hesapla ilgili tüm bilgileri kapsar. Arama kararı makul şüphe (probable cause) standardının karşılanmasını gerektirmektedir. Doktrinde arama kararlarının en sıkı usule tabi olduğu, fakat buna karşılık hizmet kullanıcının tüm e-postalarına erişim sağladığı ve bu sebeple diğer iki usulden kapsamlı olduğu belirtilmektedir (Kerr, 2004).

Microsoft davasında kullanılan prosedür *"SCA Warrant"* olarak da bilinen arama kararı usulüdür. Bu usul, en yüksek korumaya sahip e-postaları ve hesaba ilişkin tüm bilgileri kapsamaktadır. Microsoft davasında tartışılan husus ise böyle bir karar ile yurt dışında depolanan verilerin talep edilip edilemeyeceğidir.

Depolanan İletişimler Kanunu'nun Yurt Dışına Uygulanabilirliği ve Microsoft Davası

Microsoft Davası: Sulh Hâkimliğinin Arama Kararı

Depolanan İletişimler Kanunu, 1986 yılında daha e-posta yeni yaygınlaşmaya başlarken çıkmış bir kanun olmasına ve o zamandan bugüne teknolojinin hızla değişmesine karşın, mahkemelerin güncel vakaları ve teknolojileri yasanın ruhuna uygun olarak yorumlaması sayesinde günümüzde internet hizmeti kullanıcılarının gizlilik haklarını korumaya halen, kısmen de olsa, elverişli olmaktadır (Medina, 2013).

Depolanan İletişimler Kanunu zamanının ötesine geçebilmiş olsa da, geçtiğimiz senelerde meydana gelen bir uyuşmazlık Kanunun sınırlarını ortaya koymuştur. Veri depolamanın küresel olarak şekil değiştirmesi ve bulut sistemlerine taşınması (İngilizce'de ifade edildiği şekilde *"de-territorialization of data"*), çeşitli ülkelerin veri koruma yasalarıyla birlikte yargı kurumlarının verilere erişimi yönünden önemli engeller doğurmuştur (Schultheis, 2015). Bu husus özellikle Microsoft ve Amerikan devleti arasındaki davada gözle görülür hâle gelmiştir.

Microsoft davasının ilk aşamasında, New York Güney Bölgesi'nde bir sulh hâkiminin (*Magistrate Judge James C. Francis IV*) federal savcıların talebi üzerine 4 Aralık 2013 tarihinde verdiği bir arama kararı ile, Microsoft'un bir kullanıcısına ilişkin birtakım bilgileri, mevcut bir uyuşturucu ticareti soruşturması kapsamında iki hafta içinde tevdi talep edilmiştir (In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp.3d 466 SDNY, 2014).

Depolanan İletişimler Kanunu kapsamında bu çalışmanın önceki kısmında tarif edilen türden bir arama kararı ile zorunlu ifşada bulunması emredilen Microsoft ise bu talebe itirazda bulunmuştur.

Microsoft, itirazının gerekçesinde ilgili bilgilerin İrlanda'da bulunan veri merkezlerinde saklandığını ve İrlanda hukuku uyarınca bu bilgilerin açıklanmasının İrlanda mahkemelerinin kararlarına bağlı olarak mümkün olabileceğini, bu kapsamda ABD ve İrlanda arasındaki Karşılıklı Adli Yardım Anlaşması (*Mutual Legal Assistance Treaty* veya *MLAT*) kapsamında öngörülen mekanizmaların yürütülmesi gerektiği ve arama kararının hukuka uygun olmadığını belirtmiştir. Microsoft hukuk müşaviri Brad Smith, arama kararının ve içerdiği talebin, "Microsoft'a binadan binaya zıplaması, ülkeden ülkeye gezmesi ve Microsoft veri merkezlerini araması, devletin istediği bilgiyi bulması ve teslim etmesi anlamına geldiğini" ve "21. yüzyılda hayal edilebilecek en geniş kapsamlı talep olduğunu" ifade etmiştir (Nakashima, 2014).

New York Güney Bölgesi Sulh Hâkimi Francis'in Microsoft tarafından İrlanda'da yer alan verileri açıklamasına karar verdiği, Depolanan İletişimler Kanunu'na dayanan arama kararında,

- Belirtilen kullanıcının hesabında tutulan, gönderilenler dâhil e-postaların tümünün içerikleri,
- Hesabın kullanıcısının kimliğinin tespit edilmesi için gerekti tüm kayıtlar veya diğer bilgiler,
- Adres defterleri, kişi listeleri, fotoğraflar ve dosyalar dâhil olmak üzere, hesapta tutulan tüm kayıt ve bilgiler ve
- Kullanıcı ile Microsoft Network arasındaki iletişimlere dair tüm kayıtların açıklanması emredilmiştir (Schultheis, 2015).

Microsoft Davası: Sulh Hâkimliği ile Bölge Mahkemesinin Ret Kararları

Microsoft, arama kararına konu verilerin Amerika'da bulunan kısmını teslim etmiş, fakat verilerin başka bir kısmının İrlanda'daki sunucularda tutulduğunu ve Depolanan İletişimler Kanunu'nun yurt dışına uygulanabilir nitelikte olmadığını, dolayısıyla mahkeme kararının uygulanamayacağını öne sürerek kararın ortadan kaldırılması adına itirazda (*motion to quash*) bulunmuştur (Cleary Gottlieb, 2018).

New York Güney Bölgesi Mahkemesi Sulh Hâkimi Francis, 25 Nisan 2014 tarihli Kararında Microsoft'un itirazını reddetmiştir. Hâkim Francis, Depolanan İletişimler Kanunu kapsamındaki arama kararının "karma" (*hybrid*) nitelikte olduğunu, yarı arama kararı, yarı mahkeme celbi niteliği taşıdığını, bu sebeple geleneksel arama kararlarının tabi olduğu koşullar ile bağlı olmadığını, Depolanan İletişimler Kanunu zorunlu ifşa hükümlerine uygun olduğunu ve ceza muhakemesi kurallarına uyulduğunu" öne sürmüştür (Harvard Law Review, 2019). Buna ek olarak, hâkim Francis, kararın karma doğasının "internet hizmet sağlayıcısına iletilen bir mahkeme celbi niteliğinde olduğunu, kamu görevlilerinin hizmet sağlayıcılarının tesislerine girerek sunucularını araması ve ilgili e-postalara el koyması gibi bir durum bulunmadığını, bu e-postalara herhangi bir bilgisayar sayesinde herhangi bir yerde uzaktan erişim sağlanabileceğini ve kararın belgelerin konumuna bakılmaksızın uygulanacağını" belirtmiştir (Schultheis, 2015).

Hâkim Francis, itirazı reddederken Depolanan İletişimler Kanunu'nun yurt dışına uygulanabilir olup olmadığını tespit etmek adına çeşitli değerlendirmelerde bulunmuştur. Öncelikle ilgili Kanuna dair yasama geçmişini incelemiş ve 1986 tarihli bir Temsilciler Meclisi raporunun "depolanan iletişimlere erişim araçlarının yalnızca ABD toprakları dâhilinde erişime yönelik olduğuna" dair ifadelerini tespit etmiştir (ABD Temsilciler Meclisi, 1986). Daha sonra 2001 yılında ilgili Kanunda yapılan değişikliklere ilişkin bir raporda, verilerin depolandığı değil, hizmet sağlayıcının bulunduğu konumun dikkate alınacağına dair açıklamalarını dikkate alarak, Microsoft'un itirazlarının aksine, federal savcıların talep ettiği arama kararında Depolanan İletişimler Kanunu'na bir aykırılık bulunmadığına karar vermiştir (ABD Temsilciler Meclisi, 2001) (In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp.3d 466 SDNY, 2014).

Sulh Hâkimi Francis, ayrıca Depolanan İletişimler Kanunu kapsamında mahkeme celplerinin çeşitli sebeplerden ötürü yurt içinde yer alan verilere mahsus tutulamayacağını öne sürmüştür. Öncelikle, hizmet sağlayıcıların üyelerinin kaydolurken adreslerini başka ülkeler olarak gösterebileceğine, sağlayıcılar tarafından kullanıcı adresleri teyit edilmezse talep edilen bilgilerin kolluk kuvvetlerinin erişimi dışında kalabileceğine işaret etmiştir. İkincisi, yurt dışındaki verilere erişilemeyeceği yönünde bir yorum sonucunda, Depolanan İletişimler Kanunu kapsamında alınamayan bilgilerin ancak Adli Yardım Anlaşmaları kapsamında edinilebileceğini ve bu prosedürün yalnızca 60 kadar ülke için mümkün olacağından yargı makamlarının diğer ülkelerdeki bilgilere erişimini engelleyebileceğini belirtmiştir. Ayrıca, Hâkim Francis Microsoft'un Kanunların yurt dışına uygulanabilmesinin yalnızca Kanunda açıkça belirtildiği hâllerde ve istisnai olarak mümkün olabileceğine dair *Morrison v. National Australian Bank (2010)* dosyasında oluşan *Morrison* içtihadına dayanan savunmasını reddetmiş; bunun yerine arama kararına "uyrukluk ilkesinin" uygulanacağını ve Amerikan hukukuna tabi bir kişinin yurt dışında olsa dahi Amerikan hukukuna tabi olacağına karar vermiştir (Harvard Law Review, 2019).

Tartışmalar sonucunda, Microsoft'un iddiaları ilk derece mahkemesi tarafından kabul görmemiş ve Microsoft Federal Mahkeme'ye başvurmuş, fakat ABD New York Güney Bölge Mahkemesi Hâkimi Loretta A. Preska Microsoft'un itirazlarını 31 Temmuz 2014 tarihinde bir kez daha reddetmiştir (Schultheis, 2015) (In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp.3d 466 SDNY, 2014).

Bölge Hâkimi Preska, "uyuşmazlığın bir konum meselesi değil, kontrol meselesi olduğunu" ifade etmiştir. Bu kararda Hâkim Preska, 1984 senesinde ABD Temyiz Mahkemesi 11. Dairesi tarafından Bank of Nova Scotia davasında oluşturulmuş olan içtihada atıf yapmış ve bu davada belirlendiği üzere ABD yetkisine tabi bir şirketin ABD dışında depoladığı, bu şirketin hâkimiyeti, emaneti veya kontrolü dâhilinde bulunan bir bilgiyi mahkeme kararı üzerine sunmakla yükümlü olduğunu vurgulamıştır (In Re Grand Jury Proceedings the Bank of Nova Scotia United States of America, Plaintiff-appellee, v. the Bank of Nova Scotia, Defendant-appellant, 740 F.2d 817 (11th Cir.), 1984).

Microsoft, Nova Scotia dosyasında istenen banka kayıtları ile Microsoft'tan istenen e-posta yazışmaları arasında "bir dünya kadar" fark olduğunu, Microsoft sunucularında bulunan özel ve şahsi e-postaların bir tür "dijital kasa" içinde saklandığını ve kullanıcıların bu yazışmaların gizli tutulmasına dair bir beklentileri olduğunu ifade etmiştir. ABD'yi temsil eden Bölge Başsavcı Yardımcısı Serrin Andrew Turner ise "Microsoft'un deliller üzerinde kontrolü var ve önemli olan bu" şeklinde bir beyanda bulunmuştur (Schultheis, 2015).

Benzer şekilde Microsoft'un Depolanan İletişimler Kanunu'nun İrlanda hükümetinin rızası olmaksızın sınır dışı uygulanmasının uluslararası hukuku ihlal edeceği yönündeki iddialarına karşı, Amerikan devleti e-postaların İrlanda'da saklanmasına rağmen Microsoft tarafından ABD sınırları içinden erişilebilir olmasının herhangi bir sınır dışı uygulamaya yol açmayacağı yönünde savunmada bulunmuştur ve Bölge Hâkimi Preska 31 Temmuz 2014 tarihli Kararında bu itirazı kabul etmiştir. Eninde sonunda Bölge Hâkimi uyuşmazlığın konum değil, kontrolle ilgili olduğuna ve Depolanan İletişimler Kanunu kapsamındaki arama kararının, ABD yetkisi altında ve sınırları içinde bulunan bir şirketten, ABD sınırları içinde erişebileceği verilerin talep edilmesinde hukuka aykırılık bulunmadığına karar vermiştir (Schultheis, 2015).

Microsoft Davası: Microsoft Lehine Temyiz Kararı, Yeniden Yargılamanın Reddi

Sulh Hâkimi Francis ve Bölge Hâkimi Preska'nın kararlarını takiben, giderek uzayan yasal sürecin sonraki adımı olarak Microsoft, temyize gitmiştir. Microsoft, en azından temyiz seviyesinde bir değerlendirme olmaksızın arama kararında talep edilen bilgileri açıklamayacağını, bu sebeple

mahkemenin kararını yerine getirmemekten ötürü hükmedilecek tazyik yaptırımlarına (*civil contempt*) katlanacağını açıklamış, peşinden temyiz başvurusunda bulunmuştur (Schultheis, 2015).

Temyiz başvurusu, Temyiz Mahkemesi İkinci Dairesi nezdinde incelenmiş ve bu kez karar Microsoft'un lehine çıkmıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016). İkinci Daire Hâkimleri Gerard E. Lynch ve Susan L. Carney ile Temyiz Hâkimi Victor A. Bolden'dan oluşan bir panel tarafından verilen 14 Temmuz 2016 tarihli Kararda, Microsoft'un arama kararları ile yurt dışında yer alan verilerin talep edilemeyeceği savunmasına karşı, Amerikan devletinin Depolanan İletişimler Kanunu kapsamındaki arama kararlarının karma bir yapıya sahip olduğu ve bu karar kapsamında istenen belgelerin nerede olduğuna bakılmaksızın teslim edilmesini gerektirdiği yönündeki iddiaları değerlendirmiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016).

Temyiz kararı kapsamında, Microsoft'un ve Amerikan hükümetinin ilgili arama kararının doğasına dair bir uyuşmazlık hâlinde oldukları saptanmıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016). Microsoft, kararın yasal olarak tanımlandığı üzere bir arama kararı niteliğine sahip olduğu ve yurt dışında bulunan verilere uygulanamayacağını savunmaktadır. Bununla birlikte, Microsoft arama kararını ABD sınırları içinde depolanan içerik-dışı verilerini sunmak yoluyla kısmen yerine getirmiştir. Buna karşın, ABD hükümeti arama kararının niteliğinin "zorunlu ifşa" hükümlerinin uygulanmasına yol açtığını, kullanılan enstrümanın adı veya niteliğinin ya da bu verilerin nerede depolandığının önem taşımadığını, istenen verilerin kararı tebliğ alan ve açıklama yükümlülüğü altında bulunan Microsoft'un hâkimiyeti ve erişiminde bulunmasının dikkate alınması gerektiğini savunmaktadır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 5).

