

SCHREMS II KARARI

ve Sonuçları

Doç. Dr. Murat Volkan DÜLGER & Av. Gülçin GÜMÜŞ

Kişisel verilerin korunması alanında merakla beklenen gelişmelerden biri Schrems II davasında verilecek karardır. Avrupa Adalet Divanı, resmi Twitter hesabı üzerinden C-311/18 - Facebook İrlanda ve Schrems kararının 16 Temmuz'da açıklanacağını duyurmuştu. Söz konusu karar belirtilen tarihte açıklandı ve kişisel verilerin ülkeler arasında aktarımı konusundaki tartışmalar yeniden alevlendi.

Schrems II olarak adlandırılan bu karar, özellikle standart sözleşme hükümlerinin Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation – “GDPR”) uyarınca gerçekleştirilecek olan veri aktarımı için geçerli bir yöntem olup olmadığı noktasında büyük önem arz etmektedir. Öte yandan Avrupa Birliği ile Amerika Birleşik Devletleri arasında bulunan Mahremiyet Kalkanı Kararı ile sağlanan koruma düzeyinin de yeterliliği ve geçerliliği sorgulanmaktadır. Bu incelemeler GDPR ve Avrupa Birliği Temel Haklar Şartı (“Şart”) hükümleri doğrultusunda yapılmıştır.

GENEL OLARAK SCHREMS II DAVASI

Schrems II olarak adlandırılan “Veri Koruma Otoritesi v Facebook İrlanda ve Maximillian Schrems (Data Protection Commissioner

v Facebook Ireland and Maximillian Schrems) ^[1] davasının konusunu, İrlanda Yüksek Mahkemesi tarafından Avrupa Adalet Divanı'ndan görüş talep edilmesi oluşturur. Buna göre İrlanda Yüksek Mahkemesi, AB dışında veri aktarımına imkan veren 2010/87 sayılı “Standard Contractual Clause (“SCC Kararı”)^[2]” olarak anılan standart sözleşme hükümlerinin geçerliliği konusunda görüş talep etmiştir. Dolayısıyla davanın çıkış noktası Maximillian Schrems tarafından Facebook'un veri koruma uygulamalarının eleştirilmesi ve AB mevzuatı ile ABD gözetim yasalarının çeliştiği ve ABD yasaları tarafından sağlanan korumanın yetersizliğine ilişkin iddialara dayanır.

Burada söz konusu olan kararın niteliği, Avrupa Adalet Divanı'nın

AB üyesi bir devletin mahkemesinden gelen talep üzerine AB hukukunun yorumlanmasını içeren bir ön karar (preliminary ruling) olmasıdır^[3]. Bu ön kararlara ilişkin temyiz yolu açık olmayıp; kararlar, AB hukukuna ilişkin nihai tespitler içermesi bakımından oldukça önemlidir.

■ SAVCILIK GÖRÜŞÜ

Divan tarafından verilen kararın incelemesine geçmeden önce Avrupa Adalet Divanı'nda Advocate General (Hukuk Sözcüsü) olarak görevini sürdürmekte olan Henrik Saugmandsgaard Øe tarafından 19 Aralık 2019 tarihinde yayınlanan Savcılık Görüşü'nü ("Savcılık Görüşü") hatırlamak gerekir^[4].

Savcı, yayınlamış olduğu görüşünde standart sözleşme hükümlerinin geçerli olduğunu belirterek önemli bir adım atmıştı. Zira standart sözleşme hükümlerinin uygulanması özellikle Türkiye gibi güvenli kabul edilmeyen ülkelere yapılan veri aktarımları açısından kullanılabilecek en iyi mekanizmalardan biridir. Dolayısıyla bu hükümlerin kabul edilmesi, ticari faaliyetleri çerçevesinde yurt dışına veri aktarımı gerçekleştiren şirketler açısından oldukça önemlidir.

Aksi takdirde bu şirketler hukuka aykırı veri transferi gerçekleştiren bir konumda olacak ve bu aktarım için başka yöntemler aramak durumunda kalacaktır.

Bununla birlikte savcı tarafından yayınlanan görüşün yurt dışına veri aktarımına tamamen izin verilmesi şeklinde yorumlanması yanlış olacaktır. Zira görüşte veri sorumlularının standart sözleşme hükümleri kapsamında ilgili kişilerin haklarının korunması açısından GDPR düzeyinde bir korumanın temin edilmesi gerektiği belirtilmiştir.

Dolayısıyla savcının görüşü, ilgili kişilerin haklarının GDPR düzeyinde korunması şartıyla standart sözleşme hükümlerinin kabul edilmesi gerektiğine ilişkindir. Aksi takdirde ilgili veri koruma otoritesinin veri aktarımının durdurulması veya veri aktarımının yasaklanması gerektiğine ilişkin görüş belirttiğinin de altını çizmekte fayda vardır.

DİVAN TARAFINDAN YAPILAN İNCELEME VE KARAR

1.ÖN KARAR TALEBİNİN KABUL EDİLEBİLİRLİĞİ

Ön karar talebinin kabul edilemez olduğunu iddia eden taraflar ile bu iddiaların dayanakları kısaca şu şekildedir:

	İtiraz Gerekçesi	Divan Kararı
Facebook İrlanda	Ön karar için atıfta bulunulan soruların da-yandığı 95/46/EC sayılı Direktif hükümleri GDPR ile yürürlükten kaldırılmıştır.	- GDPR'nın 94/1 maddesi uyarınca 95/46/EC sayılı Direktif, 25 Mayıs 2018 tarihinden itibaren yürürlükten kaldırılmışken; mevcut ön karar talebi 9 Mayıs 2018'de iletilmiştir. - Direktif'in sorularda atıf yapılan ilgili hükümleri esasen GDPR maddeleriyle çoğaltılmıştır. - Divan, ulusal mahkemelerin karar vermek için ihtiyaç duydukları AB hukukunun tüm hükümlerini, kendisine yöneltilen sorularda açıkça belirtilmemişse bile yorumlamakla yükümlüdür.
Almanya	- Veri Koruma Otoritesi, SSC Kararı'nın geçerliliği hakkında kesin bir görüş değil yalnızca şüphelerini dile getirmiştir. - Divan'a başvuran ulusal mahkeme Schrems'in söz konusu veri aktarımlarına açık bir şekilde rıza vermiş olup olmadığına karar verememiştir, zira açık rıza söz konusu olsaydı bu sorulara cevap vermek gereksiz olurdu.	- Divan, atıfta bulunulan soruların AB hukukuna ait bir kuralın yorumlanması veya geçerliliği ile ilgili olduğu durumlarda, kural olarak bir karar vermek zorundadır. - Ulusal mahkemeler tarafından yöneltilen sorular, varsayımsal olarak ilgilidir. - Divan, kendisine yöneltilen bir soruyu, ancak yorumun talep edildiği ana eylemin veya sorunun varsayımına dayandığı veya cevap vermek için gerekli materyale sahip olmadığı durumlarda cevap vermeyi reddedebilir. - Sonuç olarak, ön karar talebinin kabul edilebilir olduğu sonucuna varılmıştır.
Birleşik Krallık	Bir ön karar için atıfta bulunulan sorular varsayımsaldır, zira ulusal mahkeme verilerin SCC Kararı'na dayanılarak veri aktarıldığını bula-mamıştır.	

