Dünyada Neler Oluyor?

Veri Koruma alanı ülkemizde ivme kazanan bir hızla gelişirken, dünya çapındaki yenilikler Kişisel Verileri Koruma Kurumu'nun ("Kurum") radarında kalmaya devam ediyor.

Daha önce defaten karşılaştığımız örneklerden Kurum'un Avrupa Veri Koruma Tüzüğü (General Data Protection Regulation, "GDPR") düzenlemeleri başta olmak üzere dünya gündemine ayak uydurduğuna ve hızlı hareket eden veri gizliliği dünyasının gereklerini yakalamaya çalıştığına şahit oluyoruz.

Dünya gündemini GRC Legal Hukuk Bürosu olarak yakından takip ediyor ve güncelden seçkileri bu içeriğimizle bilgilerinize sunuyoruz.

Aşağıda yer alan haberler 2022 Aralık ayına aittir.

Twitter x Sıfır-Gün Saldırısı

Twitter, bir tehdit aktörünün kullanıcı bilgileri veri tabanını derlemek için Sıfır-Gün (Zero-Day) güvenlik açığı kullandığını doğruladı. Twitter, bu güvenlik açığının Ocak 2022'de giderildiğini söyledi ancak 5 milyondan fazla kullanıcının halka açık olmayan bilgilerini içeren veri tabanının bir veri pazarı forumunda ücretsiz olarak paylaşıldığı, ayrıca, potansiyel olarak 17 milyon kayıt içeren başka bir veri tabanının da aynı güvenlik açığı kullanılarak oluşturulduğu bildiriliyor.

Temmuz'da 30.000 dolardan satışa sunulan 5.485.635 Twitter kullanıcı kaydının yer aldığı veri tabanı, Kasım'da Breach Forums sitesinde ücretsiz olarak paylaşıldı. Twitter kullanıcı adları, oturum açma adları ve doğrulama durumu gibi verilerin çoğu ifşa oldu ve telefon numaraları ve e-posta adresleri gibi özel bilgilerin de yer aldığı belirtiliyor.

Bilgiler, bir bilgisayar korsanı tarafından ifşa edildiği üzere bir Uygulama Programlama Arayüzü (Application Programming Interface, "API") güvenlik açığı kullanılarak toplanmış. API'lerin bilgisayarların birbirleriyle iletişim kurmasına izin verdiği ve internetten geçen tüm trafiğin yaklaşık %80'ini oluşturduğu açıklamasıyla çok önemli olduğu ve bu önemi doğrultusunda ele alınması gerektiği belirtiliyor.

Gündeme gelen güncel veri ihlallerinde kimlik doğrulama (veya eksikliği) tabanlı sorunlar, kaynak eksikliği ve hız sınırlaması, hata tespiti ve log kaydı gibi API kaynaklı sorunların ve bunların kombinasyonunun önemli miktarda kişisel veriyi açığa çıkardığına şahit olunuyor.

Ağustos ayındaki açıklamasında Twitter: *"Güvenlik açığının bir sonucu olarak, Twitter sistemlerine bir e-posta adresi veya telefon numarası tanımlanırsa, sistem e-posta adresi veya telefon numarasının hangi Twitter hesabıyla ilişkili olduğunu söyleyecektir. Hata, Haziran 2021'de kodumuzda yapılan bir güncellemeden kaynaklandı; öğrendiğimizde hemen araştırdık ve düzelttik. O sırada, güvenlik açığından yararlanıldığına dair hiçbir işaret yoktu."* dedi.

Twitter ayrıca, *"...etkilenmiş olma potansiyeli olan her hesabı doğrulayamıyoruz ve özellikle devlet veya diğer aktörler tarafından hedef alınabilecek takma hesaplara sahip kişiler konusunda dikkatliyiz."* dedi ve sorundan etkilenen herhangi bir kullanıcıyla iletişime geçeceğini teyit etti.

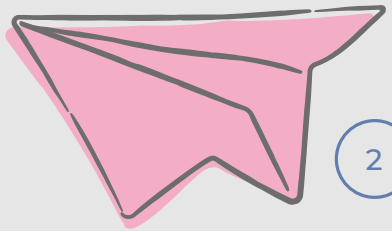
Fransız Twitter kullanıcıları için bir milyondan fazla telefon numarası içeren bu veri tabanının bir örneğinin Bleeping Computer tarafından alındığı, sayıların gerçek olduğu ve ABD'nin yanı sıra Avrupa ülkeleri ve İsrail'den veriler içerdiği birden fazla kullanıcıyla doğrulanarak belirtiliyor.