Temyiz Mahkemesi ayrıca, Depolanan İletişimler Kanunu kapsamında, bu çalışmada da açıklanan arama kararı, mahkeme celbi ve mahkeme kararı olarak adlandırılan hukuki yolların yalnızca Federal Ceza Muhakemesi Kuralları'na tabi olarak uygulanabileceğini tekrar etmektedir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 18). Bu kapsamda, Federal Ceza Muhakemesi Kuralları'nın 41. maddesinin federal arama kararlarını düzenlediği, 41(b)(5) bendinin ise arama kararlarının yalnızca ABD sınırları içinde, hâkimiyeti dâhilinde veya ABD'ye bağlı bölgelerde ya da ABD'nin yurt dışındaki diplomatik ya da elçilik kurumlarında uygulanabileceğini hükme bağladığı belirtilmektedir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 19).

Buna ek olarak, arama kararları ile yurt dışında yer alan verilerin talep edilebileceği şeklinde bir yorumun, aksi açık bir şekilde ifade edilmedikçe Kanunların yurt dışına uygulanamayacağının varsayılması gerektiğine dair *Morrison* içtihadına aykırı olacağı tespit edilmiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 6). *Morrison* içtihadına göre, eğer kanunun lafzı, yasa koyucunun kanunun Amerikan sınırları dışında uygulanacağına dair niyetini açık biçimde içermiyorsa, kanunun yurt dışına uygulanamayacağı varsayılır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 22).

Temyiz Mahkemesi, 1986'da Depolanan İletişimler Kanunu'nun yürürlüğe girmesinde Kongre'nin amacının, gelişmekte olan teknoloji bağlamında kullanıcıların gizliliğini korumak olduğunu dikkate almıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 36). Ayrıca, düzenleme kapsamında sınır ötesi uygulamaya dair açık veya örtülü bir hüküm bulunmadığını saptamıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 23).

Bu gerekçelere istinaden Temyiz Mahkemesi tarafından 14 Temmuz 2016 tarihinde Microsoft'un savunmalarının yerinde olduğu, arama kararının icra edilemeyeceği saptanmıştır. Microsoft'un yurt içinde tutulan verileri teslim etmesinden hareketle yurt dışında yer alan verilere ilişkin olarak Bölge Mahkemesi kararının bozulması, Microsoft aleyhindeki tazyik yaptırımlarının iptali ve arama

kararının kaldırılmasına dair talimatların Bölge Mahkemesi'ne iletilmesine karar vermiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 43).

Bu lehe kararı takiben, Microsoft Hukuk Müşaviri Brad Smith, bu kararın dijital gizlilik hakları bakımından bir zafer olduğunu, Microsoft'un savunmalarında da belirtildiği gibi ABD dışındaki ülkelerde ABD hükümetinin sınır ötesi erişimi korkusu bulunduğunu ve bulut hizmetlerinin kimi ülkelerde özellikle de kamu sektörü tarafından benimsenmesinin yavaşladığını ifade etmiştir (Wingfield ve Kang, 2016).

Kararın ardından Amerikan devleti, daha önce yukarıda belirtilen üç hâkim tarafından oluşturulmuş bir panel ile görülen yargılamanın, bu kez Temyiz Mahkemesinin tüm hâkimleri nezdinde duruşmalı olarak tekrar edilmesi (*en banc rehearing*) için talepte bulunmuştur. Bu talep, 24 Ocak 2017 tarihinde 4'e 4 oyla Temyiz Mahkemesi hâkimleri tarafından reddedilmiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017).

Ret kararından yana görüş veren hâkimlerden Susan L. Carney'nin görüşünde, mahkemenin devletin taleplerinin ciddiyetinin bilincinde olduğu, fakat uygulanacak kanunun Depolanan İletişimler Kanunu olduğu ve mahkemenin de her ne kadar günümüzde yetersiz kalsa da bu kanunu uyguladığı, Depolanan İletişimler Kanunu'nun yurt dışına (sınır ötesi) uygulamaya yönelik bir maksat taşımadığının taraflarca kabul gördüğü ve *Morrison* içtihadında ifade edildiği üzere yurt dışına uygulama açıkça belirtilmedikçe böyle bir uygulamanın yasal olarak mümkün olmadığının varsayılacağı açıklanmıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 2).

Ayrıca, ilk karara itirazların genel itibariyle Microsoft'un bir Amerikan şirketi olması ve verilere ABD sınırları içinde erişebileceğinden ötürü Depolanan İletişimler Kanunu'nun yurt dışında uygulanmasının söz konusu olmayacağı hususunda odaklandığı tespit edilmiş, fakat bu pozisyonun mahkemece kabul edilmediği ifade edilmiştir. Gerekçe olarak, böyle bir uygulama altında, verilerin İrlanda'da depolanması, bir İrlanda vatandaşına ait olması, ifşanın İrlanda hukukuna aykırı olması ve ABD otoritelerinin verileri mevcut Karşılıklı Adli Yardım Anlaşması altında talep edebileceği göz önüne alınarak, yurt dışı etkinin bulunduğunun reddedilemeyeceği savunulmaktadır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 9).

Dahası, her ne kadar verilere ABD sınırları içinde erişim sağlanabilse ve hatta bu erişim yıldırım hızında bile olsa, verilerin yine de İrlanda'da depolama yapılan bir tesisten çağırılacağının altı çizilmektedir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 10). Son olarak, her ne kadar yeni bir yasal düzenleme farklı hususları dikkate alacak olsa da, *Morrison* içtihadı ve günümüzde yetersiz görülen Depolanan İletişimler Kanunu altında yorum imkanlarının, mahkemenin vardığı Microsoft lehine karara yol açtığı, yeniden duruşmalı bir yargılama yapılsa da mahkemenin önünde aynı yasal düzenleme ve aynı yorum imkanlarının bulunacağı belirtilmiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 14).

Depolanan İletişimler Kanunu'nun artık çağın gerisinde kaldığı yönündeki eleştiriler, hem Temyiz Mahkemesinin her iki kararında, hem de bu kararlara ilişkin muhalefet şerhlerinde (dissent) vurgulanmıştır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 2 ve Microsoft v. United States, No. 14-2985 - 2nd Cir., 2017, s. 13).

Temyiz Mahkemesinin orijinal kararında Mahkeme, bundan 30 sene önce uluslararası sınırların, günümüzdeki hizmet sağlayıcılarının hizmetlerini hızla sunabilmek için yaptığı gibi, sıklıkla aşılmadığını ifade etmiştir (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 6). Temyiz Mahkemesi ilk kararı, bu çalışmanın önceki kısımlarında açıklanmaya çalışılan "elektronik iletişim hizmeti sağlayıcıları" ve "uzaktan işlem hizmeti sağlayıcıları" kavramlarının, düzenlemenin yürürlüğe

girdiği tarihte daha kolay ayırt edilebilir olduğunu belirterek düzenlemenin uygulamadaki pratik zorlukların altını çizmektedir. Dahası, bir tarihçinin araştırmalarında, 1988 yılına dek New York Times gazetesi haberlerinde "internet" kavramının yalnızca bir kez geçtiği saptanarak günümüz dünyası ve düzenlemenin yürürlüğe girdiği dönemin farkları oldukça çarpıcı biçimde ortaya konmaktadır (Microsoft v. United States, No. 14-2985 - 2nd Cir., 2016, s. 14).

Microsoft Davası: Federal Temyiz Mahkemesi Süreci ve Dünyadan Tepkiler

Temyiz Mahkemesinin Microsoft lehine karar vermesini ve dosyayı yeniden değerlendirmeyi reddetmesini takiben, ABD Adalet Bakanlığı (U.S. Department of Justice) dosyayı Yüksek Mahkeme önüne (Supreme Court of the U.S.) taşımıştır.

Böylece, New York Güney Bölgesi'nde bir sulh hâkiminin 4 Aralık 2013 tarihinde verdiği bir arama kararı ile başlayan bu sancılı ve uzun süreç, Bölge Hâkimliği ve Temyiz Mahkemesi yoluyla Yüksek Mahkeme'ye kadar çıkmıştır. 16 Ekim 2017'de Yüksek Mahkeme dosyayı yargılamayı kabul etmiştir (Writ of certiorari, ORDER LIST: 583 U.S., 17-2). Yüksek Mahkeme'nin 2018 yaz ayları itibariyle karar vermesi beklenmekte ise de, yargılamanın tamamlanıp kararın açıklanmasına fırsat kalmadan, 23 Mart 2018'de CLOUD Act yürürlüğe girmiştir. Dünyanın dört bir yanından ilgi toplayan bu yargılama sürecinin, Amerikan hukukuna etkisi CLOUD Act olarak tezahür etmiştir.

CLOUD Act'in yürürlüğe girmesini takiben, taraflar Yüksek Mahkeme'ye bu gelişmeyi ve buna müteakip Amerikan devletinin edindiği ve Microsoft'a ilettiği yeni bir arama kararını bildirmiştir. Tarafların yeni arama kararının, eski arama kararı yerine geçtiğine dair uzlaşısı üzerine Yüce Divan 17 Nisan 2018 tarihinde taraflar arasında bir ihtilaf kalmadığını saptamış ve yargılamaya geçmemiştir (United States v. Microsoft Corp., 584 U.S. ___ ,2018). Nihayetinde, Yüce Divan'ın kanaatinin hangi yönde olacağını anlamak mümkün olmamıştır.

Bununla birlikte, dava özellikle Temyiz Mahkemesi sürecinde ve Yüce Divan'da yargılamanın beklendiği süre içinde oldukça dikkat çekmiştir. Birçok çeşitli kurum, şirket ve kişi dosyaya görüşler sunmuştur. "Görüş" tabiri ile ifade edilmek istenen, "amicus curiae brief" adı altında, davaya taraf olmayan bir üçüncü kişi tarafından dava konusunu aydınlatmak adına Yüksek Mahkeme verilen dilekçelerdir. Bu görüşler arasından Yüksek Mahkeme nezdinde sunulanların bir listesine bu makalenin ekindeki tabloda yer verilmektedir.

Microsoft davasında Yüce Divan'a sunulan görüşler incelenirken, ilk bakışta hukukçular, akademisyenler, mühendisler, teknoloji şirketleri ve sektör örgütlerinden oluşan büyük bir çoğunluğun Microsoft'un yanında olduğu görülmektedir. Başka bir ifadeyle Amerikan federal savcılarının talebi üzerine Amerikan sulh hâkimlerinin vereceği arama kararlarının yurt dışında bulunan verilerin talep edilebilmesinin, görüş veren kimi tarafların yürüttükleri ticari faaliyetlerden, kimilerinin ise mesleki birikimlerinden kaynaklanan endişeleri bulunduğu anlaşılabilir. Bu görüşlerden kimilerini özetlemek, Microsoft davasındaki tartışmayı ve bunun ticari hayata etkilerini anlamak adına faydalı olabilecektir.

Microsoft Davası: ABD Devleti Lehine Görüşler

Eyaletler: Vermont eyaleti ile 30'u aşkın diğer Amerikan eyaletlerinin görüşünü inceleyince, bu eyaletlerin dava ile ilgisinin, bu eyaletlerin yasaların uygulanmasında kendi etkinliklerine dayandırıldığı görülmektedir. Böyle bir iddia elbette eyalet savcılarının faaliyetlerinde federal savcılar gibi yurt dışında tutulan verilere erişim ihtiyacı duymalarından kaynaklanmaktadır. Eyaletler, uyuşturucu ticareti, hırsızlık, cinayet, çocuk istismarı gibi suçlara ilişkin araştırma ve kovuşturma yürüttüklerini ve Microsoft, Google, Facebook gibi "günümüz toplumu ve kültürünün doğasıyla bütünleşik olan" çevrimiçi hizmetlerin de bazen bu suçları planlamak ve uygulamak için kullanıldığını

öne sürmektedir. Eyaletler, dosyada Microsoft lehine temyiz kararının, yetki alanlarındaki suçları araştırmaya ilişkin kabiliyetlerine müdahale ettiğini ve bu vasıtayla kamu güvenliğine bir tehlike teşkil ettiğini iddia etmektedir. Görüşte ayrıca davada daha önce yasaların sınır ötesi uygulanmasına dair içtihadın arama kararını engeller nitelikte bulunmadığını, olayda yurt içinde bir kolluk gücünün talebi üzerine ulusal ve yetkili bir mahkemenin, yurt içinde bir şirketten veri talep ettiğini ve dolayısıyla Depolanan İletişimler Kanunu'nun sınır ötesi uygulamasının söz konusu olmadığı ifade edilmekte; başka bir ifadeyle Hakim Preska'nın "uyuşmazlığın bir konum meselesi değil, kontrol meselesi olduğu" yönündeki yaklaşımı yeniden gündeme getirilmektedir. Buna ek olarak, özel şirketlerin (verileri "*shard*" adı verilen farklı parçalara ayırmak veya yurt dışında depolamak gibi) kararlarının kolluk güçlerinin yetki alanları içindeki suçları kovuşturmalarını engellememesi gerektiği, dahası uluslararası ilişkilerin veya yürürlüğe girmesi muhtemel mevzuatın Temyiz Mahkemesi kararının yarattığı riskleri ortadan kaldırmadığı ileri sürülmektedir (States Of Vermont Et Al., 2017).

Microsoft Davası: Tarafsız Görüşler

Tarafsız görüşlere gelince, bu görüşlerin çoğunlukla, uluslararası veya uluslar üstü topluluklar ya da başka ülkelerin hükümetlerinden geldiği görülmektedir. Bu görüşler arasında belki de en merak uyandırıcısı, verilerin depolandığı yer olan İrlanda devletinin görüşüdür.

İrlanda Devleti: İrlanda devleti temelde üç hususu ileri sürmektedir. Öncelikle, İrlanda devleti yabancı mahkemelerde görülen davalara müdahil olmasını, ulusal egemenliğini korumak adına bir gereksinim olarak kabul etmediğini açıklamaktadır. İkincisi, İrlanda, ABD de dâhil olmak üzere diğer devletlerle birlikte, suçla mücadele için gerekli iş birliğini sürdürmekte olduğunu, öyle ki İrlanda ve ABD arasında 18 Ocak 2001 tarihinde imzalanmış bir Karşılıklı Adli Yardım Anlaşması (*MLAT*) bulunduğunu, İrlanda'nın görüşüne göre bu vakada uygulanması en uygun düşecek prosedürün de bu anlaşma olacağını ifade etmektedir. Üçüncüsü, İrlanda, taraflardan hiçbirinin ileri sürmediği 2013 tarihli bir kararı gündeme getirmiştir (Walsh v National Irish Bank [2013] 1ESC 2). 2013 yılındaki bu olayda, National Irish Bank adlı bir bankanın İrlanda dışında (Birleşik Krallık sınırları dâhilinde) bulunan bir şubesindeki kimi bilgilerin İrlanda vergi otoriteleri tarafından talep edilmesinin uyuşmazlık konusu hâline geldiği, İrlanda Yüce Divanı'nın kararında ise bir ceza soruşturmasında *başka hiçbir yol bulunmuyorsa,* bir İrlanda mahkemesi tarafından *ilgili yabancı hukuk açısından herhangi bir ihlalin yerine gelip gelmeyeceğini tümüyle anladıktan sonra* yurt dışında bulunan bir İrlanda şirketinin İrlanda kurumlarına bilgi açıklamasına karar verilebileceği saptanmıştır.