2.SORULAR NEDEN GDPR HÜKÜMLERİ UYARINCA CEVAPLANMALIDIR?

Mahkeme'ye göre sorular GDPR (General Data Protection Regulation – "GDPR") hükümlerine göre cevaplanmalıdır. Çünkü:

- Ön kararın konusu, Bay Schrems tarafından yapılan şikayet üzerine ilgili Veri Koruma Otoritesi'nin kişisel bilgilerin Facebook İrlanda tarafından Facebook Inc.'e aktarılmasını askıya almasını veya yasaklamasını içeren bir talep üzerine ortaya çıkmıştır.
- Ön karar için atıfta bulunulan sorular 95/46/EC sayılı Direktif hükümlerine atıfta bulunmuş olsa da Veri Koruma Komiseri, söz konusu Direktif'in yürürlükten kaldırıldığı süreçte mevcut şikayete ilişkin nihai bir kararı henüz kabul etmemiştir.
- Ulusal bir kararın bulunmaması, mevcut şikayeti, 24 Eylül 2019 tarihli Google'un bölgesel kapsamına ilişkin kararına benzer şekilde Direktif'in yürürlükten kaldırılmasından önce kararların alınmış olduğu davalardan ayırmaktadır^[5].

3.DİVAN'A YÖNELTİLEN**SORULAR****VE CEVAPLAR****i. GDPR'ın kapsamı ile****Avrupa Birliği Antlaşması
arasındaki ilişki
bakımından**

AB Antlaşması uyarınca AB içerisinde ulusal güvenliğin sağlanması her bir Üye Devlet'in sorumluluğundadır ve yalnızca AB Üye Devletleri ile ilgilidir. Dolayısıyla Divan'a göre bu kuralın mevcut davada GDPR'ın kapsamına ilişkin olan 2. maddesi ile birlikte yorumlanmasına gerek yoktur^[6].

GDPR hükümleri, 2/1 maddesine göre, "kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine" uygulanır. İşleme faaliyeti ise yine GDPR'ın 4/2 maddesi ile tanımlanmış olup AB içinde gerçekleşen ve üçüncü bir ülkeyle bağlantılı olan işlemler arasında ayırım yapmaz. Öte yandan GDPR'ın "Üçüncü ülkeler veya uluslararası kuruluşlara veri aktarımları" başlıklı



beşinci bölümüyle kişisel verilerin belirli kurallar altında üçüncü ülkelere aktarılmasına imkan tanınmıştır. Buna göre bir Üye Devlet'ten üçüncü bir ülkeye kişisel verilerin aktarılması işlemi tek başına GDPR m. 4/2 uyarınca bir işlemdir ve GDPR m. 2/1 kapsamına girer. Bununla birlikte bu faaliyetin GDPR m. 2/2 kapsamında bir istisna teşkil etmediğine de dikkat edilmelidir^[7].

Mevcut davaya baktığımızda GDPR m. 2/2 çerçevesinde bir istisnanın söz konusu olmadığı anlaşılmaktadır. Zira Facebook İrlanda'dan Facebook Inc.'ye yapılan aktarımın GDPR m. 2/2-c'de belirtilen "tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından" durumunu oluşturması mümkün olmadığı gibi madde m. 2/2-a, b ve d bentlerinde yer alan Devlet veya Devlet makamlarıyla ilgili olan istisnalar kapsamında sayılması da söz konusu değildir. Divan'a göre ticari amaçlar için iki ekonomik aktör arasında aktarılan kişisel verilerin, aktarım sırasında veya daha sonra söz konusu üçüncü ülkenin yetkilileri tarafından kamu güvenliği ve savunma gibi amaçlarla işlenmesi bu aktarımı GDPR kapsamından

çıkmaz. Nitekim bu husus GDPR'nın Komisyon'un üçüncü bir ülkedeki koruma düzeyinin yeterliliğini değerlendirirken göz önünde bulundurulması gereken m. 45/2-a hükmünden de anlaşılmaktadır^[8].

Sonuç olarak GDPR'nın m. 2/1 ve m. 2/2 hükümleri uyarınca, ilk sorunun cevabına ilişkin olarak; GDPR, bir Üye Devlet'te kurulmuş bir ekonomi aktörü tarafından, üçüncü bir ülkede kurulmuş olan başka bir ekonomi aktörüne ticari amaçlarla kişisel veri aktarması işlemi, söz konusu aktarım sırasında veya sonrasında Devlet veya Devlet makamları tarafından bu verilerin kamu güvenliği, savunma veya milli güvenlik amaçlarıyla işlenip işlenmediğine bakılmaksızın uygulanır.

ii. Standart veri koruma hükümlerine dayanarak yapılan aktarıma ilişkin ikinci, üçüncü ve altıncı soru bakımından

Mahkeme, burada GDPR'nın 46/1 ve 46/2-c maddelerinin getirdiği koruma düzeyine uygun olarak kişisel verilerin standart veri koruma koşullarına göre üçüncü bir ülkeye aktarılmasına ilişkin olarak açıklama talep etmektedir. Mahkeme, özellikle böyle bir aktarım kapsamında söz konusu koruma seviyesinin sağlanıp sağlanmadığını belirlemek için hangi faktörlerin dikkate alınması gerektiğini sorgulamaktadır^[9].

Divan, gerekli koruma seviyesi ile ilgili hükümlerin birlikte okunmasıyla GDPR m. 45/3 uyarınca yeterli koruma kararının bulunmaması halinde veri sorumlusu veya veri işleyen tarafından "uygun önlemler" ile "ilgili kişiye uygulanabilir hakların tanınması" ve "etkili yasal çözümler" güvencelerinin sağlanması koşuluyla Komisyon tarafından kabul edilen standart veri koruma hükümleri ile aktarımın gerçekleştirilebileceği sonucuna ulaşmaktadır. Söz konusu güvencelerin şartları GDPR'nın 46. maddesiyle açıkça belirtilmemişse de



Divan'a göre bu madde, gerçek kişilere yönelik koruma seviyesinin zayıflatılmaması için 44. maddede yer alan genel aktarım düzenlemeleriyle birlikte okunmalıdır. Divan, bu noktada Savcılık Görüşü'ne atıf yaparak, görüşün 117. paragrafına dikkat çekmiştir; buna göre GDPR'ın beşinci bölümünde yer alan hükümler, kişisel verilerin üçüncü bir ülkeye aktarıldığı durumlarda sağlanacak olan koruma seviyesinin Gerekçe m. 6'da belirtilen hedeflere uygun olarak sürekliliğini sağlamayı amaçlamaktadır^[10].