Veri sızıntısının gündeme getirdiği kaygılar arasında, anonim kalmayı tercih eden kullanıcılarının kimliğinin açığa çıkması, göz önündeki kişilerin hesaplarının ele geçirilebileceği ve Twitter tarafından gönderildiği sanılarak açılan e-postaların fişleme amaçlı iletilebileceğinden daha fazla kişisel veriye ulaşılabileceği bulunuyor.

Telegram x Hindistan

Hindistan, Güney Asya pazarında yaklaşık 150 milyon kullanıcıyı bir araya getiren Telegram için en büyük pazarlardan biri, kısmen korsanlık sorunu nedeniyle bazı kullanıcılar arasında özellikle popülerlik kazanmıştı. Platform, filmlerin ve TV şovlarının geniş çapta paylaşıldığı, bazen on binlerce kullanıcıyla kolayca keşfedilebilen kanallarla dolu.

Telegram, Hindistan'daki bir mahkeme kararı doğrultusunda telif hakkı ihlaliyle sonuçlanan yöneticilerin adlarını, telefon numaralarını ve IP adreslerini ifşa etti. Bu ifşa, anlık mesajlaşma platformunun kullanıcıları üzerinde depoladığı ve yetkililer tarafından ifşa ettirilebilecek verilerin önemli bir örneğini teşkil etti.



Neetu Singh isimli bir öğretmen ders materyalinin Telegram kanallarında izinsiz olarak satıldığını öğrenmiş, platform materyalin yetkisiz dağıtımını önlemede yeterince çaba göstermediği için dava açmış, akabinde ise Telegram Delhi Yüksek Mahkemesi tarafından verileri paylaşmaya zorlanmıştır.

Daha önce bir Hindistan mahkemesi, Telegram'a Hindistan yasalarına uymasını ve bu tür kanalları işletenlerle ilgili ayrıntıları ifşa etmesini emretmişti. Telegram, kullanıcı bilgilerini ifşa etmenin kullanıcıların verilerini depolamak için fiziksel sunucularını yerleştirdiği Singapur'un gizlilik politika ve yasalarını ihlal edeceğini savundu ancak savunma başarılı olamadı.

Hindistan mahkemesi, Telegram sunucularını ülke dışında konumlandırmayı seçtiği için telif hakkı sahiplerinin *"gerçek ihlalcilere karşı savunmasız"* bırakılamayacağını söyledi. Yargıç Prathiba Singh, Telegram'ın bu karara uyduğunu ve verileri paylaştığını söyledi.

Mahkeme, herhangi bir üçüncü tarafa ifşa edilmeyeceğine dair açık talimatla ve yalnızca mahkemenin yürütülmesi amacıyla söz konusu verilerin hükümet yetkililerine ve polislere açıklanabileceğini belirtti.

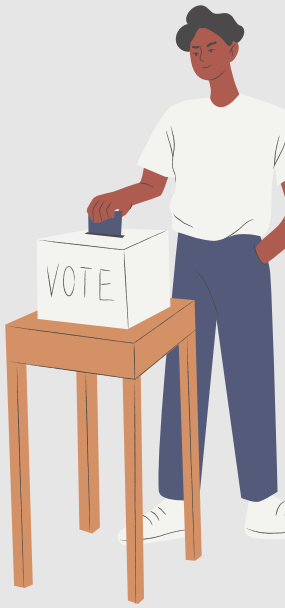
Telegram sözcüsü Remi Vaughn verdiği bir demeçte *"Telegram, kullanıcıları hakkında çok sınırlı veri depoluyor veya hiç depolamıyor. Çoğu durumda, belirli giriş noktaları olmadan herhangi bir kullanıcı verisine bile erişemiyoruz ve burada da durumun böyle olduğuna inanıyoruz. Sonuç olarak, bu durumda herhangi bir özel verinin paylaşıldığını doğrulayamıyoruz"* dedi.