İrlanda devletinin aktardığı İrlanda Yüce Divanı kararının, özellikle "verilerin edinilmesi için başka hiçbir yol bulunmaması" unsuruna yapılan vurgu bakımından, yeniden iki ülke arasındaki Karşılıklı Adli Yardım Anlaşması'nın uygulanması için bir çağrı olarak anlaşılması yanlış olmaz. Dahası, İrlanda Yüce Divanı kararı, İrlanda mahkemelerinin yurt dışında bulunan bir şirketten veri açıklaması talep edilirken "yabancı hukuk bakımından ihlal oluşturmama" kıstasının Microsoft davasında karşılanıp karşılanmadığı oldukça tartışmalıdır. Zira İrlanda bir Avrupa Birliği ("AB") üye devleti olduğundan AB'nin veri korumaya dair birincil düzenlemesi olan General Data Protection Regulation ("GDPR") uygulama alanı bulacaktır (İrlanda Devleti, 2017).

AB Komisyonu: Tam da bu noktada, AB adına görüş veren Avrupa Komisyonu'nun görüşüne değinmek uygun düşecektir. Komisyon, Microsoft davasının konusu AB sınırları dâhilinde depolanan veriler olduğundan AB Hukukunun dikkate alınmasının uygun olacağını ifade etmiş, ayrıca bu verilerin işlenmesi ve AB dışına aktarımı için GDPR kapsamında yer alan kurallara yer vermiştir. Görüşte, AB'de bulunan ve Microsoft'un AB Hukukuna tabi bir iştiraki tarafından işletilen bir veri merkezinde depolanan kişisel verilerin ABD'ye aktarımının "kişisel verilerin işlenmesi" olarak değerlendirileceği ve bu hâlde AB veri koruma kurallarının uygulanacağı belirtilmiştir. AB Komisyonu'nun görüşü, İrlanda devletinin görüşünde de belirtildiği üzere, ABD ve AB devletleri

arasında bulunan Karşılıklı Adli Yardım Anlaşmalarına atıf yapmakta ve bu alanda uluslararası iş birliğine dair bağlılığını vurgulamaktadır. Komisyon, uluslararası yükümlülükler söz konusu olduğunda, "*comity analysis*" adı verilen ve Türkçe'ye "uluslararası mücamele analizi" veya "uluslararası yetki analizi" olarak tercüme edilebilecek değerlendirmenin yapılması gerektiğini ve farklı ülkelerin hukukunun değerlendirilmesinin önemini ifade etmiş, buradan da AB'de ilgili hukukun GDPR olduğu bahsini açmıştır.

Komisyonun görüşünde ifade edildiği üzere, GDPR verilerin aktarıldığı AB-dışı ülkelerde de AB'de olduğu gibi yüksek bir koruma seviyesine tabi olduğunu temin etmek üzere yurt dışına aktarım hususunu spesifik olarak düzenlemektedir. GDPR'ın 48. maddesi, aktarımın başka hukuki gerekçelere dayandırıldığı hâllere halel getirmeksizin, yurt dışına veri aktarımını gerektiren mahkeme veya idari kurum kararlarının yalnızca bir Karşılıklı Adli Yardım Anlaşması gibi bir uluslararası anlaşmaya dayandığı hâllerde icra edilebilir olduğunu hüküm altına almaktadır. Komisyon, GDPR'ın 48. maddesi uyarınca bu gibi durumlarda yalnızca Karşılıklı Adli Yardım Anlaşmaları altında AB dışına veri aktarımının mümkün olduğunu ve yabancı mahkeme kararlarının bu kapsamda değerlendirilemeyeceğini açıklamaktadır.

Görüşte, GDPR'ın uluslararası anlaşmalar altında veri aktarımına ilişkin 48. maddesinin, aktarımın başka hukuki gerekçelere dayandırıldığı hâllere halel getirmediği ifade edilmiştir. Uluslararası anlaşmalar haricinde aktarıma izin verilen bu hâller, (1) 45. maddedeki güvenlik önlemlerine dair "yeterlilik kararı", (2) 47. maddede düzenlenen ilgili idari kurum tarafından onaylanmış "kurumsal kurallar" ve (3) 49. maddede düzenlenerek olayla ilgisi bulunabilecek istisnalar olan, AB ya da ilgili üye devlet mevzuatında tanınmış "kamu yararı" hâlleri ve ilgili kişinin haklarıyla çelişmemek kaydıyla "meşru menfaat" halleri olarak belirtilmiştir. Fakat bu hâllerin olayda bulunmadığının düşünüldüğü ifade edilmiştir. Dolayısıyla, AB Komisyonu açık bir dil ile GDPR uyarınca, bu gibi vakalarda Karşılıklı Adli Yardım Anlaşmalarının uygulanması gerektiğini belirtmiştir (Avrupa Komisyonu, 2017).

Birleşik Krallık ve Kuzey İrlanda: Farklı bir perspektiften yaklaşan Birleşik Krallık ve Kuzey İrlanda ise, günümüzde internet hizmetleri sunan şirketlerin veri depolama için kullandığı çeşitli tekniklerden bahsederek, verinin depolandığı yere dayanan bir düzenlemenin yasal makamlara yeterli erişimi sağlayamayacağını ifade etmiştir. Başka bir ifadeyle, Google, Microsoft gibi hizmet sunucuların verileri parçalara ayırıp bu parçaları aynı anda birden fazla ülkede tuttukları veya günden güne ağın ihtiyaçları doğrultusunda dünyanın farklı yerlerinde sakladıkları; bu gerekçeyle verilerin coğrafi depolama konumunun ülkelerin bu verilere erişimini belirlemesinin Birleşik Krallık görüşüne göre uygun olmadığı belirtilmiştir.

Görüşte, Birleşik Krallık'ın bu doğrultuda 2016 yılında Birleşik Krallık Soruşturma Yetkileri Kanunu'nu (*U.K. Investigatory Powers Act 2016)* kabul ettiği, bu kanunun henüz yürürlüğe girmese de yurt dışında mukim fakat Birleşik Krallık'ta hizmet sunan sunucuların Birleşik Krallık arama kararlarına istinaden kimi elektronik iletişimleri açıklama yükümlülüklerini düzenlediği aktarılmıştır. Birleşik Krallık, bunlara ek olarak, ilgili ülkede erişilebilen fakat yurt dışında depolanan verilere erişimin yurt dışı veya sınır ötesi yetki gerektirmediğini savunmuş, ayrıca Temyiz Mahkemesi kararının Birleşik Krallık ile ABD arasındaki Karşılıklı Adli Yardım Anlaşması'nı sekteye uğrattığını ifade etmiştir. Özellikle, Birleşik Krallık'ın, ülke sınırları içinde faaliyet gösteren ABD'li şirketlerden bilgi edinmek istemesi hâlinde bu iki ülke arasında mevcut Karşılıklı Adli Yardım Anlaşması kapsamında ABD kurumlarına başvurulduğu, fakat temyiz kararının bu verilerin ABD kurumları için erişilemez olduğu sonucunu doğurduğu ve anlaşmayı bu açıdan uygulanamaz hâle getirdiği belirtilmiştir (Birleşik Krallık Devleti, 2017).

E-Discovery Institute: Bir başka görüşte, sınır ötesi (özel hukuk) keşifleri üzerine çalışan uzman ve profesörlerden oluşan kâr amacı gütmeyen bir kurum olan E-Discovery Institute, görüşüne tam da Vermont ve diğer eyaletlerin iddiasının aksine, "yurt içi" arama kararlarının da sınırları aşabilecek ve devletlerin egemenliğine dair endişeler yaratabilecek bir yönü olduğunu belirterek başlamaktadır. E-Discovery Institute'un görüşüne göre, delillerin dijital olması ve ABD'den erişilebilir olması, uluslararası yetki analizinin yapılmasını gereksiz kılmamaktadır ve ayrıca Depolanan İletişim Kanunu bu mücamele analizi ve yabancı hukuk sistemlerine saygının, hukukun üstünlüğü için can alıcı olduğunu göstermektedir. Özetle, E-Discovery Institute farklı hukuk sistemleri ve ulusların egemenliğine dair değerlendirmeler yapılmaksızın verilerin mahkemece celbinin hukukun üstünlüğüne zarar vereceği görüşünü savunmaktadır. Dolayısıyla, usulen tarafsız biçimde sunulmuş olsa da bu görüşün Microsoft'un pozisyonunu destekler nitelikte olduğu söylenebilir (E-Discovery Institute, 2017).

Eski Kolluk Kuvveti, Ulusal Güvenlik ve İstihbarat Yetkilileri: Son olarak, tartışma konusuna günlük uygulamaya daha yakın bir açıdan bakacak olursak, Eski Kolluk Kuvveti, Ulusal Güvenlik ve İstihbarat Yetkilileri tarafından sunulan bir görüşte, davanın yalnızca Depolanan İletişimler Kanunu altındaki arama kararlarının yurt dışında yer alan verilerin celp edilip edilemeyeceği değil, aynı zamanda bu verilerin celp edilmesinin gerekliliğine ilişkin olduğu ifade edilmiştir. Görüşte, Depolanan İletişimler Kanunu'nun eksikliklerinin Yüce Divan tarafından bu davada giderilmesinin veya her iki yönde alınacak bir kararın uluslararası ilişkiler ve ABD dış politikası bakımından önemli sonuçlar doğuracağı, dolayısıyla Yüce Divan yerine Kongre'nin yönlendirmesinin gerekli olduğu ve Kongre'nin de bu konuda çeşitli düzenleme taslaklarını değerlendirdiği belirtilmiştir.

Eski Kolluk Kuvveti, Ulusal Güvenlik ve İstihbarat Yetkilileri ayrıca internetin "Balkanlaştırılmasının" veya başka bir deyişle parçalara ayrılmasının bir risk olduğunu ifade etmiştir. Bu "Balkanlaşma" kapsamında, Fransa ve Almanya devletlerinin ulusal bulut teknolojileri kullanarak verileri yerelleştirme girişimleri bulunduğu, Rusya Federasyonu'nun Rus vatandaşlarına ilişkin verileri işleyen operatörlerin verileri ancak Rusya'da yer alan veri tabanlarında saklayabileceği ve Çin devletinin aynı şekilde işletme verileri ve Çin vatandaşlarının kişisel verilerini depolayan "kritik bilgi altyapısı" operatörlerinin de bu verileri Çin'de yer alan veri tabanlarında tutabileceği yönündeki düzenlemeler getirdiğine değinilmiş ve bu durumun uluslararası adli yardımlaşma önünde bir engel teşkil ettiği yönünde görüş sunulmuştur (Former Law Enforcement, National Security and Intelligence Officials, 2017).

Microsoft Davası: Microsoft Lehine Görüşler

Microsoft yanındaki görüşler arasında, ABD Kongre üyeleri, GDPR'ın hazırlanmasında önemli rol oynadığı bilinen Jan Philipp Albrecht ve diğer Avrupa Parlamentosu üyeleri Sophie In 'T Veld, Viviane Reding, Birgit Sippel ve Axel Voss, Dördüncü Düzenleme Akademisyenleri, Avrupa Şirket Avukatları Derneği, Avrupa Baroları ve Hukuk Toplulukları Konseyi, Apple, Amazon, Facebook gibi şirketlerin de dâhil olduğu Teknoloji şirketleri görüşü gibi çok çeşitli perspektifler yer almaktadır.

Avrupa Parlamentosu Üyeleri: Jan Philipp Albrecht ve diğer Avrupa Parlamentosu üyeleri Sophie In 'T Veld, Viviane Reding, Birgit Sippel ve Axel Voss, veri gizliliği haklarının temel insan haklarından olduğunu ifade etmişlerdir. Görüşte, AB sınırları içinde bulunan verilerin, ilgili kişinin verileri üzerindeki hâkimiyetini korumak adına sıkı kurallara tabi olduğu ve AB Temel Haklar Bildirgesi uyarınca her bir ilgili kişinin verilerini korumaya dair haklarının temel insan haklarından olduğu belirtilmektedir. İlgili kişinin verilerini, ABD hukuku uyarınca kurulu Microsoft gibi şirketler de dâhil olmak üzere, bir hizmet sağlayıcıya açıklaması hâlinde, AB hukuku kapsamında bu kişilerin haklarının kısıtlanmadığı hatırlatılmaktadır.

Avrupa Parlamentosu üyeleri bu hassasiyetle birlikte, yasaların etkin uygulanmasının da kamu yararı maksadı içerdiğini de teslim etmektedir. Bu amaçla ABD ve AB arasında imzalanan Karşılıklı Adli Yardım Anlaşması ve ABD-AB Çerçeve Anlaşması'na işaret edilmektedir. ABD-AB Çerçeve Anlaşması kapsamında, ABD ve AB arasındaki veri paylaşımının yalnızca "yasal dayanak" bulunduğu hâlde mümkün olacağının ifade edildiğini, bu "yasal dayanağın" da her iki tarafın yasalarını kapsaması gerektiği; bu anlamda Microsoft davasında verilen ve yalnızca Amerikan hukukuna dayanan arama kararının aranan şartı taşımadığı vurgulamaktadır. Hem ABD ve AB arasında imzalanan Karşılıklı Adli Yardım Anlaşması, hem de her bir üye devlet (örneğin, İrlanda) ile ABD arasında imzalanan münferit Karşılıklı Adli Yardım Anlaşmaları kapsamında ABD ve AB hukuk sistemlerinin farklılıklarının dikkate alındığı, bu sözleşmelerin özellikle farklı yetki alanları göz önüne alınarak kişisel verilerin nasıl kullanılacağını düzenlediği vurgulanmaktadır.

Karşılıklı Adli Yardım Anlaşmalarının spesifik olarak bu tür bir davada uygulanması gerekecek mekanizmaları oluşturduğu, açık biçimde ABD adli makamlarına AB'de bulunan kişisel verilere, gerekli korumalar altında, erişim sağlayacak hükümler içerdiği, Microsoft davasındaki arama kararının ise bu anlaşmaların hükümlerinin etrafından dolaşmak anlamına geleceği, ayrıca GDPR'ı ihlal edeceği tekrar edilmiştir. Bu gerekçeyle Karşılıklı Adli Yardım Anlaşması altındaki mekanizmaların işletilmesi adına Temyiz Mahkemesi'nin ret kararının onanması talep edilmektedir (Albrecht, Veld, Reding, Sippel ve Voss, 2018).

Teknoloji Şirketleri: Amazon, Apple, Cisco, Dropbox, eBay, Facebook, HP, Mozilla, Oath, Reddit, Salesforce, SAP ve Verizon'ın aralarında bulunduğu teknoloji şirketleri de Microsoft'u destekleyen bir görüş sunmuşlardır. Bu şirketler, dava ile ilgilerini, arama motorları, e-posta hizmetleri, sosyal medya platformları, uzaktan işlem, bulut depolama ve internet altyapı hizmetleri sunmalarına ve bu hizmetlerin milyarlarca insan tarafından kullanılmasına dayandırmaktadır. Görüşte, kullanıcıların en önemli bilgilerini bu şirketlere emanet ettikleri, bu şirketlerin de bahsedilen bilgilerin hassasiyetinden ötürü sürekli olarak kullanıcı verilerini ve gizliliklerini korumak için çaba sarf ettiği belirtilmektedir. Şirketler, çeşitli sebeplerden ötürü Microsoft'un argümanına katılmakta ve arama kararının hukuka aykırı olduğunu savunmaktadır. Bu kapsamda özetle, Depolanan İletişimler Kanunu'nun zorunlu ifşa hükümlerinin yurt dışında depolanan veriler bakımından uygulanamaz olduğu, yasanın bu şekilde uygulanmasının *Morrison* içtihadına aykırı olacağı, arama kararının icra edilmesinin ABD ve diğer ülkelerin çıkarları arasında bir çatışmaya yol açacağı ve de ABD Kongresinin bu tür sınır ötesi veri vakalarda Amerikan adli makamları, yabancı devletler ve ABD'li hizmet sağlayıcılar arasındaki ihtilafları çözmek için (nihayetinde CLOUD Act'e yol açacak) girişimlerde bulunduğu ifade edilmektedir.