GDPR m. 45, kişisel verilerin üçüncü bir ülkeye aktarılmasında başkaca bir izin veya onay olmaksızın Komisyon kararı ile izin verilebileceğini öngörmektedir. Bu durumda her ne kadar ilk bakışta AB yasal düzenlemeleriyle garanti edilen seviyede bir korumanın sağlanmasının gerekmediği anlaşılsa da "yeterli koruma seviyesi" için Gerekçe m. 104'e bakıldığında aslında durumun böyle olmadığı anlaşılabacaktır. Buna göre üçüncü ülkenin kendi iç hukuku ve uluslararası taahhütleri bağlamında temel hak ve özgürlükler bakımından yeterli ve geçerli standartları sağlaması gerekir. Ayrıca üçüncü ülke Birlik dahilinde sağlanan korumayla eşdeğer yeterli bir koruma seviyesi temin etmelidir ve bu kapsamda özellikle etkili ve bağımsız veri koruma denetimi sağlamalı ve AB üyesi devletlerin veri koruma yetkilileri ile işbirliği mekanizmaları sağlamalıdır. Öte yandan veri sahiplerine etkili ve uygulanabilir haklar ve etkili yasal mekanizmalar tanınmış olmalıdır. Öyleyse esasen bu durumda da AB kapsamında söz konusu olan koruma seviyesinin sağlanması zorunludur. Zira Divan'a göre aksi takdirde Gerekçe m. 6'da açıklanan hedeflere ulaşılması mümkün değildir^[11].

Komisyon yeterli koruma seviyesinin sağlanmadığı kararı verebilir mi?

Gerekçe m. 107, Komisyon'un üçüncü bir ülkeye yönelik olarak yeterli düzeyde veri koruması sağlanmadığına karar verebileceğini düzenler. Bu durumda bağlayıcı şirket kuralları veya geçerli başkaca bir dayanak olmadıkça veri aktarımı yasaktır. Hangi hallerde aktarım yapabileceğinin belirlenmesi açısından ise Gerekçe m. 108 yol göstericidir. Buna göre bir yeterlilik kararının olmaması durumunda, veri sorumlusu veya veri işleyen, aktarım yapabilmek için üçüncü bir ülkedeki veri koruma eksikliğini, veri sahibi için uygun güvenceler yoluyla telafi etmek için bazı önlemler alacaktır. Bu güvencelerin bağlayıcı şirket kuralları veya denetim otoriteleri tarafından kabul edilen standart veri koruma hükümleriyle sağlanması mümkündür. Ancak bu güvencelerin veri koruma gerekliliklerine ve AB içinde veri sahipleri açısından, uygulanabilir hak ve etkili hukuk yollar dahil olmak üzere veri sahipleri açısından söz konusu olan koruma düzeyini sağlaması gerektiğine dikkat edilmelidir. Divan'a

göre böyle bir güvencenin sağlanması esasen Savcılık Görüşü'nün 115. paragrafında da belirtildiği için AB içerisinde garanti edilen yeterli koruma seviyesi ile eşdeğer bir koruma seviyesi anlamına gelir^[12].

AB Antlaşması'nın 6/3 maddesine göre Sözleşme'de yer alan temel haklar AB hukukunun genel ilkelerini oluşturmaktadır ve ayrıca AB Temel Haklar Şartı'nın 52/3 maddesi, Şart'ta yer alan hakların Sözleşme ile güvence altına alınan haklara karşılık geldiğini ve aynı anlam ve kapsamda anlaşılması gerektiğini düzenlemiştir. Bu çerçevede Divan'a göre, Mahkeme'nin AB hukukunun yorumlanması ve AB mevzuatının incelenmesine yönelik olarak yapacağı bir incelemede Şart tarafından güvence altına alınan temel haklar ışığında gerçekleştirilmelidir^[13]. Nitekim aşağıda görüleceği üzere Divan tarafından yapılan birçok inceleme AB Temel Haklar Şartı hükümlerine göre yapılmıştır.

■ Sonuç olarak;

Bir AB üyesi devlette kurulmuş olan ekonomik bir aktör tarafından üçüncü bir ülkede kurulmuş olan başka bir ekonomik aktöre ticari amaçlarla kişisel verilerin aktarılması GDPR kapsamdadır,



Bunun nedeni, Gerekçe m. 10'da belirtildiği gibi gerçek kişilerin tutarlı ve yüksek düzeyde korunmasını sağlamak ve temel hak ve özgürlüklerin korunmasına ilişkin kuralların GDPR m. 46/1'de belirtilen hususlara uygun olarak tutarlı ve homojen bir biçimde uygulanmasını sağlamaktır^[14].

Yeterli koruma düzeyinin belirlenmesinde hangi faktörler ele alınmalıdır?

GDPR m. 46, koruma seviyesinin yeterliliğini değerlendirmek için dikkate alınması gereken faktörleri listelemese de, m. 46/1, uygun güvenceler, veri sahiplerine yönelik olarak uygulanabilir haklar ve etkili etkili çözüm yollarının mevcut olması gerektiğini belirtmiştir. Divan, bir transfer bağlamında yeterli koruma seviyesine ilişkin değerlendirmede AB'de yerleşik olan veri sorumlusu veya veri işleyen ile söz konusu üçüncü ülkede kurulan alıcı arasındaki sözleşme hükümlerinin dikkate alınması gerektiği kanaatindedir. Ayrıca üçüncü ülkenin kamu otoritelerinin aktarım konusu olan kişisel verilere erişime ilişkin sisteme bakılmalıdır. Öte yandan GDPR m. 46 bağlamında dikkate alınması gereken

faktörler, GDPR m. 45/2 ile öngörülen faktörlere eşdeğerdir. Dolayısıyla Divan'a göre bu faktörler için m. 45/2 hükümlerinin de esas alınması mümkündür.

iii. Denetim otoritelerinin konuyla ilgili yetkileri bakımından sekizinci soru

Mahkeme, denetim otoritelerinin yetkileri bakımından GDPR m. 58/2-f (bir işleme yasağı da dahil olmak üzere geçici veya kati bir sınırlama getirilmesi) ile GDPR m. 58/2-j (üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa yönelik veri akışlarının askıya alınması yönünde talimat verilmesi) maddelerinin kapsam ve niteliğini sorgulamaktadır.

