Schrems II, beş yıl sonra

Kişisel verilerin uluslararası aktarımı hukukunu değiştiren karar. Beş yıl sonra, Avrupa'nın günlük ofis işlerinin önemli bir kısmı sanki hiçbir şey olmamış gibi işlemeye devam ediyor.

Kuralları değiştirmesi üç saat süren karar

16 Temmuz 2020'de, Lüksemburg saatiyle sabah on buçuk sularında, Avrupa Birliği Adalet Divanı C-311/18 davasındaki kararını açıkladı. Takip eden üç saat içinde, Avrupa'dan Amerika Birleşik Devletleri'ne günlük kişisel veri aktarımını destekleyen yasal rejim —resmi adıyla Privacy Shield, yani Gizlilik Kalkanı— sona erdi. Avrupalı veri koruma görevlileri o gün öğle yemeklerini bitirdiklerinde, şirketlerinin ve idarelerinin faaliyet gösterdiği çerçeve artık geçerli değildi.

Karar bugün, Facebook Ireland aleyhindeki şikayetiyle süreci başlatan Avusturyalı aktivist Maximilian Schrems'in adıyla Schrems II olarak biliniyor. Şikayet, somut olarak Facebook İrlanda ile Facebook ABD arasındaki aktarımlarla ilgiliydi. Karar, genel olarak çok daha ileri gidiyor: Avrupa topraklarında toplanan herhangi bir kişisel verinin ABD'ye nasıl ve hangi koşullar altında geçebileceğini dikte ediyor.

Neredeyse altı yıl sonra, yerine geçen çerçeve mevcut —Temmuz 2023'te kabul edilen EU-US Data Privacy Framework— ve o da hukuki baskı altında. Yeni bir Schrems turu hazırlanıyor. Bu sırada, küçük ve orta ölçekli Avrupalı şirketler günlük işler için bulut hizmetlerini kullanmaya devam ediyor, çoğunlukla bu hizmetlerin dayandığı hukuki sorunun hala açık olduğunu bilmeden.

Schrems II tam olarak ne diyordu

Karar üç parça üzerinde duruyor. Birincisi, Avrupa Birliği Temel Haklar Şartı, özellikle 7. (özel ve aile hayatı), 8. (kişisel verilerin korunması) ve 47. (etkili yargısal koruma) maddeleri. İkincisi, Genel Veri Koruma Yönetmeliği —birçok Avrupalının sadece çerez uyarılarından hatırladığı GDPR—, özellikle uluslararası aktarımlarla ilgili V. Bölüm, 44 ila 50. maddeler. Üçüncüsü, ABD istihbarat mevzuatı: Foreign Intelligence Surveillance Act'in 702. bölümü, hukuk dilinde FISA 702 ve 12333 sayılı Başkanlık Kararnamesi.

Mahkeme kıyaslama yoluyla ilerledi. Temel Haklar Şartı, Avrupalı vatandaşların kişisel verilerinin Birlik dışına çıktıklarında, GDPR tarafından garanti edilen düzeye esasen eşdeğer bir koruma düzeyinden yararlanmasını gerektirir. Sonuç olarak soru, ABD'nin bu esasen eşdeğer düzeyi sunup sunmadığıydı.

Yanıt olumsuzdu ve bu sadece nüanslardan kaynaklanmıyordu. FISA 702, ABD hükümetine, ulusal topraklar dışındaki ABD vatandaşı olmayanların iletişimlerini önceden bireysel adli izin almadan, etkilenen kişiye bildirimde bulunmadan ve Avrupa ile kıyaslanabilir etkili bir başvuru yolu olmadan toplama izni veriyor. 12333 sayılı Başkanlık Kararnamesi bu yetkiyi ulusal topraklar dışında benzer şekilde genişletiyor. Mahkeme, Avrupalı vatandaşın ABD hukuk sistemi karşısında Şart'ın gerektirdiği esasen eşdeğer korumaya sahip olmadığı sonucuna vardı. Bu nedenle eşdeğerlik mevcut değildir.

Bunun doğrudan sonucu olarak: Privacy Shield'ı aktarımlar için uygun bir çerçeve olarak onaylamış olan Avrupa Komisyonu'nun 2016/1250 sayılı Kararı geçersiz ilan edildi. Sadece bu çerçeveye dayanan tüm aktarımlar o

andan itibaren hukuki dayanaktan yoksun kaldı.