Görüşte dikkat çekici olan bir husus, teknoloji şirketlerinin internet teknolojileri ve kullanıcı tabanının gelişimine yaptığı vurgudur. Şirketler, günümüzde insanların evlerinin yan odasında oturan arkadaşları veya aileleriyle bile WhatsApp, iMessage uygulamaları üzerinden iletişim kurduğunu, haberleri internet üzerinden takip ettiklerini, aile fotoğraflarını telefonlarındaki uygulamaları kullanarak kaydettiklerini, kalori alımlarını telefonları ile takip ettiklerini, kâğıt haritaların yerini GPS'in aldığını, artık kullanıcılara süt almalarını akıllı buzdolaplarının söylediğini ve soğuk havalarda evlerini akıllı termostatların ısıttığını ifade etmektedir. 2015 yılındaki bir araştırma sonucunda dünyadaki yetişkinlerin üçte ikisinin interneti kullandıkları, gelişmekte olan ülkelerde bile toplumun ortalama %54'ünün interneti kullandığı ifade edilmekte, bu kullanımın yalnızca ABD ile sınırlı olmadığı ise Gmail kullanıcılarının %70'inin ve Facebook kullanıcılarının %84'ünün ABD dışında ülkelerde ikamet ettiği istatistiği ile sergilenmektedir. Şirketler, 1986'da internetin günümüzdeki gibi olmadığını, öyle ki 1991 yılına kadar internette gezinme fonksiyonunun ve web tabanlı e-mail hizmetlerinin bulunmadığını, kısıtlı depolama yapılabildiğini, hatta kullanıcılar bir e-postayı okuduklarında bu e-postanın sunucularda başka e-postalara yer açmak için silindiğini ifade etmektedir. Teknoloji şirketleri 1986 yılında internetin bu hâlinden yola çıkarak, Depolanan İletişimler

Kanunu'nun günümüz teknolojisi ve dünyası ile ilişkisini oldukça etkili biçimde sorgulamakta ve özellikle de internet gibi gelişen teknolojilere ilişkin güncel yasaların önemini ortaya koymaktadır (12 Teknoloji Şirketi, 2018).

Avrupa Baroları ve Hukuk Toplulukları Konseyi: Konsey ("*The Council of Bars and Law Societies of Europe"*), görüşünde çeşitli argümanlar getirmektedir. Konsey, Depolanan İletişimler Kanunu'nun ABD hükümeti tarafından benimsenen yorumunun dünyanın çeşitli ülkelerinde uygulanan hukuk kurallarını ihlal edecek sınır dışı aramalara müsaade edeceğini, ABD hükümetinin argümanlarının gün geçtikçe yaygınlaşan veri koruma kurallarını görmezden geldiğini, profesyonel ve hukuki gizlilik haklarını dikkate almadığı, *Morrison* içtihadını ihlal ettiğini, bu olaydaki gibi bir arama kararının "yurt içi" etkiye sahip olduğunu kabul etmenin ABD hükümetinin erişebileceği veri miktarını dramatik ölçüde genişleteceğini ve uluslararası yardımlaşmanın temelini sarsacağını, ABD'yi "dünyanın veri takas odası" yapacağını, modern bir yaklaşımın elektronik kayıtların depolandıkları konumu dikkate alacağını ifade etmektedir (The Council of Bars and Law Societies of Europe, 2018).

CLOUD ACT'İN YÜRÜRLÜĞE GİRMESİ VE DÜZENLEMELERİ

Amerikan Anayasası'nın Dördüncü Ek Maddesinin korumaları, Üçüncü Kişi Doktrini, gizlilik beklentisi kapsamında evrimleşen çevrimiçi gizlilik tartışmaları, 1986 yılında Depolanan İletişimler Kanunu altındaki düzenlemeler çerçevesine oturtulmuştur. Bu Kanun yürürlük tarihinden bu yana uygulamada çoğunlukla yeterli olsa da, günümüzde veri depolamanın teknolojik boyutu ile bir kez daha evrim geçirmesi gerekmiş, bu ihtiyaçtan ise CLOUD Act doğmuştur. CLOUD Act'e yol açan gelişmeler, Microsoft davasında vurgulanmıştır.

CLOUD Act, ABD Kongresi tarafından detaylı olarak tartışılmamış, federal harcamalara ilişkin "Consolidated Appropriations Act" adlı bir torba yasaya ayrıca bir görüşmeye konu olmaksızın eklenmiştir. Öyle ki, Kanun aynı gün içinde (6 Şubat 2018) hem Temsilciler Meclisi (H.R. 4943), hem Senato (S. 2383) tarafından onaylanarak Adalet Komitesi'ne (*Committee on the Judiciary*) iletilmiştir. 2232 sayfalık bir torba yasanın içinde yer alan CLOUD Act'in neredeyse tartışılmadan yasalaşması, eleştirilere yol açmıştır (Davis ve Gressel, 2018).

CLOUD Act'in Gerekçeleri

CLOUD Act'in "Kongre'nin saptamaları" başlıklı 102. kısmı düzenlemenin arkasındaki gerekçeleri ifade etmektedir (CLOUD Act, Sec. 102). Bu kısımda 6 farklı gerekçeye yer verilmiştir. Birinci gerekçe, iletişim hizmeti sağlayıcıları tarafından tutulan elektronik verilere zamanında erişimin kamu güvenliğini korumak ve terörizm de dâhil olmak üzere ciddi suçlarla mücadele etmede devlet çalışmalarının önemli bir bileşeni olduğunu ifade etmektedir (CLOUD Act, Sec. 102).

İkinci gerekçe, ABD devletinin suçla mücadele çabalarının, ABD yetki alanında bulunan iletişim hizmeti sağlayıcıları tarafından erişilebilen, kontrol edilen ve bu şirketlerin zilyetliğinde bulunan, fakat yurt dışında depolanan verilere erişim sağlanamadığı için aksadığı yönündeki tespittir (CLOUD Act, Sec. 102).

Düzenlemenin üçüncü gerekçesi, yabancı devletlerin de gün geçtikçe ABD'de bulunan hizmet sağlayıcılar tarafından tutulan verilere, suçla mücadele maksadıyla erişim sağlamak yönündeki artan talepleri olarak gösterilmiştir (CLOUD Act, Sec. 102).

Dördüncü gerekçe, hizmet sağlayıcıların ABD hukuku bakımından açıklanması yasaklanmış verilerin yabancı devletler tarafından talep edilmesi hâlinde çatışan hukuki yükümlülükler ile karşılaşması olarak belirtilmiştir (CLOUD Act, Sec. 102).

Beşinci gerekçe, yabancı hukuk tarafından ifşası yasaklanmış verilerin, Depolanan İletişimler Kanunu kapsamında açıklanmasının talep edilmesi hâlinde ortaya çıkan hukuki çatışmadır. Bu gerekçe, AB Komisyonu'nun Microsoft görüşünde ifade edildiği gibi GDPR uyarınca ancak Karşılıklı Adli Yardım Anlaşması altında talep edilebilecek verilerin, Amerikan mevzuatı kapsamında arama kararı ile celp edilmesi gibi durumlarda ortaya çıkabilecek çelişkileri ifade eder (CLOUD Act, Sec. 102).

Son olarak, hem ABD'nin hem de gizlilik hakları ile hukukun üstünlüğüne bağlı yabancı devletler arasında imzalanacak uluslararası anlaşmaların bu çelişki ve çatışmaları gidermek için uygun bir mekanizma olduğu belirtilmektedir (CLOUD Act, Sec. 102).

Yurt Dışında Depolanan Verilere Erişim

CLOUD Act, temelde iki yenilik getirmektedir. Microsoft davasında detaylı bir şekilde tartışıldığı ve taraflar ile mahkemelerce eninde sonunda anlaşıldığı üzere, Depolanan İletişimler Kanunu'nun yurt dışına uygulanamayacağı saptanmıştır. CLOUD Act'in birinci değişikliği de bu kanunu yurt dışında yer alan verilere uygulanabilir hâle getirmektedir. Öyle ki, CLOUD Act açıkça, verilerin yurt içinde veya yurt dışında bulunmaksızın celp edilebileceğine dair bir düzenleme getirmektedir (CLOUD Act, Sec. 103, 18 U.S. Code 119. Bölümü §2713 kısmı).

CLOUD Act'in ilk düzenlemesi *Morrison* içtihadının gerektirdiği koşulu sağlamakta ve Kanun kapsamında yurt dışında yer alan verilerin celp edilebileceğini hüküm altına almaktadır. Bununla birlikte, bir ABD mahkemesinin CLOUD Act ile değiştirilmiş Depolanan İletişimler Kanunu'na dayanarak, ABD hukukuna tabi bir hizmet sağlayıcıdan yurt dışında yer alan verileri sunması yönünde bir talebi, yine de uluslararası hukuk bakımından değerlendirilmesi gerekmektedir. Zira hizmet sağlayıcılar tarafından böyle bir talebin yerine getirilmesi KVKK ya da GDPR gibi düzenlemeleri ihlal edebilecektir.

Bu duruma karşılık, CLOUD Act Amerikan veya yabancı hizmet sağlayıcılar için bir itiraz mekanizması öngörmektedir. Bu kapsamda, şirketlerin verileri istenen kişilerin ABD kişisi olmadığı ya da ABD'de ikamet etmediğini öne sürerek itirazda bulunması mümkündür. İkinci itiraz sebebi ise, verilerin açıklanmasının, aşağıda açıklanacağı şekilde bir "kalifiye yabancı devlet" hukukunu ihlal etmek için esaslı bir risk teşkil edeceğidir. Bu sebeplere dayanan bir itiraz hâlinde mahkeme, *"comity analysis"* adı verilen ve Türkçe'ye *"uluslararası mücamele analizi"* veya *"uluslararası yetki analizi"* olarak tercüme edilebilecek değerlendirmeyi yapacak; değerlendirme kapsamında Amerikan devleti ve yabancı devletin menfaatleri, oluşabilecek cezalar, hizmet sağlayıcının ABD ile bağlantısı, verileri açıklanacak kişinin konum ve milliyeti gibi çeşitli hususları dikkate alacaktır. Mahkeme, bu analiz sonucunda bulunacak üç sonuçta itirazı kabul ederek hukuki süreci değiştirmeye veya ortadan kaldırmaya karar verebilecektir. Bu hâller, zorunlu ifşanın kalifiye yabancı devlet hukukunu ihlal etmesi, durumun tamamı değerlendirildiğinde hukuki sürecin değiştirilmesi ya da ortadan kaldırılması gerekmesi ve son olarak ilgili hizmet kullanıcısı veya müşterinin bir ABD kişisi olmaması ve ABD'de ikamet etmeyen biri olması hâlleridir (CLOUD Act, Sec. 103, 18 U.S. Code 119. Bölümü §2713 kısmı).

Uygulama Anlaşmaları ve Kalifiye Yabancı Devletler

İkinci değişiklik, ABD ile diğer devletler arasında imzalanması öngörülen ve 18 U.S. Code § 2523 kapsamında düzenlenmiş bulunan *Executive Agreement* veya Türkçe tercümesiyle "*Uygulama*

Anlaşması" kapsamında veri paylaşımı modelidir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı). Bu tür anlaşmalar kapsamında kararlaştırılan prosedürlerin, suçla mücadelenin acil doğasına yeterli gelmediği yönünde eleştirilere tabi olan Karşılıklı Adli Yardım Anlaşmaları'ndan daha kısa sürede sonuçlanması amaçlanmaktadır.

Bu anlaşmaların en önemli boyutu, herhangi bir devlet ile ABD arasında bu tür bir anlaşma yapıldıktan sonra, bu devletlerin mahkemelerinin diğer devlet sınırları içinde faaliyet gösteren şirketlere doğrudan arama kararı türünden emirler gönderebilecek yetkiye sahip olmasıdır. Daha doğrusu, Depolanan İletişimler Kanunu kapsamında bulunan şirketlerin, *Uygulama Anlaşması* adı verilen ve aşağıda değinilecek koşulları taşıyan yabancı hükümetlerin ilgili kurumları tarafından gönderilecek emirler üzerine veri açıklanmasının, gönüllü ifşayı yasaklayan hükümler arasında istisnai bir durum olarak tanımlandığı ve Depolanan İletişimler Kanunu kapsamında böyle bir açıklamanın ihlal teşkil etmeyeceği düzenlenmiştir (CLOUD Act, Sec. 104, 18 U.S. Code 119. Bölümü §2511(2) kısmı).