Şart'ın 8/3 maddesi ile GDPR'ın 51/1 ve 57/1-a maddelerine göre ulusal denetim makamları, gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunmasına ilişkin AB kurallarına uyulup uyulmadığının izlenmesinden sorumludur. Bu nedenle, bu makamların her biri, kişisel verilerin kendi Üye Devletinden üçüncü bir ülkeye transferinin GDPR ile belirtilen gerekliliklere uygun olup olmadığını kontrol etme yetkisine sahiptir. Buradan hareketle denetim otoritelerinin birincil sorumluluğunun GDPR

hükümlerinin uygulanmasını izlemek ve uygulanmasını sağlamak olduğu sonucuna varılabilir. Bu sorumluluk, kişisel verilerin üçüncü bir ülkeye aktarıldığı durumlarda özellikle önemlidir. Zira Gerekçe m. 116'da da belirtildiği gibi kişisel veriler Birlik dışındaki sınırlar içinde hareket ettiğinde gerçek kişilerin, bilgilerinin yasa dışı kullanımından veya ifşa edilmesinden korumak için veri koruma haklarını kullanması daha fazla risk altına girer^[15].

GDPR'ın 57/1-f maddesi uyarınca, her denetim makamı, kendi topraklarında, kişisel verilerin işlenmesinin GDPR düzenlemelerini ihlal ettiğine yönelik bir şikayet aldığı takdirde bunun niteliğini gerektiği gibi incelemek zorundadır. Denetim makamı bu tür bir şikayeti gereken tüm özenle ele almalıdır.

GDPR m. 58/1, denetim otoritelerine, kendilerine sunulan şikayetleri ele almak için kapsamlı soruşturma yetkileri verir. Bir denetim makamı, bir soruşturmanın ardından, kişisel verileri üçüncü bir ülkeye aktarılan bir veri sahibi için o ülkede yeterli düzeyde koruma sağlanmadığı görüşüne varırsa, AB yasaları uyarınca, bu yetersizliğin nedeni veya niteliğine bakılmaksızın,

uygun önlemleri almalıdır. GDPR m. 58/2 de denetim makamlarının bu amaçla benimseyebileceği çeşitli düzeltici yetkileri listelemektedir. Denetim otoritesi, kişisel verilerin aktarımının tüm koşullarını dikkate alarak hangi eylemin uygun ve gerekli olduğunu belirleyecektir. Nitekim Savcılık Görüşü'nün 148. paragrafında da belirtildiği gibi üçüncü bir ülkede standart veri koruma şartlarına uyulmaması halinde denetim makamı tarafından GDPR m. 58/2'de yer alan yetkilerin kullanılması gerekir. Divan'a göre bu durum, SSC kararı ile çelişmemektedir^[16].

Sonuç olarak, GDPR'ın 46/2-c maddesi uyarınca Komisyon'a standart veri koruma şartlarını kabul etmeye yönelik olarak verilen yetki, ulusal denetim otoritelerinin GDPR m. 58/2 uyarınca kullanabileceği yetkilerini kısıtlayamaz. Dolayısıyla Komisyon, bir yeterlilik kararı kabul etmiş olsa bile, kişisel verilerin işlenmesine ilişkin hak ve özgürlüklerinin korunması ile ilgili bir şikayetin söz konusu olması halinde denetim otoriteleri tarafından söz konusu aktarımın GDPR hükümlerine uygun olarak yapıp yapılmadığını inceleyebilir^[17].

iv.SSC Kararı'nın geçerliliğine ilişkin yedinci ve on birinci soru bakımından

SCC Kararı'nın 1. maddesi, standart veri koruma hükümlerinin, bireylerin mahremiyetinin ve temel hak ve özgürlüklerinin korunması ile ilgili yeterli güvenceler sunduğunu öngörmektedir. Ancak bu hükümler, her ne kadar söz konusu maddeleri içeren bir sözleşme yaptıkları takdirde, Avrupa Birliği'nde yerleşik olan bir veri sorumlusunu ve üçüncü bir ülkede kurulan kişisel verilerin transferini alan alıcıyı bağlasa da; sözleşmeye taraf olmadıkları için ilgili üçüncü ülkenin diğer yetkililerini bağlayabilmesi mümkün değildir. Bu durum bir yandan kararın geçerliliğinin sorgulanamaması anlamına gelebilmektedir. Zira karardaki standart veri koruma maddelerinin, sözleşmeye dayalı olduğu göz önünde bulundurulduğunda sözleşmenin doğası gereği verilerin aktarılabilceği üçüncü ülkenin yetkililerini bağlamaz. Ancak Divan, bu geçerliliğin, SSC Kararı'nın GDPR gerekliliklerine uygunluğuna bağlı olduğu kanaati dolayısıyla bu yönden bir inceleme yapılmasını uygun görmüştür^[18]. Gerçekten, de ilgili üçüncü ülkede yürürlükte olan

yasa ve uygulamalara bağlı olarak, böyle bir aktarımın yalnızca standart veri koruma hükümlerine dayanması halinde, söz konusu standart hükümlerin içeriğinin, uygulamada, kişisel verileri etkili bir şekilde korunmasını sağlamak açısından yetersiz kalması mümkündür. Divan'a göre özellikle üçüncü ülkenin yasaları tarafından kamu makamlarına müdahale yetkisi verilmesi hallerinde bu durum ortaya çıkmaktadır^[19].

Divan'ın yapmış olduğu birçok incelemede özellikle kamu makamlarına verilen erişim yetkisine dikkat ettiğinin altını çizmek gerekir. Öyle ki, aşağıda görüleceği üzere Mahremiyet Kalkanı Kararı'nın geçerliliği büyük ölçüde ABD makamlarının yetkileri çerçevesinde ele alınmıştır. Öyleyse bir ülkedeki veri koruma seviyesinin AB hukuku ile eşdeğer bir seviyede olup olmadığının incelenmesinde kamu makamlarına ait erişim yetkileri ile bu yetkilerin sınırlarının büyük ölçüde önem arz ettiği sonucu ortaya çıkar.GDPR m. 46/1'e göre bir yeterlilik kararı olmadığı takdirde, kişisel verilerin aktarılması yalnızca bir veri sorumlusunun veya veri işleyenin uygun güvenlik önlemlerini sağlaması ve veri sahibinin haklarını yerine getirmesi durumunda

GDPR



gerçekleştirilebilir. GDPR m. 46/2-c ise bunun Komisyon tarafından hazırlanan standart veri koruma hükümleri ile sağlanabileceğini düzenlemiştir^[20]. Dolayısıyla standart sözleşme hükümlerine dayanılarak aktarım yapılması mümkündür. Bununla birlikte Savcılık Görüşü'nün 126. paragrafında da belirtildiği gibi bu aktarım işlemi veri sorumlusunun başarısız olması halinde denetim otoritesinin yetkilerini kabul etmek gerekir. İlgili denetim otoritesi ülkenin yasalarını özellikle standart hükümlerin uygulanmasına herhangi bir engel olup olmadığı bağlamında bir inceleme yapacak ve buna göre bir karar alacaktır^[21].