Hayatta kalanlar (ve hangi koşullar altında)

Schrems II tüm araçları ortadan kaldırmadı. Standart Sözleşme Maddeleri —İngilizce kısaltmasıyla SCC (Standard Contractual Clauses)— hayatta kaldı. Bunlar Avrupa Komisyonu tarafından onaylanmış model sözleşmelerdir: bir Avrupalı ihracatçı ve hedef ülkedeki bir ithalatçı, verileri Avrupa standartlarına göre işlemeyi taahhüt ederek bunları imzalar. Sorunu 17 Temmuz 2020'de çözdüğünü düşünen şirket, sağlayıcısıyla SCC imzaladı ve halinden memnun oldu.

Rahatsızlık karar yavaş yavaş okunduğunda geldi. Mahkeme, SCC'lerin hala geçerli olduğunu açıkça belirtti, ancak geçerlilikleri vurgulanması gereken bir koşula bağlıdır: veri ithalatçısının bunları pratikte yerine getirebilmesi. Hedef ülkenin ulusal mevzuatı maddeleri yerine getirmesini engelliyorsa —örneğin, FISA 702 kapsamındaki bir emir onu Avrupalı muhatabına bildirmeden verileri teslim etmeye zorluyorsa— maddeler gerçekte koruma sağlamaz. Ve o zaman, der mahkeme, Avrupalı ihracatçı aktarımı askıya almalıdır.

Bu durum, Avrupa veri koruma uygulamasına yeni bir nesne getirdi: İngilizce kısaltması TIA ile bilinen Transfer Impact Assessment, yani aktarım etki analizi. Avrupalı bir şirket SCC himayesinde ABD'ye veri taşımak istediğinde, alıcının kendisine uygulanan mevzuat göz önüne alındığında maddelere uyup uyamayacağını resmen değerlendirmelidir. Avrupa Veri Koruma Kurulu (EDPB), TIA'nın nasıl yürütüleceğine dair ayrıntılı kılavuzlar yayımladı. Dürüst uygulama genellikle aynı sonucu verir: ithalatçı bir bulut devinin ABD'deki iştiraki ise, TIA'ya verilecek samimi yanıt, maddelerin yazıldığı şekliyle yerine getirilemeyeceğidir.

Privacy Framework ve beklenen Schrems III

10 Temmuz 2023'te Avrupa Komisyonu yeni bir Uygunluk Kararı kabul etti: 2023/1795. Bu karar, yürürlükten kalkan Privacy Shield'ın yerini aldı ve EU-US Data Privacy Framework adı altında faaliyet gösteriyor. Amerika Birleşik Devletleri daha önce, sinyal istihbaratının kapsamını «gerekli ve orantılı» —Avrupalı okuyucu için tanıdık, ancak ABD idari uygulaması için pek öyle olmayan bir terminoloji— olanla sınırlayan 14086 sayılı Başkanlık Kararnamesi (Executive Order) ile iç rejimini değiştirmiş ve Data Protection Review Court (DPRC) adlı bir inceleme organı oluşturmuştu. Komisyon, bu değişikliklerin esasen eşdeğer düzeyde korumayı geri getirmek için yeterli olduğunu düşündü.

Schrems tarafından kurulan noyb kuruluşu, 7 Eylül 2023'te yeni Karara karşı bir şikayette bulundu. Argümanlar beklendiği gibidir: DPRC, Şart'ın 47. maddesi anlamında bağımsız bir mahkeme değildir; «gerekli ve orantılı» kavramları Avrupa standartlarını mekanik olarak karşılamaz; ve son olarak, bir Başkanlık Kararnamesine dayanan bir koruma, bir sonraki Başkanlık Kararnamesi ile iptal edilebilir. CJEU'nun yeni Karar hakkındaki kararı —birçok kişinin şimdiden bir miktar tevekkülle Schrems III olarak adlandırdığı karar— önümüzdeki yıllarda bekleniyor. Sonuç tahmin edilemez. Her halükarda argümanın yapısı 2020'dekini çok andırıyor.

Avrupalı KOBİ'lerin duymadıkları

CJEU'nun büyük dairesi müzakere ederken, orta ölçekli hukuk bürosu Avrupa bölgelerinde barındırılan ancak FISA 702'ye tabi bir ABD şirketine ait olan Microsoft 365 aracılığıyla müşterileriyle yazışmaya devam ediyor. Özel muayenehane ajandalarını Google Workspace üzerinden senkronize ediyor. Veri danışmanı DocuSign aracılığıyla imzalı beyannameler gönderiyor. Psikolog Notion'daki bir tablodan fatura kesiyor. İş hukuku bürosu dosyaları Dropbox'ta arşivliyor. Ve hemen hemen hepsi müşterilerine WhatsApp üzerinden hizmet veriyor. Sağlayıcılara göre tüm bunlar 2023/1795 Uygunluk Kararı himayesinde yürütülebilir. Bu Kararın Schrems III ile düştüğü gün, tüm bu ilişkiler aynı saniyede korumasız kalır.