Bu tür anlaşmaların imzalandığı ülkeler, CLOUD Act kapsamında "*qualifying foreign governments*" veya Türkçe tercümesiyle "kalifiye yabancı devletler" statüsünü kazanacaktır ve verilere yukarıda belirtilen şekilde doğrudan devlet kurumlarının Depolanan İletişimler Kanunu kapsamında yer alan şirketlere gönderebileceği talepler yoluyla erişebilecektir. Böyle bir anlaşmayı imzalamak isteyen devletlerin, 11 farklı kıstası yerine getirmesi gerekir. Bu kıstaslar ABD Adalet Bakanı (*Attorney General*) tarafından değerlendirilecek ve ABD Dışişleri Bakanı (*Secretary of State*) tarafından onaylandığı ve gerekli uzman görüşü alındığı hâliyle kongreye sunulacaktır (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Uygulama Anlaşmalarının Kıstasları ve Hükümleri

Uygulama Anlaşması imzalayabilecek ülkeler için aranan birinci kıstas, ilgili devletin yerine getireceği veri toplama aktiviteleri ışığında, devletin ulusal hukuku ve uygulamasının gizlilik ve medeni özgürlüklere dair sağlam maddi ve usuli korumalar sağlamasıdır. Bu kıstas altında, ilgili devletin Budapeşte'de 2001 yılında imzaya açılan ve Türkiye'nin de 8 Kasım 2001 tarihinde imzalayıp 1 Ocak 2015 tarihinden itibaren yürürlüğe koyduğu Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne taraf olmasıyla başlamak üzere kimi koşullar aranmaktadır. Bunlar, ilgili devletin yeterli hukuki kurallar ile siber suçlar ve elektronik delilleri düzenlemiş olması, hukukun üstünlüğüne ve ayrımcılık yasağına bağlılık göstermesi, uygulanabilir uluslararası insan hakları yükümlülükleri ve taahhütlerine uyması ve özellikle bu kapsamda bireylerin gizlilik hakkına adaletsiz ve fuzuli müdahalelerden kaçınması, adil yargılama hakkı sağlaması, ifade, dernek ve toplantı özgürlüklerini sağlaması, haksız tutuklama ve gözaltıları yasaklaması, işkence, insanlık dışı veya küçük düşürücü muamele ve cezayı yasaklamasını da kapsar. Dahası, ilgili devletin veriye erişim sağlayacak devlet kurumlarının bu verileri nasıl toplayacağı, saklayacağı, kullanacağı ve paylaşacağı hususları da dâhil olmak üzere, bağlı olduğu kurallar ve denetiminin açık biçimde hukuken düzenlenmiş olması, ilgili devletin elektronik verileri toplama ve kullanımında hesap verilebilirlik ve şeffaflığı sağlayacak yeterli mekanizmaların bulunması ve ilgili devletin bilginin küresel olarak serbest akışı ve internetin açık, dağıtık ve bağlı doğasını desteklemek ve korumak yönünde bir taahhüt göstermesi aranmaktadır (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

İkinci kıstas, anlaşmaya konu olabilecek "ABD kişilerine" ilişkin verilerin edinilmesi, saklanması veya paylaşılmasını en aza indirecek uygun prosedürlerin benimsenmesini aramaktadır. Bu kapsamda ABD kişileri, vatandaşlar, oturma izni bulunanlar, ABD hukuku uyarınca kurulmuş şirketler veya üyelerinin önemli kısmı Amerikan vatandaşı olan adi ortaklıklar olarak tanımlanmıştır (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Üçüncü kıstas, anlaşma hükümlerinin, hizmet sunucuların verileri şifrelemek (*decryption*) adına yeterliliğe sahip olmasına veya verileri şifrelemesinin yasaklanmasına dair bir yükümlülük içermemesidir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Dördüncü kıstas ise anlaşma kapsamında veri açıklanmasına dair yabancı devletlerden gelebilecek emirleri düzenler. Bu kapsamda, ilgili yabancı devletin bir ABD kişisini ya da ABD'de mukim bir kişiyi hedeflememesi ve böyle bir hedeflemeyi engelleyecek prosedürler benimsemesi, ayrıca ABD dışında mukim olan başka ülke vatandaşı bir kişiyi de bu yasaklı kişilere ilişkin bilgi edinmek amacıyla hedeflememesi koşulu aranmaktadır. Yabancı devletin, ABD devletinin ya da bir üçüncü taraf devletin talebi üzerine veya bu devletlerle paylaşmak amacıyla veri talep etmesi, ya da talep edilen bu verileri bu devletlerle paylaşması engellenmektedir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Yabancı devletin kurumları tarafından gönderilecek emirlerin, ceza muhakemesi bakımından belirli koşulları taşıması gerekir. Öncelikle, terör suçları dâhil olmak üzere ağır suçların engellenmesi, tespiti ya da kovuşturulması amacıyla, spesifik bir kişi, hesap, adres ya da kişisel cihazı belirtmesi bir koşul olarak belirlenmiştir. Ayrıca, ilgili devletin yerel hukukuna ve hizmet sağlayıcılara ilişkin kurallara uygun olması, araştırma konusu davranışın ağırlığı, hukukiliği ve özelliğine dair ifade edilebilen ve güvenilir gerçeklere dayanan, makul bir gerekçelendirmeye sahip olması aranmaktadır. Bir başka koşulda, ilgili emrin, kullanılacağı soruşturma öncesinde veya sırasında bir mahkeme, hâkim, sulh hâkimi veya diğer bir bağımsız otorite tarafından inceleme ve denetime tabi olması aranmaktadır. Eğer ilgili emir, bir kablolu ya da elektronik iletişimin ele geçirilmesini gerektiriyorsa, bu emir sınırlı ve belirli bir süre ile yalnızca onaylanan amaçların gerektirdiği süre boyunca geçerli olması, ayrıca bu emir olmaksızın ve gizlilik haklarına daha hafif bir müdahale olmadan ele geçirilemeyecek olması hâlinde verilmesi aranmaktadır (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Anlaşmaların, yabancı devlet tarafından verilen emrin ifade özgürlüğünü kısıtlamak için kullanılamayacağını hüküm altına alması şart koşulmuştur. Yabancı devletin anlaşma kapsamında toplanan materyalleri derhal gözden geçireceği ve gözden geçirilmeyen iletişimleri yalnızca eğitimli kişilerin erişebileceği güvenli bir sistemde depolayacağı düzenlenmelidir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Anlaşma kapsamında, 50 U.S.C. 1801 kodlu Yabancı İstihbarat Gözetim Kanunu kapsamında tanımlanan şekilde minimizasyon prosedürleri aranmalıdır. Ayrıca, bu Kanuna uygun şekilde paylaşıldığı hâller ve ABD kişileri ya da ABD'ye ciddi bir zarar ya da bu yönde bir tehdidin bulunduğu ağır suçlar, terörizm, şiddet suçları, çocuk istismarı, uluslararası organize suç ya da finansal dolandırıcılık hâlleri haricinde, ilgili yabancı devletin bir ABD kişisine ilişkin iletişimleri ABD otoritelerine açıklayamayacağı düzenlenmelidir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Uygulama Anlaşması kapsamında ayrıca ilgili devletlere, ABD'ye karşılıklı veri erişimi hakları tanımaları ve gerekli hâllerde ABD yetkisine tabi sağlayıcılar da dâhil olmak üzere iletişim hizmeti sağlayıcılarına uygulanan kısıtlamaları kaldırmaları ve bu sağlayıcıların veri ifşalarına ilişkin devlet kurumlarının taleplerine riayet etmelerini sağlamaları yönünde bir yükümlülük getirileceği öngörülmüştür. Türkiye örneğinde, Türkiye Devleti ve ABD arasında imzalanacak bir *Uygulama Anlaşması'nı* takiben, KVKK'nın kişisel verilerin işlenmesi ve yurt dışına aktarılmasına dair şartlarının gözden geçirilmesi ve (Amerikan hukukuna tabi olanlar da dâhil olmak üzere) iletişim hizmeti sağlayıcılarının kişisel verileri Amerikan devlet kurumlarına aktarmasının Türk hukuku bakımından mümkün kılınması gerekecektir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

Son olarak, bu anlaşmalarda yabancı devletlerin anlaşma hükümlerine uyum bakımından periyodik olarak ABD tarafından denetim yapılmasına imkân tanımalarının aranacağı, ayrıca ABD'nin uygun bulmadığı emirlere dair, anlaşmayı uygulanamaz kılabileceği düzenlenmektedir (CLOUD Act, Sec. 105, 18 U.S. Code 119. Bölümü §2523 kısmı).

İMZALANAN İLK CLOUD ACT ANLAŞMASI

2019 yılının Ekim ayı itibariyle, CLOUD Act kapsamında ilk kez bir *Uygulama Anlaşması* imzalanmıştır. "Birleşik Krallık ve Kuzey İrlanda Devleti ve ABD Arasında Ciddi Suçlarla Mücadele Amacıyla Elektronik Verilere Erişim Hakkında Anlaşma", 3 Ekim 2019 tarihinde imzalanmıştır (U.S. Department of Justice, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, 2019). Anlaşma metni Birleşik Krallık hükümeti tarafından 7 Ekim 2019'da açıklanmıştır (United Kingdom Foreign ve Commonwealth Office, 2019).

ABD Adalet Bakanlığı; Birleşik Krallık ile imzalanan anlaşmaya ilişkin açıklamasında, bu anlaşmanın ABD ve Birleşik Krallık'ın organize uluslararası suçlar, terörizm ve çocuk istismarı gibi ciddi suçlarla mücadelede, hızla ilerleyen soruşturmalarda kullanılmak üzere verilere daha etkin erişime imkân tanıyacağı ve iki ülkenin suçla mücadele kabiliyetlerini artıracağı ifade edilmiştir. Açıklamada ancak soruşturmanın yürütüldüğü bir ülkede işlenen suça ilişkin başka ülkede bulunan elektronik verilere erişilebilirse 21. yüzyılın tehditleriyle etkin şekilde mücadelenin mümkün olacağı belirtilmiştir. Açıklamada ülkeler arasında mevcut Karşılıklı Adli Yardım Anlaşmaları kapsamında soruşturmaların aylarca uzayabildiği ifade edilmekte, bir örnek olarak internet üzerinden çocuk istismarı, şantaj, zorla çalıştırma ve uygunsuz görsellerin paylaşımı gibi çeşitli suçlar işleyen bir suçlunun ancak 8 yılın sonunda ceza aldığına değinilmektedir (U.S. Department of Justice, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, 2019) .

Anlaşmanın diğer tarafı olan Birleşik Krallık'ın anlaşmaya dair açıklayıcı notunda, benzer hususlara değinilmektedir. Öncelikle, Birleşik Krallık makamlarının ABD'de internet hizmeti sağlayan şirketlerin elinde bulunan verilere erişim sağlayabilmesinin Karşılıklı Adli Yardım Anlaşması mekanizmaları altında yıllar sürebildiği, bu sebeple günümüzde imzalanan türden bir anlaşmanın uzun zamandır beklendiği ifade edilmiştir. Açıklayıcı not, terörist ve suçluların global haberleşme hizmetleri ve sosyal medya uygulamalarını suç faaliyetlerinde artan bir hızla alet ettiklerini, bu sebeple bahsedilen uygulamalar tarafından üretilen verilerin ciddi suçların soruşturma ve kovuşturmasında can alıcı bir kaynak olduğunu belirtmektedir. Bu anlaşmayla birlikte, ABD'li internet hizmet sağlayıcılarının Birleşik Krallık emirlerine uygun biçimde veri sağlamasının önündeki hukuki engellerin kaldırılmasının soruşturma ve kovuşturmalardaki gecikme ve imkânsızlıkları azaltması hedeflenmektedir (United Kingdom Foreign ve Commonwealth Office, 2019).

Anlaşma metni incelendiğinde, özetle anlaşmanın iki ülkede mevcut mevzuat ile birlikte uygulanacak; fakat tarafların kendi hukuk sistemlerinde yapacağı değişiklikler ile bir tarafın yetki alanında ve hukukuna bağlı olarak faaliyetlerini yürüten bir internet hizmeti sağlayıcısının, diğer taraf ülkeden gönderilecek veri taleplerine, herhangi bir hukuki ihlalde bulunmaksızın riayet edebilmesi sağlanacaktır. Hizmet sağlayıcıların veri taleplerine riayet etmesi bir zorunluluk olarak getirilmeyecek ve bu taleplere karşı talepte bulunan ülkenin hukuku doğrultusunda itiraz edilebilecektir. Daha yalın bir ifadeyle, anlaşma kapsamında diğer ülkede faaliyet gösteren hizmet sağlayıcılara iletilecek emirler, bu emri yollayan ülke hukukuna göre değerlendirilecektir (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, 2019).

Anlaşma kapsamında yer alan suçlar, ciddi suçlar olarak anılan ve üst sınırı en az üç yıl hapis cezasını gerektiren suçlar olarak belirtilmiştir. Anlaşma kapsamında bilgileri talep edilebilecek kişiler ise, bir "Alıcı Taraf Kişisi (Receiving-Party Person)" haricindeki kişilerdir; alan taraf kişileri, her iki taraf için farklı bir şekilde belirlenmiş olsa da genel itibariyle emrin gönderildiği ülke sınırları içindeki devlet ve kamu kurumları, şirketler, vatandaşlar veya ilgili ülke sınırları içindeki diğer kişileri kapsamaktadır. Örneğin, Birleşik Krallık makamlarının ABD'de faaliyet gösteren bir hizmet sağlayıcıya göndereceği emir, ABD vatandaşlarını, ABD'de yasal olarak oturma izni bulunan kişileri, ABD hukuku uyarınca kurulmuş kişileri veya ABD Sınırları dâhilinde bulunan kişileri hedef alamayacaktır; fakat böyle bir emir kapsamında ABD'de bulunmayan bir Birleşik Krallık vatandaşı hakkında bilgi talep edilmesi mümkündür. İki ülkenin de, gönderecekleri emirler kapsamında "Alıcı Taraf Kişilerini" hedeflememek adına gerekli prosedürleri oluşturma yükümlülükleri bulunmaktadır (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, 2019).

Anlaşma kapsamında yer alan hizmet sağlayıcılar, kamuya bilgisayar ya da telekomünikasyon araçları vasıtasıyla iletişim veya veri depolama ya da işleme imkânları sunan özel hukuk kişilerini ve bunlar adına veri işleyen ya da depolayan kişileri tanımlamaktadır. Anlaşma kapsamında talep edilmesi mümkün veriler ise bahsedilen hizmet sağlayıcıları tarafından sahip olunan ya da kontrol edilen elektronik veya kablolu iletişim içerikleri, bir kullanıcı için depolanan ya da işlenen bilgisayar verileri, bir elektronik ya da kablolu iletişim ya da bilgisayar verisinin depolanması ya da işlenmesine dair trafik verileri ve meta datayı ve son olarak müşterilerin isim, adres, ödeme yönetimi, telefon bağlantı kayıtları gibi abonelik verileridir (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, 2019).

Böylece, her iki ülke, diğer ülke sınırları dâhilinde faaliyet gösteren ve anlaşma kapsamında yer alan hizmet sağlayıcılarına, anlaşma kapsamında yer alan kişilere ilişkin, doğrudan karşılanacak veri taleplerini (veya emirlerini) iletebilecektir. Her iki ülke adına gönderilecek talepler, gönderen ülkenin mahkemeleri veya hâkimlerinin denetimine tabi olacak ve ilgili ülkelerin belirlenen makamlarınca incelenecektir. Bu incelemeden sorumlu makamlar, ABD tarafından gönderilecek talepler için ABD Adalet Bakanlığı, Birleşik Krallık tarafından gönderilecek talepler içinse İçişlerinden Sorumlu Devlet Bakanı olacaktır. (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, 2019)

Anlaşma metni, taleplerin tabi olduğu inceleme mekanizması, talepleri alan hizmet sağlayıcıların önce talebi gönderen ülkenin yetkili makamlarına ve ardından kendi ülkesinin yetkili makamlarına itirazda bulunma imkanı tanıması, bu gibi hâllerde talebi alan ülke makamlarına veto hakkı tanıması, ayrıca ABD makamlarına ifade özgürlüğünün ihlallerine yol açabilecek taleplere ilişkin ve Birleşik Krallık makamlarına ölüm cezasına yol açabilecek delillerin kullanımına dair veto hakkı tanıması, ülkelerin anlaşma kapsamında talep edilen raporlara ilişkin senelik raporlar hazırlamasını gerektirmesi gibi taraflara güvence sağlayan çeşitli unsurlar içermektedir (Daskal & Swire, The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards, 2019).