Bu çerçevede denetim otoritesine tanınmış olan aktarımın yasaklanması veya askıya alınması kararı verilmesinin SSC Kararı ile çelişen herhangi bir tarafı yoktur. Öyleyse SSC Kararı'nın geçerliliği bakımından da herhangi bir sorun olmayacaktır. Nitekim Divan, AB Temel Haklar Şartı'nın 7, 8 ve 47. maddeleri uyarınca yaptığı incelemede SSC Kararı'nın geçerliliğini etkileyecek herhangi bir hususun söz konusu olmadığını belirtmiştir^[22].

v.ABD'nin Mahremiyet Kalkanı Kararı'na^[23] ilişkin dört, beş, dokuz ve onuncu sorular bakımından

Mahkeme, bu sorularla ABD'nin yeterli düzeyde koruma sağladığına dair Mahremiyet Kalkanı Kararı'nı sorgulamıştır ve özellikle bu kararın AB üyesi devletlerin denetim otoriteleri üzerinde ne ölçüde bağlayıcı olduğunu öğrenmek istemiştir. Bu sorular bakımından ABD hukuku ile standart veri koruma hükümleri uyarınca kişisel veri aktarılıp aktarılamayacağı yönünde bir inceleme söz konusudur^[24].

Facebook İrlanda, Mahremiyet Kalkanı Kararı'nın ABD tarafından sağlanan koruma seviyesinin yeterliliğini garanti etmesi bakımından bağlayıcı olduğunu ve bu nedenle de SSC Kararı'nın ekinde yer alan standart veri koruma hükümleri uyarınca yapılan aktarımın yasal olduğunu iddiasındadır^[25].

Divan'a göre, Mahremiyet Kalkanı Kararı'nda yer alan ABD'nin yeterli düzeyde koruma sağladığına dair düzenlemenin bağlayıcı olup olmadığı sorusunun cevaplanması, kişisel verilerin SSC Kararı uyarınca aktarılmasında veri sorumlusu ve alıcısı

tarafından yeterli korumanın sağlanıp sağlanmadığı ile denetim makamının aktarımı yasaklama veya askıya alma gibi yetkilerinin olup olmadığıyla ilgilidir^[26].

Ancak kararın bu kısmını okur ve değerlendirirken şu hususun gözden kaçırılmaması gerekir. Schrems'in yaptığı başvuruların ve bu kararların verilmesinin nedeni ABD'nin istihbarat kuruluşları tarafından her türlü dijital iletişim ve paylaşımın "meta-data"lar yoluyla gözetlenmesidir. Eski Ulusal Güvenlik Ajansı (NSA) çalışanı Edward Snowden'ın ifşaatlarına bakılacak olursa, ABD'nin istihbarat kurumları kendi yaptıkları gözetlemeyle yetinmemekte, hemen hemen tüm büyük bilişim, teknoloji ve sosyal medya şirketleriyle de iş birliği yaparak (ya da iş birliğine zorlayarak) bunların elde ettiği verileri de gözetlemektedir. Buna herhangi bir anlaşma dahilinde ABD'ye aktarılan veriler de dahildir. Zira ABD istihbarat ve güvenlik kurumları, veri bir kez ABD'ye geldikten sonra, ulusal güvenliği gerekçe göstererek verilere sınırsız erişim sağlamakta ve bunu mahkeme denetiminden kaçırmak için de türlü yollara başvurmaktalardır.^[27]

Mahremiyet Kalkanı Kararı denetim otoriteleri için bağlayıcı mı?

Divan, bu sorunun yanıtını "evet" olarak cevaplamıştır. Buna göre Karar'ın 1/1 maddesi ABD'nin aktarılan kişisel veriler için yeterli düzeyde koruma sağladığını düzenler. Ayrıca 1/3 maddesi de kişisel verilerin AB – ABD Mahremiyet Kalkanı kapsamında aktarılmış olarak kabul edildiğini ve bu kapsamda Mahremiyet Kalkanı Listesi'nde yer alan kuruluşlara aktarılabileceğini öngörmüştür^[28].

Avrupa Birliği mevzuatı uyarınca bu Karar, Amerika Birleşik Devletleri'nin yeterli düzeyde koruma sağladığını ve bu nedenle AB-ABD Mahremiyet Kalkanı kapsamında aktarılan kişisel verileri onaylama etkisine sahip olduğunu düzenlemiş olduğundan, geçersiz ilan edilene kadar Üye Devletler için ve dolayısıyla bu devletlerin denetim otoriteleri için bağlayıcıdır. Öyleyse Üye Devletler ve organları bu karara aykırı tedbirler alamaz ve aktarımı yasaklayamaz^[29].

Bir şikayet halinde durum ne olacaktır?

Mahremiyet Kalkanı Kararı, bağlayıcı olmakla birlikte bir kişi denetim makamına şikayette bulunduğu, söz konusu makam, kişisel

verilerin transferinin GDPR tarafından belirlenen şartlara uygun olup olmadığını incelemelidir. Bu kararın geçerliliğine ilişkin itirazları bulunan kişinin itiraz gerekçelerinin sağlam olması halinde bir ön karar için ulusal mahkemeler nezdindeki haklarını da kullanmaları mümkündür. Divan'a göre şikayete konu olan ülkenin kanun ve uygulamalarının yeterli düzeyde koruma sağlamadığının anlaşılması, aslında söz konusu kararın kişilerin özel hayatının ve kişilerin temel hak ve özgürlüklerinin korunmasına uygun olup olmadığı ile ilgili olarak anlaşılmalıdır^[30].

Mevcut davada da Schrems, denetim otoritesinden üçüncü bir ülkenin yeterli düzeyde koruma sağlamadığı gerekçesiyle, kişisel verilerinin Facebook İrlanda tarafından ABD'de kurulan Facebook Inc.'e aktarılmasının yasaklanmasını veya askıya alınmasını talep etmiştir. Soruşturmayı yürüten denetim otoritesi konuyu ulusal mahkemenin önüne taşımıştır. Bu çerçevede Divan'ın önüne gelen sorular Mahremiyet Kalkanı Kararı'nın yeterli korumayı sağladığına dair geçerliliğini sorgulamayı gerektirmiş

olup; bunun tespit edilebilmesi için kararın GDPR gerekliliklerine uygun olup olmadığının incelenmesi gerekir^[31]

Mahremiyet Kalkanı Kararı ne diyor?