Konu retorik değildir. 2022 ile 2024 yılları arasında, birkaç Avrupa otoritesi, Privacy Framework yürürlüğe girmeden önce bile CJEU'nun akıl yürütmesini harfiyen uygulayarak, uygun bir aktarım aracı olmadan Google

Analytics kullandıkları için veri sorumluları aleyhindeki dosyaları karara bağladı. Fransız otoritesi CNIL, 2022'de kriteri resmileştiren ilk kurum oldu; Avusturya, İtalya ve diğer otoriteler kısa süre sonra onu izledi. Avrupalı KOBİ'lerin mevcut operasyonel tasarımı altındaki uyumsuzluk, nereye bakacağını bilen biri için gerçek zamanlı olarak belgelenmektedir.

Bir ritüel olarak değil, bir araç olarak TIA

Avrupa ofislerinde dolaşan TIA'ların önemli bir kısmı, dikkatle okunduğunda, biçimsel egzersizlerdir. Sözleşme araçlarını listelerler, sağlayıcının sertifikalarını sayarlar, teknik garantileri zikrederler, kutuyu işaretlerler. Çok azı bir FISA 702 emrinin sağlayıcıyı verileri teslim etmeye zorlayıp zorlamayacağını ciddi olarak sorar. Daha da azı, Privacy Framework'ün varsayımsal bir revizyonu altında bu aktarıma ne olacağını sorar. GDPR'nin 5. maddesi, veri sorumlusunun uyumu kanıtlayabilmesini gerektirir. Ciddiyetle yapılmayan bir TIA hiçbir şeyi kanıtlamaz; kanıtladığı şey, pratikte tam tersi yapılırken kağıt üzerinde uyma isteğidir.

TIA'nın samimi versiyonu basit bir soruyla başlar: Yarın bu sağlayıcıya bu belirli veriler hakkında bir FISA 702 emri gelse ne olurdu? Eğer dürüst yanıt «bize haber vermeden verileri teslim etmek zorunda kalırdı» ise, sözleşme maddeleri sorunu çözmez. Sorunun gerçekten önemli olduğu durumlarda bunu çözen şey, veriyi o sağlayıcının ellerine bırakmamış olmaktır.

Yapısal bir risk olarak siyasi değişim

Dramatize etmeden isimlendirilmesi gereken ek bir siyasi katman var. 2023/1795 Uygunluk Kararı, nihayetinde Başkan Biden tarafından Ekim 2022'de imzalanan 14086 sayılı Başkanlık Kararnamesine dayanmaktadır. Bir Başkanlık Kararnamesini bir başkan imzalar ve bir sonraki başkan iptal edebilir, değiştirebilir veya içeriğini boşaltabilir. ABD'deki Avrupa verilerinin korunması, bu nedenle ne Amerikan Kongresi'nin garanti ettiği ne de Amerikan hukuk sisteminin diğer iç meseleleri koruduğu sağlamlıkla koruduğu idari bir karara bağlıdır. Ocak 2025'ten bu yana ABD'yi yeni bir yönetim yönetiyor ve EO 14086'nın pratik sürekliliği hakkındaki soru bir hipotez olmaktan çıkıp güncel hale geldi. Yönetimin Kararnameyi geri çekmeye veya yumuşatmaya karar vereceği herhangi bir senaryo, Avrupa Kararını üzerine inşa edildiği parçadan yoksun bırakacaktır.

Bu komplo temelli bir argüman değil. Hukuki tasarımın ölçülü bir okumasıdır. Transatlantik veri koruma çerçeveleri daha önce iki kez düştü: 2015'te Safe Harbor (Schrems I kararı), 2020'de Privacy Shield (Schrems II). Üçüncüsü, öncekilerden daha kırılgan bir parça üzerinde duruyor. Bugün veri işlemesini bu parçaya yatıran bir Avrupalı şirket, sadece bir mevzuat uyumu kararı değil, bir risk yönetimi kararı almaktadır.