Buna karşın, anlaşma insan hakları ihlallerine yol açabileceği, taleplerin doğrudan hizmet sağlayıcılara iletilmesinin talebin iletildiği ülke makamlarının incelemesini gerektirmediği, bu sebeple hizmet sağlayıcıların aldıkları talepleri mahremiyet ve insan hakları bakımından değerlendirmelerinin mümkün olmayabileceği, ABD makamlarının erişebileceği bilgilerin Birleşik Krallık makamlarının erişebileceği bilgilere kıyasla daha geniş tanımlandığı gibi çeşitli sebeplerle eleştirilere tabi tutulmuştur (Human Rights Watch, 2019).

Ayrıca, anlaşma metninde, bu çalışmanın ilerleyen kısımlarında açıklanacağı üzere, veri lokalizasyonu uygulamalarının, açık, serbest ve güvenli bir internetin oluşumuna zarar verdiğine de değinilmektedir.

Bunun yanı sıra, ABD ile Avustralya ve ABD ile Avrupa Birliği arasında imzalanmak üzere anlaşma müzakerelerinin sürdüğü açıklanmıştır (U.S. Department of Justice, Joint US-EU Statement on Electronic Evidence Sharing Negotiations, 2019; U.S. Department of Justice, 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, 2019).

ABD ile Avrupa Birliği arasında imzalanması söz konusu olabilecek bir *Uygulama Anlaşması'*nın, Microsoft davasında Avrupa Parlamentosu üyeleri tarafından vurgulanan, ABD-AB Çerçeve Anlaşması ve GDPR'ın 48. maddesi kapsamında veri paylaşımları için gereken yasal dayanağı oluşturması mümkün olabilecektir. Bununla birlikte, ABD ile AB arasındaki veri paylaşımı çerçevesinin bütünsel olarak değerlendirilmesi daha fazla soru işaretine yol açacaktır. Bu çerçeve, 2016 yılını takiben ABD-AB Çerçeve Anlaşması (*"Umbrella Agreement"* olarak da bilinen 10 Aralık 2016 tarihli anlaşma) ve detayları 1 Ağustos 2016 tarihli 2016/1250 sayılı AB Komisyon Uygulama Kararı ile belirlenen "Gizlilik Kalkanı" (*Privacy Shield)* anlaşması ile çizilmiştir (Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016) (Commission Implementing Decision (EU) 2016/1250, 2016).

Fakat, Avrupa Birliği Adalet Divanı'nın kamuoyunda "Schrems II" kararı olarak da bilinen kararı ile, ABD-AB arasındaki Gizlilik Kalkanı geçersiz kılınmış, bu çerçevede ticari veri paylaşımının esas dayanağı ortadan kalkmıştır (Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, 2020).

Bu gelişmeler ışığında Avrupa Komisyonu ve ABD Ticaret Bakanlığı ortak açıklamasında gelişmiş bir gizlilik kalkanı için görüşmelerin başlatıldığı belirtilmiştir (Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross, 2020). Gizlilik kalkanı aslen ticari veri paylaşımını ilgilendirse de ve ceza soruşturma ve kovuşturmalarını ilgilendiren ABD-AB Çerçeve Anlaşması geçerliliğini korusa da, "Schrems II" kararı Transatlantik işbirliğinin çerçevesine dair belirsizlik yaratmıştır. Mevcut belirsizliğin ABD ve AB üyeleri arasında CLOUD Act türü anlaşmalar için imkan sağladığı ve ABD'nin veri aktarımı alanındaki yaklaşımını yönünde yorumlar kamuoyuna yansımıştır (Goldfield ve Sonkar, 2020; Farrell ve Newman, 2020).

CLOUD ACT'İN TÜRK VERİ KORUMA HUKUKU İLE İLİŞKİSİ

Türk veri koruma mevzuatı perspektifinden değerlendirilecek olursa, Türkiye'de veri depolayan ve Türk vatandaşlarına hizmet sunan, fakat aynı zamanda Amerikan hukukuna tabi olan Microsoft, Facebook veya Google gibi internet hizmeti sağlayıcıları, Türkiye'deki veri işleme faaliyetlerinde, Türk hukukunun veri gizliliğini düzenleyen 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bu Kanuna dayanan ikincil düzenlemelere tabi bulunmaktadır. İnternet hizmeti kullanıcılarına ilişkin e-posta yazışmalarının bir ceza soruşturması kapsamında Amerikan adli makamları tarafından talep edilmesi ve bahsedilen şirketlerce verilerin ilgili adli makama teslim edilmesi, KVKK'nın 9. maddesinde düzenlenen "Kişisel verilerin yurt dışına aktarılması" faaliyetini teşkil edecektir. Dolayısıyla, yabancı bir mahkemenin delil edinmek adına bir internet hizmeti sağlayıcısına göndereceği, kişisel veri içeren e-posta yazışmalarının teslimini gerektiren bir karar eğer Türkiye'de depolanan bir veriye ilişkinse KVKK'nın kriterlerini karşılamalıdır.

KVKK uyarınca, ilgili kişinin verilerinin işlemesi ve yurt dışına aktarılmasına açık rıza vermediği hâllerde, öncelikle KVKK'nın 5. maddesinin ikinci fıkrası ile 6. maddenin üçüncü fıkrasında belirtilen şartların varlığı ve verilerin aktarılacağı yabancı ülkenin KVKK'nın 9. maddesinde belirtilen koşulları sağlaması aranmalıdır. KVKK'nın 9. maddesi, ilgili kişinin kişisel verilerinin yurt dışına aktarımına ilişkin açık rızasının bulunmadığı hâllerde, 5. maddenin ikinci fıkrası ile 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı hâlinde yurt dışına aktarım yapılabileceğini düzenlemektedir. Fakat bu şartların bulunduğu hâllerde de, kişisel verinin aktarılacağı yabancı ülkenin, KVKK'nın 9. maddesinde belirtilen koşulları sağlaması gerekliliği bakidir.

Kişisel Verilerin İşlenme Şartları Bakımından Değerlendirme

Yabancı mahkeme tarafından verilmiş bir karar ile veriler yurt dışına aktarıldığında, KVKK'nın 5. maddesinde yer alan kişisel verilerin işlenme şartlarından birinin bulunduğunun iddia edilmesi, KVKK'nın geniş bir şekilde yorumlanmasını gerektirecektir. KVKK'nın 5. maddesinin ikinci fıkrasında yer alan iki bendin böyle bir talebe dayanak oluşturabileceği ileri sürülebilir.

ABD mahkemelerinin veya devlet kurumlarının kararlarına dayanarak verilerin yurtdışına aktarılmasına dayanak teşkil edebilecek veri işleme sebeplerinden ilki, kişisel verilerin işlenmesinin "*veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi için zorunlu olması"* hâlidir. Bu şarta dayanarak veri işlendiğine dair bir iddia, yabancı mahkemelerin kararlarının veri sorumlusu/veri işleyen için "hukuki yükümlülük" olduğunun kabulünü gerektirir. KVKK, hukuki yükümlülük kavramını açıkça tanımlamamaktadır. Hukuki yükümlülük kavramı, açık olarak yalnızca Türk hukuku kapsamındaki yükümlülükler olarak sınırlandırılmamıştır, fakat aynı zamanda ifadede yabancı hukuka atıf bulunmamaktadır. Bununla birlikte, yabancı mahkeme kararlarının muhatapları adına KVKK anlamında hukuki yükümlülük olarak kabulü suretiyle verilerin yurt dışına aktarımının, kişilerin verileri üzerindeki hâkimiyetlerini azaltacağı, "hukuki yükümlülük" tanımının kapsamına dair belirsizlik yaratacağı ve KVKK'nın "*başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak*" şeklinde ifade edilen amacına aykırı olacağı düşünülmektedir. Dolayısıyla, mevcut durumda (bir *Uygulama Anlaşması*'nın yokluğunda) bir ABD mahkemesi veya devlet kurumunun kararı doğrultusunda kişisel verilerin yurtdışına aktarılmasında, KVKK kapsamında veri sorumlusunun hukuki yükümlülüklerini yerine getirmesi için bir zorunluluk olarak kabul edilemeyeceği düşünülmektedir.

CLOUD Act hükümlerine göre, ABD ile Türkiye arasında bir *Uygulama Anlaşması* imzalanması hâlinde, bu çalışmanın 3. kısmında da belirtildiği üzere, (Amerikan hukukuna tabi olanlar da dâhil olmak üzere) iletişim hizmeti sağlayıcılarının kişisel verileri Amerikan devlet kurumlarına aktarmasının Türk hukuku bakımından mümkün kılınmasına ihtiyaç duyulacaktır. Bu hâlde, KVKK'nın "*veri sorumlusunun hukuki yükümlülüğünün yerine getirmesi için zorunlu olması"* şeklindeki veri işleme şartı ile yurt dışına aktarım koşullarının, Uygulama Anlaşması kapsamında Amerikan mahkemeleri ve devlet kurumlarına bir ceza soruşturması veya kovuşturması kapsamında kişisel veri aktarımına izin verecek şekilde değiştirilmesi veya Türk otoritelerince bu şekilde yorumlanması söz konusu olabilecektir.

Aksi hâlde, kişisel verilerin yabancı mahkeme kararına istinaden yurtdışına aktarılmasının önündeki bir başka engel, CLOUD Act'in öngördüğü itiraz mekanizmaları olacaktır. İşbu çalışmanın 3. kısmında açıklandığı üzere CLOUD Act'in 2713. kısmı altında, "uluslararası yetki analizi" veya "uluslararası mücamele analizi" olarak tercüme edilebilecek "*comity analysis*" süreci ile elektronik hizmet sağlayıcıları ve uzaktan işlem hizmeti sağlayıcılarının başvurabileceği bir itiraz mekanizması öngörülmektedir. Bu başvuru, CLOUD Act kapsamında delil talebinin, Türk hukukunu ihlal ettiği

yönünde bir itiraza imkân sağlayacaktır. Eğer bir Uygulama Anlaşması'nı takiben Türk hukukunda gerekli düzenlemeler yapılmaz ise, verilerin Amerikan mahkemelerine açıklanması veri sorumlusunun hukuki yükümlülüğünü yerine getirilmesi için zorunlu olarak kabul edilmeyebilecektir. Zira CLOUD Act Türk hukukuna aykırılıklar hâlinde de veri sorumlularına bir itiraz mekanizmasını mümkün kılmaktadır. ABD mahkemelerinin veya devlet kurumlarının kararlarına dayanarak verilerin yurtdışına aktarılması hâlinde bu aktarımın dayanağı olarak ileri sürülebilecek diğer veri işleme şartı, KVKK'nın 5. maddesinin ikinci fıkrasının (f) bendinde yer alan *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* hâlidir. Söz konusu adli taleplerin karşılanmasının, veri sorumlusunun meşru menfaatleri için zorunlu olduğunu söylemek yanlış olmayacaktır. Zira mahkeme kararlarına riayet edilmemesi, birçok ülkede yüksek tutarlı para cezaları ve hatta hapis cezalarına yol açabilecektir.

Buna karşın, ilgili bentte, meşru bir menfaatin veri işlemeyi zorunlu kıldığı hâllerde bile ilgili kişinin temel hak ve özgürlüklerine zarar verilemeyeceği açıkça ifade edilmiştir. Yabancı mahkemelerin taleplerine uyularak kişisel verilerin yurt dışına aktarılması, kişinin özel hayatın gizliliği, haberleşme hürriyeti, savunma hakkı ve adil yargılanma hakkı gibi birçok temel hak ve özgürlüğüne zarar verebilecektir. Türkiye Cumhuriyeti Anayasası, özel hayatın gizliliği ve haberleşme hürriyetinin milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi gibi hâllerde usulüne göre verilmiş hâkim kararı üzerine sınırlanabileceğini düzenlese de Anayasa'nın adil yargılanma hakkını düzenleyen 36. maddesi bu tür bir sınırlamaya imkân tanımamaktadır. Dahası, yabancı mahkeme kararlarının özel hayatın gizliliği ve haberleşme hürriyetinin sınırlanması için bir gereklilik olan "usulüne göre verilmiş hâkim kararı" niteliğini taşımadığı açıktır. Zira, hâkim kararlarının tabi olacağı usuller farklı hukuk sistemlerine göre değişmektedir, hatta Amerikan hukukunda görülebileceği ve bu çalışmada ortaya konduğu üzere arama kararı veya mahkeme kararı gibi farklı karar tipleri için bile farklı şüphe gereksinimleri bulunmaktadır.

Türk mevzuatının mevcut hâli değerlendirildiğinde, kişisel verilerin bir yabancı mahkeme kararına istinaden yurt dışına aktarılması, veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi için bir zorunluluk olarak kabul edilememektedir. Aynı zamanda, verilerin bir ceza soruşturması kapsamında yurtdışına aktarılması ilgili kişinin temel hak ve özgürlüklerinin bir ihlalini teşkil edebileceğinden, KVKK'ya tabi internet hizmeti sağlayıcılarının meşru menfaatleri doğrultusunda bu şekilde veri aktarımında bulunmalarının hukuka aykırı olacağı düşünülmektedir. Bu durumun sonucu olarak, bir *Uygulama Anlaşması* bulunmaması hâlinde Türkiye'de kurulu ve Türk hukukuna tabi hizmet sağlayıcıları, kişisel verileri Amerikan mahkeme kararlarına istinaden açıklamaları hâlinde KVKK kapsamındaki yükümlülüklerini ihlal etme riskiyle karşılaşacaktır.

Başka bir açıdan, CLOUD Act, Amerikan şirketlerine doğrudan uygulanmakta ve kanun kapsamındaki sağlayıcılara verileri nerede depolandığına bakılmaksızın açıklama yükümlülüğü getirmektedir. Bir *Uygulama Anlaşması* imzalanmaz ise Türkiye CLOUD ACT anlamında bir "kalifiye yabancı devlet" olarak kabul edilemeyecek ve Türk hukukunun ihlalleri, mahkeme taleplerine itiraz olarak sunulamayacaktır. Bu hâlde, ABD'de kurulu ve mukim bir şirket, Türkiye'de depoladığı verileri mahkemeye açıklamak ve KVKK'yı ihlal etmek durumunda kalacaktır.

Dahası, KVKK'nın 5. maddesinin 2. fıkrasında yer alan veri işleme şartlarının bulunduğu, hizmet sağlayıcının hukuki yükümlülükleri kapsamında, ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermeksizin meşru menfaatlerinden ötürü verileri aktardığı kabul edilirse bile, kişisel verinin aktarılacağı yabancı ülkeye ilişkin şartların sağlanması gerekecektir. KVKK'nın 9. maddesi, ilgili kişinin açık rızası bulunmuyorsa ve veri işleme şartlarına dayanarak aktarım yapılıyorsa, ilgili yabancı ülkede yeterli korumanın bulunmasının, ya da yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunmasının gerekli olduğunu düzenlemektedir. Dolayısıyla, ilgili kişinin

açık rızasının bulunmadığı hâllerde, ABD menşeli bir hizmet sağlayıcısının CLOUD Act kapsamında ABD adli makamlarına veri ifşa etmesi için ABD'nin yeterli korumanın bulunduğu ülkeler arasında sayılması gerekecektir.