- ABD, AB – ABD Mahremiyet Kalkanı kapsamında aktarılan kişisel verilere ilişkin olarak yeterli düzeyde koruma sağlar (m. 1/1).
- ABD Ticaret Bakanlığı tarafından yayımlanan ilkeler kararın ekinde yer almaktadır.
- AB- ABD Mahremiyet Kalkanı Çerçeve İlkeleri, ulusal güvenlik, kamu yararı veya yasa uygulamalarının gerektirdiği ölçüde sınırlandırılabilir. (Para.1.5–EK II).
- Dolayısıyla buna göre belirlenen istisnalar söz konusu ilkelere göre önceliğe sahip bir şekilde düzenlenmiştir ve bu kapsamda, AB'den kişisel verileri alan ve kendi kendini yeterli korumaya sahip olduğuna ilişkin olarak onaylayan bir kuruluş, gereksinimlerle çalıştığını düşündüğünde herhangi bir sınırlama olmaksızın ilkeleri göz ardı edilebilecektir
- Bu çerçevede gerçekleştirilebilecek bir müdahaleye olanak tanınmıştır^[32].

Bu kapsamda yeterli bir korumadan bahsedilebilir mi?

Divan, Mahremiyet Kalkanı Kararı'nın geçerliliğinin tespit edilebilmesi için GDPR ilkelerine olan uygunluğunu denetlerken öncelikle kişisel verilerin AB Temel Haklar Şartı ve GDPR düzenlemelerindeki yerini açıklamıştır. Bu çerçevede özellikle kişisel verilerin işlenmesine ilişkin istisnalara ve hakkın hangi hallerde sınırlandırılabilceğine değinmiştir. Bu noktada Divan'ın yaptığı teorik açıklamalara atıf yapmakla yetinerek bu açıklamaları somut olaya ilişkin olarak ele almaya çalışacağım^[33].

Mevcut durumda ABD, temel olarak kişisel veriler için GDPR tarafından garanti edilenle eşdeğer düzeyde bir koruma sağladığı iddiasındadır. Ancak Divan, özellikle "Yabancı İstihbarat İzleme Yasası (Foreign Intelligence Surveillance Act – FISA)" kapsamında yaptığı incelemede burada yer alan hükümlere dayalı olarak kullanılan gözetim programlarından kaynaklanan müdahalelerin GDPR gereksinimlerini ve özellikle orantılılık ilkesini karşılamadığı görüşündedir. Öyle ki, bireylerin yabancı istihbarat bilgileri edinmeye uygun bir şekilde

hedeflenip hedeflenmediğini kontrol edecek bir denetim mekanizması da öngörülmemiştir. Bu da gözetim uygulamaları çerçevesinde yapılacak müdahalede herhangi bir sınırlamaya gidilmediğinin göstergesidir^[34].

Nitekim aynı husus Savcılık Görüşü'nde de dile getirilmiştir. Savcı, Şart'ın özel hayatın ve kişisel verilerin korunmasına ilişkin 7. ve 8. maddeleri kapsamında güvence altına alınan hakların kullanımına yönelik herhangi bir müdahalenin özellikle orantılılık ilkesi bakımından incelenmesi gerektiği düşüncesindedir. Buna göre kişisel verilerin herhangi bir ayırım, sınırlama veya istisna olmaksızın ve nesnel kriterler belirlenmeksizin kamu makamlarının erişimine ve kullanımına açık olması ve kullanım amaçlarının sınırlandırılmamış olması yeterli güvencelerin varlığının sorgulanmasına neden olmalıdır^[35].

Bunun yanında Divan, gözetim yasalarından kaynaklanan müdahalelere ilişkin olarak ABD makamlarının dava edilebilmesine yönelik hakların da verilmemiş olduğunu tespit etmiştir. Bu nedenle Mahremiyet Kalkanı Kararı'nın esas

olarak Şart'tan kaynaklanan koruma düzeyi ile GDPR m. 45/2-a ile düzenlenmiş olan kişisel verileri üçüncü bir ülkeye aktarılmakta olan veri sahiplerinin etkin ve uygulanabilir haklara sahip olması gerektiği koşullarını sağlayabilmesi mümkün değildir^[36].

Bu çerçevede, ABD mevzuatına dayanan gözetim programları aracılığıyla gerçekleştirilen müdahaleler, AB hukuku kapsamında sağlanması gereken orantılılık ilkesi çerçevesinde değerlendirildiğinde "gerekli olanla sınırlı" olarak nitelendirilememektedir. İkinci olarak, Şart'ın 47. maddesi uyarınca AB hukuku tarafından güvence altına alınan hakları ve özgürlükleri ihlal edilen herkesin, o maddede belirtilen şartlara uygun olarak bir mahkeme önünde etkili bir hukuk yoluna başvurma hakkına sahip olması gerekir. Buna göre herkesin bağımsız ve tarafsız bir mahkemeye başvurma hakkı vardır. Divan'a göre bir bireye kendisiyle ilgili kişisel verilere erişmek veya bu tür verilerin düzeltilmesini veya silinmesini sağlamak için yasal yollara başvurma imkânı sağlamayan yasalar, temel hakkın özüne saygı göstermez^[37].

Sonuç olarak, her ne kadar Mahremiyet Kalkanı Kararı'nın 1. maddesinde ABD'nin AB – ABD Mahremiyet Kalkanı kapsamında yeterli düzeyde koruma sağladığı belirtilmiş olsa da, Divan bu kararın Şart'ın 7, 8 ve 47. maddeleri ile GDPR m. 45 gereklerini sağlamadığı görüşündedir. Dolayısıyla Karar'ın bu gerekleri sağladığını içeren 1. maddesi geçersizdir. Dahası Mahremiyet Kalkanı Kararı'nın 1. maddesi, bu kararın 2. ve 6. maddeleri ile eklerinden ayrılmaz olduğundan, bu maddenin geçersizliği, kararın bütünüyle geçerliliğini etkiler. Divan, yukarıda belirtilen tüm hususların ışığında, Mahremiyet Kalkanı Kararı'nın geçersiz olduğu sonucuna varmıştır^[38].

Mahremiyet Kalkanı Kararı'nın geçersizliğine ilişkin kararda hali hazırda aktarılmakta olan veriler için herhangi bir geçiş süresi öngörülüş müdür?