Profesyonel okuyucu için

Profesyonel veriler için bir bulut hizmeti seçmeden önce sorulması gereken operasyonel sorular —bir veri koruma müfettişinin soracağı titizlikle— şunlardır:

1. Veriler fiziksel olarak nerede saklanıyor? Operatör ABD'li ise bir Avrupa bölgesi yeterli bir cevap değildir.
2. Hizmeti kim işletiyor, hangi yargı yetkisine bağlı ve hangi yasal emirlere tabi tutulabilir?
3. Hangi aktarım aracı öne sürülüyor: 2023/1795 Uygunluk Kararı, TIA ile birlikte SCC, GDPR'nin 49. maddesi kapsamındaki muafiyet mi? Bu seçim bir denetim karşısında savunulabilir mi?
4. Uygunluk Kararı yarın düşerse, faaliyeti sürdürmek için hangi operasyonel plan mevcut?
5. Bu işlev için Avrupa menşeli veya kendi kendine barındırılan bir alternatif var mı ve geçişin gerçek maliyeti ne olur?

Günlük ofisin tüm işlevleri aynı yanıtı gerektirmez. Dahili muhasebe için bir tablo muhtemelen soruyu bu seviyeye taşımaz. Bir müşterinin ceza dosyası, tıbbi geçmişi, çalışanların maaş bordrosu ise taşır. Orantılılık meşrudur; Avrupalı KOBİ'lerin her şey için —en hassas olanlar için bile— ABD'li sağlayıcılarda kalmış olması şeklindeki kolektif atalet ise değildir.

Schrems II bu Temmuz'da altı yaşına giriyor. Karar, çoğu Avrupalı şirketin günlük alışkanlıklarını değiştirmedi. Ancak, bu şirketlerin maruz kaldığı risk haritasını kesinlikle değiştirdi. Bir ABD idari kararı, Avrupa yönetmeliği ile bir KOBİ'nin gerçek operasyonu arasına girdiğinde, en azından bu kararın orada olduğunu ve kırılgan olduğunu bilmek gerekir. Arada bir operatör olmayan bir mimariyi seçen bizler —Cuadernos Lacre boyunca uzanan hat— her bir Schrems itiraz etmek için oturduğunda bu tür analizler yazmak zorunda kalmamayı tercih ederdik. Ancak bunları yapmaya devam edeceğiz.

Kaynaklar ve ek okumalar

- Avrupa Birliği Adalet Divanı — 16 Temmuz 2020 tarihli karar, C-311/18 sayılı dava, *Data Protection Commissioner v Facebook Ireland Ltd ve Maximillian Schrems*.
- (AB) 2016/679 Sayılı Yönetmelik, V. Bölüm, 44 ila 50. maddeler — kişisel verilerin uluslararası aktarımı.
- Komisyonun 10 Temmuz 2023 tarihli (AB) 2023/1795 Sayılı Uygulama Kararı, EU-US Data Privacy Framework kapsamında kişisel verilerin korunmasının uygun düzeyi hakkında.
- Avrupa Veri Koruma Kurulu — *AB kişisel veri koruma düzeyine uyumu sağlamak için aktarım araçlarını tamamlayan önlemler hakkında 01/2020 Sayılı Tavsiyeler*, 18 Haziran 2021'de kabul edilmiştir.
- noyb.eu — 7 Eylül 2023'te (AB) 2023/1795 Sayılı Karara karşı Avrupa veri koruma makamlarına sunulan şikayet.
- *Foreign Intelligence Surveillance Act*, 702. bölüm (50 U.S.C. § 1881a olarak kodlanmıştır) ve ABD'nin ulusal topraklar dışındaki istihbarat faaliyetleri hakkındaki 12333 sayılı Başkanlık Kararnamesi.

← ÖncekiArada kimse olmadığındaSonraki → SHA-256 Gerçekte Nedir

Son okumalar

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Bu makaleyi ihtiyacınız olan her yere yanınızda götürün.

↓ Markdown ↓ Düz metin ↓ PDF

Dosya cihazınıza indirilecektir. Oradan kaydedebilir, Solo2'ye aktarabilir veya istediğiniz yerde paylaşabilirsiniz. Cuadernos hedef noktaya sizin yerinize karar vermez.

Mühür mumu · SHA-256 e4d47ef773f746b86874452d940bd72292fe33676f4c431621e7e90ab2c2a825

Cuadernos Lacre · Menzuri Gestión S.L. yayını ·
R.Eugenio tarafından yazıldı · Solo2 ekibi tarafından düzenlendi.