KVKK'nın 9. maddesi, yabancı bir ülkede yeterli koruma bulunup bulunmadığına ve bu ülkeye veri aktarımına izin verilip verilmeyeceği değerlendirilirken Türkiye'nin taraf olduğu uluslararası sözleşmelerin, kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunun, kişisel verinin niteliği ile işlenme amaç ve süresinin, verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasının ve ilgili ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemlerin değerlendirileceğini düzenlemektedir. Karşılıklılık unsurunu içerecek bir uluslararası sözleşme olarak tanımlanabilecek bir *Uygulama Anlaşması* imzalanmasının böyle bir değerlendirme kapsamında faydalı olacağı düşünülmektedir.

Türk hukuku bakımından değerlendirilecek olursa, Türkiye ve ABD arasında bir *Uygulama Anlaşması* imzalanması mümkün görülmektedir. Hâlihazırda, iki ülke arasında imzalanmış "Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Yardım Anlaşması" yürürlükte bulunmaktadır. (06.07.1979 tarihinde imzalanmış Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Yardım Anlaşması) Bu anlaşmanın 15. maddesi kapsamında tarafların "suçun işlenmesinde kullanılmış veya kanıt olarak gerekli olabilecek eşyalara" kendi yasalarına ve üçüncü tarafların haklarına bağlı olarak el koyabileceği ve bunları karşı tarafa teslim edeceği düzenlenmiştir (06.07.1979 tarihinde imzalanmış Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Yardım Anlaşması, madde 15). Anlaşma gerekçesinde ceza işlerinde karşılıklı yardım hükümlerinin gerekçesi olarak "karşılıklı bilgi sağlanması" hususunun düzenlendiği belirtilmiştir (06.07.1979 tarihinde imzalanmış Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Yardım Anlaşması Genel Gerekçesi). Günümüzde söz konusu olabilecek bir *Uygulama Anlaşması* aynı temellere dayalı olabilecek ve hizmet sağlayıcılarına ABD mahkemelerinin kararlarını KVKK'yı ihlal etmeden yerine getirme imkânı ve yükümlülüğü sağlayabilecektir. Bu hâllerde, KVKK'nın veri işleme şartlarından olan veri sorumlusu veya işleyenin "hukuki yükümlülüğü" koşulu, Anayasa'nın 90. maddesi uyarınca Kanun hükmünde olan uluslararası anlaşma uyarınca ortaya çıkacaktır.

Bununla birlikte, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenleyen Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik ("Yönetmelik") kapsamındaki düzenlemelerin de dikkate alınması gerekmektedir. Yönetmelik'in 4. maddesinin 2. bendi kapsamında, "kişisel veriler yurt dışına çıkarılamaz" hükmü ile, "yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi" olarak tanımlanmış işletmeci şirketlerin verileri yurt dışına aktarması men edilmektedir. Dolayısıyla, CLOUD Act kapsamında yurt dışına veri aktarımının hukuka uygun şekilde yapılabilmesi adına, Türk hukukunda yeniden düzenlemelere gidilmesi gerekebilecektir.

Bir başka bakış açısından, CLOUD Act altında imzalanacak bir *Uygulama Anlaşması* altında talep edilecek verilerin ceza soruşturmaları ve kovuşturmalarına etkilerinin ceza hukuku ve insan hakları hukuku bakımından değerlendirilmesi önem arz etmektedir. Benzer örnekleri incelemek gerekirse, CLOUD Act altında Birleşik Krallık ve ABD arasında imzalanan *Uygulama Anlaşması* öncesinde Birleşik Krallık'ta yürürlüğe giren ve CLOUD Act ile benzer minvalde hükümler içeren 2019 Ceza (Denizaşırı Celp Emirleri) Kanunu ekleri kapsamında, ABD'ye aktarılacak verilerin idam cezasına yol açmayacağına dair güvenceler alınana dek bir *Uygulama Anlaşması* imzalanamayacağı hüküm altına alınmıştır (Niblock, 2019). Bu yaklaşıma gerekçe olarak, bir ülke mahkemelerinin diğer ülke kişilerine göndereceği emirlerde, emri karşılayan kişinin bulunduğu ülkede geçerli hukuk sisteminin

güvencelerinin baypas edilmesi olarak gösterilmektedir. Aynı zamanda, Birleşik Krallık ve ABD arasındaki muhtemel anlaşmanın insan hakları perspektifinden yaratacağı olumsuz etkiler ise sivil toplum örgütlerinin eleştirilerine konu olmuştur (Human Rights Watch, 2019).

GÜNÜMÜZDE BULUT TEKNOLOJİLERİ VE ULUSAL TUTUMLAR

CLOUD Act'in gerekçelerinin, gittikçe dijital ve karmaşık hâle gelen dünyamızın gerçekleri olduğu ve bu gerçeklerin yasal prosedürleri güçleştirdiği tartışmasız görülmektedir. Bulut sistemleri günümüzde üç farklı model ile açıklanmaktadır (Schwartz, 2018).

Bu üç bulut modelinden ilki, verilerin "shard" adı verilen küçük parçalara ayrıldığı Veri Parçalama ("*Data Shard*") modelidir. Veri Parçalama modelinde, veriler parçalara ayrılarak birden fazla uluslararası ülkede, sürekli bir seyahat hâlinde saklanmaktadır. Google Pennslyvania davasında mahkeme Google'ın bu modeli benimsediğini, kullanıcıların verilerini anlamlı tek bir bütün olarak saklamadığını, aksine her bir veri dosyasını parçalara böldüğünü ve uluslararası sunucularda sakladığını, ayrıca Google'ın buluttaki verilere yalnızca ABD sınırları içinde eriştiğini saptamıştır (232 F. Supp. 3d 708, 723 E.D. Pa. 2017).

İkinci model, Microsoft davasında da olduğu gibi, verinin sabit olarak bir ülkede saklandığı Veri Lokalizasyonu (*"Data Localization"*) modelidir. Bu modelde, veri bütün olarak veya bir kısmıyla, sabit bir lokasyonda saklanır. Örneğin, Microsoft davasında kullanıcının içerik-dışı bilgileri ABD'de saklanmaktayken, yazışma içerikleri İrlanda'da saklanmaktadır. Benzer şekilde Amazon İnternet Hizmetleri, dünyanın çeşitli ülkelerinde 55 adet depolama lokasyonu kurmuştur ve Alman telekomünikasyon şirketleri münhasıran Almanya'da depolanması gereken veriler için Almanya'da kurulu bulut sistemleri kullanmaktadır (Schwartz, 2018).

Son model ise *"Data Trust"* olarak adlandırılan, Veri Lokalizasyonu modelinin farklı bir biçimidir. Bu modelde, veriler yine bir ülke veya bölgede bulunan bir bulutta saklanabilir, fakat buradaki farklılık verilere erişimi olan Veri Yediemini *"(Data Trustee")* ve sistemi yöneten ama verilere erişimi bulunmayan Veri Yöneticisi *("Data Manager")* olmak üzere iki farklı kişiliğin söz konusu olmasıdır. Güncel olarak, yalnızca Microsoft'un bu metodu kullandığı, bu model altında *Microsoft Cloud Germany* adı verilen bir hizmet sunduğu ve burada saklanan verilerin T-systems adlı bağımsız bir Alman şirketinin emanetinde olduğu bilinmektedir. Microsoft ile T-systems arasında Alman hukukunun şartları doğrultusunda kurulan hukuki ilişki Microsoft'un verilere erişimini ciddi ölçüde kısıtlamaktadır (Schwartz, 2018).

Günümüzde bulut teknolojilerinin gelişiminin, Depolanan İletişimler Kanunu gibi 30 yaşını aşmış kanunlar veya Karşılıklı Adli Yardım Anlaşmaları gibi hukuki enstrümanlar ile çözülemeyecek hukuki sorunlara yol açtığı görülmektedir. Bu sorunlar, Google gibi çokuluslu bulut hizmeti sağlayıcılarının birçok ülkede faaliyet göstermesi ve verileri "shard" adı verilen parçalara ayırarak birden fazla ülkede yer alan sunucularda saklamasından kaynaklanmaktadır. Bu sistemden ötürü, veri "parçalarının" hangi sunucuda depolandığı hizmet sağlayıcılar dâhil kimse tarafından bilinmediğinden, hangi ülke hukukunun uygulanabileceği ya da ihlâl edilebileceği meçhuldür (Krishnamurthy, 2016). Bunun yanında, elektronik iletiler açılmadan önce kimin kişisel verilerini içerdiği bilinmediğinden kimin gizlilik haklarının ihlâl edilebileceği bilinememektedir (Krishnamurthy, 2016).

SONUÇ

Amerikan adli makamlarının ve hâkimlerinin Microsoft davasının ilk aşamalarında Depolanan İletişimler Kanunu'nun yorumlanmasında benimsediği yaklaşımın saldırgan ve taşkın olduğunu söylemek yanlış olmayacaktır. Amerikan savcıları, sulh hâkimi ve bölge mahkemesinin yürüttüğü mantık, herhangi bir Amerikan şirketinin erişimi ve kontrolü bulunduğu sürece, verilerin depolandığı ülkenin hukuku veya ilgili kişinin veri koruma haklarına bakılmaksızın, her türlü verinin Amerikan adli kurumlarına açıklanmasını gerektirecekti. Bu şekilde arama kararları iki riske yol açmaktaydı: birincisi Microsoft davasında Temyiz Mahkemesi'nin verdiği kararda olduğu gibi yargı denetimi sonucunda böyle bir arama kararının uygulanamaz olduğu tespit edilebilecekti.

İkincisi, CLOUD Act öncesinde, böyle bir uygulamanın yerleşik hâle gelmesi durumunda, herhangi bir suçla ilgileri bulunmasa da, ABD hukuku uyarınca kurulmuş olan veya ABD sınırları içinde varlığı bulunan internet hizmet sağlayıcılarının başka ülkelerde veri sağlamaları veya başka ülke vatandaşlarının verilerini depolamaları hâlinde büyük bir risk altına girdikleri söylenebilecekti. Bu şirketler bir arama kararı hâlinde iki seçeneğe sahipti: ya Amerikan adli makamlarının geniş ve saldırgan yorumuna boyun eğerek verileri sunacak ve yurt dışında veri depolanan ülkenin veri koruma mevzuatını ihlal etme riskini üstlenecek, ya da Amerikan mahkemelerinin kararlarına uymayarak yaptırımlara davet çıkaracaklardı.

CLOUD Act ile birlikte, bu riskler kısmen ortadan kaldırılmış görünmektedir. Amerikan hükümetinin *Uygulama Anlaşması* adı verilen anlaşmaları yürürlüğe koyacağı devletlerin sınırları dâhilinde depolanan verilerin edinilmesi ciddi ölçüde kolaylaşmış olacaktır. Ayrıca, CLOUD Act uyarınca *Uygulama Anlaşması'nın* imzalanması için ilgili yabancı devletin hizmet sağlayıcılar üzerindeki gizlilik yükümlülüklerini, ABD makamlarının taleplerine uygulanacak ölçüde, ortadan kaldırmaları aranacaktır.

Böyle bir anlaşmanın imzalanmadığı ülkelerde depolanan verilere ilişkin uygulama ise hâlen tam olarak belirli görünmemektedir. Microsoft davasında, Temyiz Mahkemesi'ne kadar giden süreçte Microsoft'un ABD sınırları dâhilinde erişebildiği verilerin aslında yurt dışında bulunan veriler olmadığı, dolayısıyla erişim esasına göre Depolanan İletişimler Kanunu'nun yurt dışı veya sınır ötesi uygulamasının söz konusu olmadığı kabul edilmiştir. Temyiz Mahkemesi ise, bu tür bir yorumun kanunun yurt dışına uygulandığı anlamına geleceğini, bunun ise kanunda açıkça düzenlenmedikçe mümkün olmadığını saptamıştır. CLOUD Act yurt dışında yer alan verilerin talep edilebileceğini açıkça düzenleyerek *Morrison* içtihadında öngörülen, kanunun yurt dışına etkisinin açıkça düzenlenmesi koşulunu yerine getirmektedir. Dolayısıyla CLOUD Act kapsamında, Amerikan hukukuna tabi bir hizmet sağlayıcısından yurt dışında depoladığı verileri açıklaması talep edilebilecektir. Fakat bu düzenleme ile mahkemelerin şirketlerden yurt dışında depoladıkları verileri talep etmesi, Uygulama Anlaşması imzalanmayan ülkelerde yerel hukuk kuralları ile çelişki yaratabilecektir. Bu ülkelerde yerel hukuk kurallarına aykırılıktan kaçınmak için, hâlen yürürlükte olan fakat yavaşlığı ile eleştirilen Karşılıklı Adli Yardım Anlaşmalarına başvurulması gerekecektir (Bilgiç, 2018). Dolayısıyla, CLOUD Act'in sorunları kökünden çözdüğünü söylemek mümkün görülmemektedir.

CLOUD Act, İnsan Hakları İzleme Komitesi gibi kurumlar tarafından, hak ve özgürlükler rejimi zayıf ülkelerin kalifiye yabancı devlet olarak tanımlanabileceği ve bu devletlere kişisel verilere geniş bir erişim sağlanabileceği endişeleri ile eleştirilmektedir (Davis ve Gressel, 2018). Bunun yanında, CLOUD Act kapsamında belirlenen koşulları taşımayan ve dolayısıyla kalifiye olmayan hükümetlerin veriye erişiminin kısıtlanmasına karşın, Amerikan adli makamları tarafından ABD'li şirketlerin dünyanın her yerinde depoladığı verilere sınır tanımadan erişilebilecek olmasının adaletsiz bir durum yaratılabileceği yönünde eleştiriler dile getirilmektedir (Bilgiç, 2018).

ABD Adalet Bakanlığı ise, Karşılıklı Adli Yardım Anlaşmalarının, delil taleplerinin artan hacmi karşısında yetersiz kaldığı bir dünyada CLOUD Act'in uluslararası veri paylaşımı için önemli bir gelişme olduğunu savunmaktadır. ABD Adalet Bakanlığı'nın CLOUD Act'e ilişkin raporu, verilerin parçalara ayrılarak farklı konumlarda yer alan veri depolama merkezleri ya da bulut teknolojilerde saklanmasının geleneksel adli yardım anlaşmalarının uygulamasını güçleştirdiğini ileri sürmektedir (U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2019). ABD Adalet Bakanlığı, Amerikan hukukuna tabi bulut hizmeti sağlayıcılarının yabancı hükümetlere veri sunmaktan kaçındığını, bu yönde taleplerin farklı hukuk sistemleri bakımından ihtilafa yol açabildiğini, CLOUD Act ile bu sorunların çözülmesinin amaçlandığını ve bu çözümlerin kişilerin gizlilik haklarına zarar vermeyeceğini belirtmektedir (U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2019). CLOUD Act'in, hükümetlerin elektronik verilere erişimini hukukun üstünlüğü, gizlilik hakları ve insan haklarına uygun biçimde ve ülkelerin hukuk sistemleri arasındaki ihtilafları kaldırarak sağlamayı amaçladığı, bu amaca ulaşılamazsa veri lokalizasyonunun teşvik edileceği ve uluslararası ticaret ve kamu güvenliğinin zedeleneceği ifade edilmektedir (U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, 2019). Benzer ifadeler, Münih'te 5. Alman-Amerikan Veri Koruma Günü konferansına katılan ABD Başsavcı Yardımcısı Richard W. Downing tarafından tekrar edilmiş, CLOUD Act ile uluslararası adli yardımlaşmanın kolaylaştırılacağı, *Uygulama Anlaşması* kapsamında bir ülkenin diğer ülkede bulunan hizmet sağlayıcısına talimat verebileceği ve bu şekilde ülkelerin veriye erişimi önündeki engellerin kaldırılacağı öne sürülmüştür (Downing, 2019).