Divan, herhangi bir geçiş süresi öngörmemiştir. Dolayısıyla söz konusu geçersizlik kararının üzerinde, hali hazırda Mahremiyet Kalkanı Kararı uyarınca aktarılmakta olan veriler artık hukuka aykırı bir aktarımın konusunu oluşturur. Dolayısıyla bu

aktarıma devam etmek için Divan tarafından açıklanan koruma seviyesinin sağlanması gerekir^[39].

Mahremiyet Kalkanı Kararı'nın geçersizliği, diğer aktarım yöntemlerini de etkiler mi?

Bu sorunun cevabının “evet, etkiler” olması gerekir. Zira Divan tarafından verilen geçersizlik kararı aslında ABD'nin ulusal mevzuatı ile AB hukuku arasındaki uyumsuzluğa dayanmaktadır. Dolayısıyla kullanılan aktarım yöntemi her ne olursa olsun bu veriler ABD mevzuatı uyarınca AB hukukunun gerekliliklerine uygun bir biçimde korunamadığı sonucu çıkar. Bu durumda, verilen kararın yalnızca Mahremiyet Kalkanı Kararı'nın geçersizliği şeklinde okunmaması gerekir. Burada çok daha derin bir şekilde ABD ulusal mevzuatına ilişkin problemler yatmaktadır. Hal böyle iken söz konusu geçerlilik kararının ABD'ye veri aktarımını sağlayan diğer aktarım yöntemlerini de etkilemesi gerekir. Nitekim Avrupa Veri Koruma Kurulu tarafından Schrems II kararıyla ilgili olarak sıkça sorulan soruları cevaplamak üzere yayımlanan dokümanda da Divan tarafından açıklanan

veri koruma eşiğinin GDPR'ın 46. maddesi kapsamındaki tüm yöntemler için geçerli olduğu ve dolayısıyla bu geçersizlik kararının ABD'ye yapılan herhangi bir veri aktarımını da etkileyeceği belirtilmiştir^[40].

Temel problem ABD'nin ulusal mevzuatı ise ABD'ye SSC Kararı uyarınca gerçekleştirilen bir aktarımın da geçersiz olduğu söylenebilir mi?

Bunu kesin bir şekilde kabul etmenin zor olacağını düşünmekteyim. Her ne kadar Divan temel problemin ABD'nin ulusal mevzuatından kaynaklandığı tespitinde olsa da ABD'ye SSC Kararı uyarınca yapılan bir aktarımın hukuka uygunluğunu değerlendirmek için belirlenmiş olan standart sözleşme hükümlerinin incelenmesi ve bu bağlamda bir karar verilmesi gerekir. Somut olayda tüm aktarım koşullarının dikkate alınarak ulusal mevzuata ek güvencelerin sağlandığı söylenebilmekteyse bu aktarımın hukuka uygun olduğu sonucu çıkabilir. Dolayısıyla bu konuda kesin bir sınırın çizilmemesi ve ancak somut aktarımda alınan ek güvencelerin incelenmesiyle bir karar verilmesi gerektiğini düşünüyorum.

Avrupa Veri Koruma Kurulu da bu hususla ilgili olarak aktarım koşulları ile ek güvenceler değerlendirildiğinde yeterli korumanın sağlanamadığı sonucuna varılırsa bu aktarımın askıya alınması veya yasaklanması gerektiği görüşündedir^[41].

ABD'de yer alan bir şirket için Bağlayıcı Şirket Kuralları uyarınca yapılan aktarımın geçerliliği ne olacaktır?

Bu sorunun cevabı da yukarıda yer alan soruyla benzer biçimde cevaplanmalıdır. Yukarıda belirtmiş olduğum gibi Mahremiyet Kalkanı Kararı geçersizdir, çünkü ABD yasaları üçüncü bir ülkeye kişisel verileri aktarılan gerçek kişilerin temel hak ve özgürlüklerine sınırsız bir biçimde müdahale etmektedir. Öyleyse Bağlayıcı Şirket Kuralları uyarınca yapılan aktarımda da bu problem devam eder. Dolayısıyla bu durumda da Bağlayıcı Şirket Kuralları çerçevesinde alınan ek önlemlerin değerlendirilmesi gerekecektir.

Avrupa Veri Koruma Kurulu, bu açıdan da aktarım koşulları ile ek güvenceler değerlendirildiğinde yeterli korumanın sağlanamadığı sonucuna varılırsa Bağlayıcı Şirket Kuralları uyarınca

gerçekleştirilen aktarımın askıya alınması veya yasaklanması gerektiği görüşündedir^[42].

Peki ABD'ye hiçbir şekilde veri aktarımı yapılamayacak mı?

Divan tarafından verilen geçersizlik kararı her ne kadar ABD'ye yapılan tüm aktarımları etkileyecek şekilde gerekçelere dayansa da; bu karar neticesinde hiçbir şekilde ABD'ye veri aktarımı yapılamayacağını söylemek doğru olmayacağı gibi uygulama açısından da gerçekçi olmayacaktır. İlk olarak GDPR'ın 49. maddesi^[43] hala yürürlüktedir ve bu maddeye istisnaden veri aktarmak hala mümkündür^[44]. Örneğin, ilgili kişinin rızası, ilgili kişinin yararına yapılan bir sözleşmenin imzalanması ve yürütülmesi gibi amaçlarla yapılan veri aktarımı 49. madde kapsamında hala geçerli olacaktır. Ancak bu maddenin uygulamadaki yerinin çok sınırlı olduğunu unutmamak gerekir. Dolayısıyla ekonomik aktörler arasında ticari amaçlarla gerçekleştirilecek olan aktarım sorununu anılan maddenin çözmesi hala mümkün değildir.

Öyleyse ilk olarak GDPR'ın 49. maddesi uyarınca çeşitli somut durumlarla özgü olarak ABD'ye hukuka

uygun olarak veri aktarımı yapılabilir. Ancak Divan'ın söz konusu geçersizlik kararı üzerine ABD'de yer alan ekonomik aktörlere ticari amaçlarla yapılacak olan aktarımın geçerli olması için ABD ulusal mevzuatında ciddi değişimlerin yapılması gerekir.

■ Sonuç olarak;

Divan tarafından kendisine sorulan sorulara karşılık varılan temel kanaatler şu şekildedir^[45]:

- GDPR m. 2/1 ve m. 2/2, kişisel verilerin bir AB üyesi devlette yerleşik bir ekonomik aktörü tarafından üçüncü bir ülkede yerleşik başka bir ekonomik aktöre ticari amaçlarla aktarılmasına uygulanır. Kişisel verilerin söz konusu üçüncü ülke yetkilileri tarafından kamu güvenliği, savunma veya devlet güvenliği amaçlarıyla işlenmesi bu durumu değiştirmez.
- GDPR m. 46/1 ve m. 46/2-c ile Temel Haklar Şartı, kişisel verileri standart veri koruma hükümlerine göre kişisel verileri üçüncü bir ülkeye aktarılan veri sahipleri için uygun güvenceler, uygulanabilir haklar ve etkili yasal çözümler öngörmüştür. Bu nedenle böyle bir aktarım bağlamında sağlanan veri koruma seviyesinin değerlendirilmesinde AB'de yerleşik veri sorumlusu veya işleyici arasında sağlanan sözleşme maddeleri, söz konusu üçüncü ülkede yer alan veri alıcısı, üçüncü ülkenin kamu makamlarının verilere olan erişimi ve hukuk sistemi de ele alınmalıdır.
- GDPR m. 58/2-f, j bentlerine göre, her ne kadar geçerli bir yeterlilik kararı olmadığı takdirde kişisel verilerin standart sözleşme hükümleri doğrultusunda aktarılması mümkünse de bu aktarımın tüm koşulları ışığında söz konusu üçüncü ülkede AB hukukunun gerektirdiği koruma seviyesi sağlanmadıkça yetkili denetim makamının veri aktarımını askıya alma veya yasaklama hakkı vardır.
- SSC Kararı'nın geçerliliğine ilişkin olarak, Temel Haklar Şartı'nın 7, 8 ve 47. maddelerinde bu kararın geçerliliğini etkileyecek hiçbir husus tespit edilememiştir.
- Mahremiyet Kalkanı Kararı geçersizdir, çünkü ABD yasaları üçüncü bir ülkeye kişisel verileri aktarılan gerçek kişilerin temel hak ve özgürlüklerine sınırsız bir biçimde müdahale etmektedir.

SONUÇ

ABAD'ın Schrems II kararına özel olarak ulaşılan sonuçlar ve sorulması gereken bazı sorular yukarıda ele alındı. Bunun haricinde konuya kişisel verilerin korunması hakkı ve bu hakka ilişkin ilke ve prensipler perspektifinden, ancak ülkeler arasındaki ticari amaçlarla yapılan aktarımın mecburiyetini de göz ardı etmeden yurt dışına veri aktarım sorununa bakmak gerekir. Kişisel verilerin yurt dışına aktarılması ülkemizde olduğu kadar diğer ülkelerde de büyük bir sorundur. Her ülke kendi topraklarında yaşayan kişilere ait verilerin değerinin önemine varmış ve bunların ancak belirli sıkı şartlar dahilinde aktarılmasına ve işlenmesine izin verir hale gelmiştir. Bu durum ise ister istemez büyük sorunların ortaya çıkmasına neden olmaktadır. Zira ABD ile AB üyesi ülkeler arasında kişisel verilerin kaydedilmesi, işlenmesi ve aktarılması konusunda derin bir felsefi bakış açısı farklılığı bulunur. ABD, bu verileri ticari bir meta, bir eşya olarak görüp sektörel bazı kısıtlamalara giderken, AB ve üye ülkeler bunu bir insan hakkı süjesi olarak görmekte ve bu alana ilişkin genel düzenlemelere yer vermektedir.

İşte ABD'nin bu bakış açısı ABD'ye ve burada yer alan şirketlere aktarılan verilerin ABD istihbarat ve güvenlik kurumları tarafından da işlenmesine olanak sağlamaktadır. Bu ABD hukuku açısından meşru bir durum iken AB hukukuna göre hukuka aykırıdır. Mahremiyet Kalkanı Kararı da bu uyumsuzluğu aşmak için çıkarılmıştır. Ancak ABAD'ın vermiş olduğu karar ile Mahremiyet Kalkanı Kararı geçersiz hale gelmiştir. Dolayısıyla bu Karar dayanılarak AB'den ABD'ye veri aktarımı artık mümkün değildir. ABAD, bunun çözümü için SCC'yi göstermiştir.

Her ne kadar SCC tam olarak veri mahremiyetini sağlayamasa da, Mahremiyet Kalkanı Kararı ile getirilen rejime göre tarafları daha bağlayıcı ve daha sıkı şartlar içermektedir. AB ile ABD arasında veri aktarımı yapan şirketlerin, işleyişlerini buna göre dizayn etmesi gerekir.

Ancak açıkça ifade etmeliyim ki, hem ülkemizde hem de AB'de yakın ve orta gelecekte, bu konuda daha çok düzenleme yapılması ve kararlar verilmesi kuvvetle muhtemeldir. Bu konuda son sözün söylenmesinin ve bir uygulama birliğinin sağlanmasının önünde daha çok uzun bir zaman bulunmaktadır. ■

DİPNOTLAR

- [1] Kararın tamamı için bkz: shorturl.at/crzP5
- [2] shorturl.at/jpzNQ
- [3] Avrupa Birliği Adalet Divanı'nın ön karar sistemine ilişkin detaylı için bkz: shorturl.at/dhijk
- [4] Savcılık Görüşü'nün tam metni için bkz: shorturl.at/pszB1
- [5] Avrupa Birliği Adalet Divanı, 24 Eylül 2019, C-507/17, EU:C:2019:772; shorturl.at/uKQRW
- [6] Para, 81.
- [7] Para 82-84.
- [8] Para, 85-88.
- [9] Para. 90.
- [10] Para 91-93.
- [11] Para 94.
- [12] Para 95, 96.
- [13] Para. 98-100.
- [14] Para 101.
- [15] Para. 107, 108.
- [16] Para. 109 -114.
- [17] Para 120, 121.
- [18] European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 Temmuz 2020, s. 1.
- [19] Para. 124 – 127.
- [20] Para. 128.
- [21] Para. 134, 146.
- [22] Para. 148, 149.
- [23] shorturl.at/qDJ36

- [24] Para. 150.
- [25] Para. 152.
- [26] Para. 154.
- [27] Bu konuda bkz: Edward Snowden, Sistem Hatası,
- [28] Para. 155.
- [29] Para. 156, 157.
- [30] Para. 158.
- [31] Para. 159 – 162.
- [32] Para. 163 – 167.
- [33] Divan'ın konuyla ilgili açıklaması için bkz: 168, 177.
- [34] Para. 178 – 180.
- [35] Savcılık Görüşü, para. 291 – 297.
- [36] Para. 181.
- [37] Para. 183 – 187.
- [38] Para. 198 – 201.
- [39] EDPB, s. 2.
- [40] EDPB, s. 2.
- [41] EDPB, s. 3.
- [42] EDPB, s. 3.
- [43] GDPR'ın 49. Maddesiyle ilgili detaylı için bkz: European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 Mayıs 2018.
- [44] EDPB, s. 4.
- [45] Para. 203.