CLOUD Act, uluslararası hukuk normlarının yerel düzenlemeler ile şekillenebileceği bir örnek olarak karşımıza çıkmaktadır. Bu anlamda, CLOUD Act'in etkisi GDPR veya çeşitli AB düzenlemelerine benzetilmektedir. CLOUD Act, ABD hukuku kapsamında geçerli olacak bir düzenleme olsa da, iki sebepten ötürü uluslararası hukuka etki edecektir. Birincisi, büyük miktarlarda veri yöneten uluslararası teknoloji şirketlerini kapsadığından, bu şirketler aracılığıyla dünyanın diğer ülkelerinde sonuç doğuracaktır. İkincisi, ABD devleti ile *Uygulama Anlaşması* imzalamak isteyen ülkelerin bu düzenlemenin koşullarına uyum sağlaması gerekecektir. Kimi hukukçular CLOUD ACT'in uluslararası veri koruma standartları geliştirebileceğini, hatta Birleşik Krallık hukukunda bu maksatla veri korumaya ilişkin yeni düzenlemeler getirildiğini ifade etmekte ve ABD'nin uluslararası standartları belirlemek adına değerli bir çaba sarf ettiğini öne sürmektedir. Bu doğrultuda, iyi ihtimalde gizlilik ve güvenliği merkeze alan uluslararası veri koruma standartlarının benimsenmesi ve kötü ihtimalde yaygın Veri Lokalizasyonu ve bölünmüş pazarlara yol açabileceği öne sürülmektedir (Daskal, 2018).

Son olarak, verinin gün geçtikçe değer kazandığı dünyamızda, Fransa, Almanya, Rusya ve Çin gibi ülkelerin, vatandaşlarına ilişkin verilerin yalnızca yurt içinde yer alan sunucu ve bulut sistemlerinde saklanabileceğini düzenlemesinin ya da ABD ve Birleşik Krallık gibi ülkelerin CLOUD Act veya Birleşik Krallık Soruşturma Yetkileri Kanunu ile yurt dışında yer alan verilere erişim sağlamayı amaçlamasının ya da bu amaçla imzalanan uluslararası anlaşmaların yaygın uygulama hâlini alacağı düşünülmektedir.

KAYNAKLAR

12 Teknoloji Şirketi. (2018, Ocak 18). Brief for Technology Companies as Amici Curiae in Support of Respondent. https://www.supremecourt.gov/DocketPDF/17/17-2/28322/20180118154539559_17-2%20USA%20v.%20Microsoft%20Corporation.pdf adresinden alındı.

ABD Temsilciler Meclisi. (1986). H.R. Report 99-647. https://www.justice.gov/sites/default/files/jmd/legacy/2013/10/16/houserept-99-647-1986.pdf adresinden alındı.

ABD Temsilciler Meclisi. (2001). H.R. Report 107-236. https://www.hsdl.org/?abstract&did=487675 adresinden alındı.

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. (2019, Ekim 3). Washington. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf adresinden alındı.

Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences. (2016, 12 10). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN adresinden alındı.

Albrecht, J. P., Veld, S. I., Reding, V., Sippel, B., & Voss, A. (2018, Ocak 18). Brief of Amici Curiae Jan Phillip Albrecht, Sophie In't Veld, Viviane Reding, Birgit Sippel and Axel Voss, Members of the European Parliament in Support of Respondent Microsoft Corporation. https://www.supremecourt.gov/DocketPDF/17/17-2/28328/20180118155453076_17-2%20bsac%20Jan%20Philipp%20Albrecht.pdf adresinden alındı.

Avrupa Komisyonu. (2017, Aralık 13). Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party. https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf adresinden alındı.

Beattie, A. (2019, Haziran 24). *Technology: how the US, EU and China compete to set industry standards*. Financial Times: https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271 adresinden alındı.

Bilgiç, S. (2018). Something Old, Something New and Something Moot: The Privacy Crisis Under the Cloud Act. *Harvard Journal of Law & Technology, Vol. 32 No. 1 Fall 2018*. https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech321.pdf adresinden alındı.

Birleşik Krallık Devleti. (2017). Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Neither Party. https://www.supremecourt.gov/DocketPDF/17/17-2/23693/20171213140104710_17-2%20-%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland.pdf adresinden alındı.

Boyd v. United States, 116 U.S. 616 (U.S. Supreme Court 1886).

Brignall, M. (2018, Kasım 21). *Amazon hit with major data breach days before Black Friday*. The Guardian: https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday adresinden alındı.

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

Cleary Gottlieb. (2018). CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications. https://www.clearygottlieb.com/news-and-insights/publication-listing/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications adresinden alındı.

Commission Implementing Decision (EU) 2016/1250. (2016, 8 1). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN adresinden alındı.

Daskal, J. (2018, Mayıs). *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0.* Stanford Law Review: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/ adresinden alındı.

Daskal, J., & Swire, P. (2019, Ekim 8). *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards.* lawfareblog.com: https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards adresinden alındı.

Davis, F. T., & Gressel, A. R. (2018). *Storm Clouds or Silver Linings? The Impact of the U.S. Cloud Act.* American Bar Association. https://www.debevoise.com/insights/publications/2019/02/storm-clouds-or-silver-linings adresinden alındı.

Downing, R. W. (2019, Mayıs 16). *Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the 5th German-American Data Protection Day on "What the U.S. Cloud Act Does and Does Not Do"*. justice.gov: https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american adresinden alındı.

E-Discovery Institute. (2017, Aralık 13). Brief for Amici Curiae E-Discovery Institute et al. in Support of Neither Party. https://www.supremecourt.gov/DocketPDF/17/17-2/23694/20171213140407555_Microsoft%20Amicus%20-%20TO%20FILE.PDF adresinden alındı.

Farrell, H., & Newman, A. L. (2020, 7 28). Schrems II Offers an Opportunity—If the U.S. Wants to Take It. https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it adresinden alındı.

Former Law Enforcement, National Security and Intelligence Officials. (2017, Aralık 13). Brief of Former Law Enforcement, National Security and Intelligence Officials as Amici Cruiae in Support of Neither Party. https://www.supremecourt.gov/DocketPDF/17/17-2/23633/20171213113332456_17-2%20Amicus%20Brief%20in%20Support%20of%20Neither%20Party.pdf adresinden alındı.

Goldfield, C., & Sonkar, S. (2020, 8 25). 'Schrems II' requires a rethink of the CLOUD Act. iapp.org. https://iapp.org/news/a/schrems-ii-requires-a-rethink-of-the-cloud-act/ adresinden alındı.

Grundy, C. (2019, Mayıs 9). *Facebook's Worst Privacy Abuses & Data Scandals – Timeline*. selfkey.org: https://selfkey.org/facebook-data-privacy/ adresinden alındı.

Harvard Law Review. (2019). District Court Holds That SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers. *128 Harv. L. Rev. 1019*. https://harvardlawreview.org/2015/01/in-re-warrant-to-search-a-certain-email-account-controlled-maintained-by-microsoft-corp/ adresinden alındı.

Human Rights Watch. (2019). *Groups Urge Congress to Oppose US-UK Cloud Act Agreement*. Human Rights Watch: https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement adresinden alındı.

In Re Grand Jury Proceedings the Bank of Nova Scotia United States of America, Plaintiff-appellee, v. the Bank of Nova Scotia, Defendant-appellant, 740 F.2d 817 (11th Cir.) (US Court of Appeals for the Eleventh Circuit 1984).

In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp.3d 466 SDNY, 15 F.Supp.3d 466 (New York Güney Bölge Mahkemesi 2014). https://casetext.com/case/in-re-warrant-to-search-a-certain-endashmail-account-controlled-amp-maintained-by-microsoft-corp adresinden alındı.

İrlanda Devleti. (2017). Brief For Ireland As Amicus Curiae. https://www.supremecourt.gov/DocketPDF/17/17-2/23732/20171213152516784_17-2%20ac%20Ireland%20supporting%20neither%20party.pdf adresinden alındı.

Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. (2020, 8 10). https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en adresinden alındı.

Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems. (2020, 7 16). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62018CJ0311&from=EN adresinden alındı.

Kerr, O. (2017, 11 27). *Microsoft Challenged the Wrong Law. Now What?* lawfareblog.com: https://www.lawfareblog.com/microsoft-challenged-wrong-law-now-what adresinden alındı

Kerr, O. S. (2004). A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. *72 George Washington Law Review 1208*. Available at SSRN: https://ssrn.com/abstract=421860 adresinden alındı.

Krishnamurthy, V. (2016). *Cloudy with a Conflict of Laws*. The Berkman Klein Center for Internet & Society Research Publication. https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1 adresinden alındı.

Medina, M. (2013). The Stored Communications Act: An Old Statute for Modern Times. *63 American University Law Review 267*.

Microsoft v. United States, No. 14-2985 - 2nd Cir., No. 14-2985 (United States Court of Appeals for the Second Circuit Temmuz 14, 2016). https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html adresinden alındı.

Microsoft v. United States, No. 14-2985 - 2nd Cir., 14-2985 (United States Court of Appeals for the Second Circuit Ocak 24, 2017).

Nakashima, E. (2014, Haziran 10). *Microsoft fights U.S. search warrant for customer e-mails held in overseas server*. Washington Post: https://www.washingtonpost.com/world/national-security/microsoft-fights-us-

search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html adresinden alındı.

Niblock, R. (2019). *Lexology Criminal Law Blog*. Lexology: https://www.lexology.com/library/detail.aspx?g=0d08a16a-1c4a-4c3f-9396-69f09c1579dc adresinden alındı.

Nichols, S. (2018, Haziran 4). *Your Phone Is Listening and it's Not Paranoia*. Vice.com: https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia adresinden alındı.

Pendergast, T. (2018, Mart 28). *The Next Cold War is Here, and It's All About Data*. Wired.com: https://www.wired.com/story/opinion-new-data-cold-war/ adresinden alındı.

Schultheis, N. (2015). *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.

Schwartz, P. M. (2018, Ekim). Legal Access to the Global Cloud. *Columbia Law Review, vol 118.*, s. 1681-1762. https://www.jstor.org/stable/10.2307/26511248 adresinden alındı.

States Of Vermont Et Al. (2017, Temmuz 27). Brief for the States Of Vermont Et Al. as Amici Curiae. https://www.supremecourt.gov/DocketPDF/17/17-2/23704/20171213142200573_U.S.%20v.%20Microsoft%20-%20multistate%20amicus%20brief.pdf adresinden alındı.

The Council of Bars and Law Societies of Europe. (2018, Ocak 18). Brief of The Council of Bars and Law Societies of Europe as Amicus Curiae in Support of Respondent. https://www.supremecourt.gov/DocketPDF/17/17-2/28246/20180118123639107_17-2%20Council%20of%20Bars%20and%20Law%20Societies%20Amicus%20Brief.pdf adresinden alındı

Thompson II, R. M., & Cole, J. P. (2015). *Stored Communications Act: Reform of the Electronic Communications Privacy Act.* Congressional Research Service.

U.S. Department of Justice. (2019, Ekim 7). 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. https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us#:~:text=Underpinned%20by%20Australian%20legislation%20yet,based%20companies%2C%20and%20vice%20versa. adresinden alındı.

U.S. Department of Justice. (2019, Eylül 26). Joint US-EU Statement on Electronic Evidence Sharing Negotiations. justice.gov: https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations adresinden alındı.

U.S. Department of Justice. (2019, Nisan). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. https://www.justice.gov/opa/press-release/file/1153446/download adresinden alındı.

U.S. Department of Justice. (2019, Ekim 3). U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online. justice.gov: https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists adresinden alındı.

United Kingdom Foreign & Commonwealth Office. (2019, Ekim 7). *UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019]*. gov.uk: https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_conten adresinden alındı.

United States v. Miller, 425 U.S. 435, No. 74-1179 (U.S. Supreme Court Nisan 21, 1976).

Wingfield, N., & Kang, C. (2016, Temmuz 14). *Microsoft Wins Appeal on Overseas Data Searches.* nytimes.com: https://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overseas-data-searches.html adresinden alındı.

EK: Microsoft v. ABD davasında sunulan görüşlerin listesi.

ABD Hükümeti Lehine Görüşler	Tarafsız Görüşler	Microsoft Lehine Görüşler
Çeşitli ABD eyaletlerinin görüşü	Birleşik Devletler Gizlilik Hakkı Özel Raportörü Joseph Cannataci görüşü	Electronic Privacy Information Center ile 37 teknik uzman ve hukuk akademisyeninin görüşü
	Eski Kolluk Kuvveti, Ulusal Güvenlik ve İstihbarat Yetkilileri görüşü	Almanya, Fransa, Polonya ve İrlanda sektör derneklerinin görüşü
	Avrupa Birliği'ni temsilen Avrupa Komisyonu görüşü	51 Bilgisayar mühendisinin görüşü
	Yeni Zelanda Gizlilik Memurluğu görüşü	The Competitive Enterprise Institute, CATO Institute, TechFreedom, Reason Foundation ve American Consumer Institute Center for Citizen Research görüşü
	Birleşik Krallık ve Kuzey İrlanda görüşü	Avrupa Baroları ve Hukuk Toplulukları Konseyi görüşü
	E-Discovery Institute görüşü	ABD Kongre üyeleri görüşü
	İrlanda devleti görüşü	Uluslararası ve Sınır Ötesi Hukuk Akademisyenleri görüşü
		12 Ticaret ve Tüketici Derneğinin görüşü
		Avrupa Birliği Veri Koruma ve Gizlilik Akademisyenleri görüşü
		Basın Özgürlüğü Komitesi raportörleri ve 40 medya organizasyonu görüşü
		New York Üniversitesi Hukuk Fakültesi Polis Projesi görüşü
		Teknoloji şirketleri görüşü
		Avrupa Parlamentosu üyeleri Jan Philipp Albrecht, Sophie in't Veld, Viviane Reding, Birgit Sippel ve Axel Voss'un görüşü
		DigitalEurope, Bitkom Tech in France, Syntec Numérique ve diğer Avrupa Ulusal Ticaret Organizasyonları görüşü
		International Business Machines Corporation görüşü
		Privacy International, İnsan ve Dijital Haklar Organizasyonları ve uluslararası hukuk akademisyenleri görüşü
		Avrupa Şirket Avukatları Derneği görüşü

		NYU Hukuk Fakültesi Brennan Adalet Merkezi, Amerikan Toplumsal Özgürlükler Derneği, Electronic Frontier Foundation, Restore the Fourth Inc. ve R Street Institute görüşü
		Washington Hukuk Derneği görüşü
		(ABD Anayasası) Dördüncü Ek Madde Akademisyenleri görüşü
		InternetLab Hukuk ve Teknoloji Merkezi görüşü