Macaristan x Seçim Kampanyası

İnsan Hakları Örgütü (Human Rights Watch, "**HRW**") bugün yayınladığı bir raporda, Macaristan hükümetinin 2022 ulusal seçim kampanyası sırasında kişisel verileri kötüye kullandığını ve zaten dengesiz olan oyun alanını iktidar partisinin lehine çevirdiğini söyledi.

Hükümet ile iktidar partisi kaynakları arasındaki sınırların bulanıklığı ve kilit kurumların hükümet tarafından ele geçirilmesi, yasaların seçici bir şekilde uygulanmasına yol açtı ve bu da Fidesz'in avantajıyla sonuçlandı.

"Trapped in a Web: The Exploitation of Personal Data in Hungary's 2022 Elections" başlıklı rapor, Macaristan'da Fidesz ve Başbakan Viktor Orbán'ın art arda dördüncü dönemiyle sonuçlanan Nisan 2022 seçimlerindeki veriye dayalı kampanyayı inceliyor. *HRW, kamu hizmetlerine başvuran kişilerden toplanan verilerin Fidesz'in **kampanya mesajlarını yaymak için** kullandığını tespit etti.*



HRW araştırmacısı Deborah Brown, *"İnsanların kamu hizmetlerine erişebilmek için toplanan kişisel verilerini kullanarak onları siyasi kampanya mesajlarıyla bombardımana tutmak güvene ihanet ve gücün kötüye kullanılmasıdır. Macar hükümeti kişisel verileri siyasi kampanyalar için kullanmayı bırakmalı ve seçimler için eşit şartlar sağlanmalı"* dedi.

HRW, gizlilik ve veri koruma, seçim dürüstlüğü ve siyasi kampanyalar hakkında uzmanlarla görüştü; uzmanlar arasında siyasi partilerin temsilcileri, veriye dayalı kampanyalara dahil olan şirketler ve verileri siyasi kampanyalar tarafından kötüye kullanılan kişiler yer alıyor.

Hükümetin Fidesz'in kampanya mesajlarını yaymak için; **Covid-19 aşısı için kaydolan**, vergi avantajları için başvuran veya bir meslek birliğine zorunlu üyelik için kaydolan kişilerden topladığı verileri farklı amaçla kullandığı tespit edildi. Örneğin, kişisel verilerini Covid-19 aşısına kaydolmak için devlet tarafından işletilen bir web sitesine gönderen kişiler, iktidar partisi lehine seçimleri etkileme amaçlı siyasi mesajlar aldı.

2022 seçimleri, **yargı bağımsızlığının baltalandığı, kamu kurumlarının ele geçirildiği, medya ortamının kontrol edildiği, sivil toplum kuruluşu faaliyetlerinin suç sayıldığı, savunmasız grupların ve azınlıkların şeytanlaştırıldığı** Orbán hükümetinin 12 yıllık yönetimi sonrasında gerçekleşti.

Macaristan, gizliliği korumak ve demokratik seçimlere katılma hakkını güvence altına almak için ulusal ve uluslararası hukuka göre sorumluluğa sahiptir. Bunu sağlamak için ise tarafların aynı koşullara tabi olarak hareket edebildiği eşit bir siyasi oyun alanı gerekir.

Verileri kötüye kullanılan kişiler, aşı web sitesine kaydolduklarında diğer hükümet iletişimlerini almaya izin verdiklerine inanmadıklarını, kayıt verilerinin siyasi ve seçim kampanyaları için kullanılmasına kızdıklarını ve pandemi sırasında özellikle savunmasız bir zamanda hükümetin onlardan yararlandığını hissettiklerini söylediler.

Macaristan'daki siyasi partiler, diğer ülkelerdeki gibi, *ayrıntılı seçmen veri tabanları oluşturmak, çevrimiçi anket ve istişareler yürütmek, reklam satın almak, sosyal medyada sohbet robotları yerleştirmek, doğrudan otomatik aramalar, toplu SMS mesajları ve e-postalar aracılığıyla seçmenlere erişim sağlamak* gibi veri bazlı kampanyalara yatırım yapılar ve bu yatırımların gizlilik başta olmak üzere insan hakları açısından önemli sonuçlara sebebiyet verebileceğini unuttular.

HRW, muhalefet partilerinin de kişisel verileri işlemesinin şeffaflıktan yoksun olduğunu ve gizlilik riskleri taşıdığını tespit etti ancak iktidar partisinin aksine verileri ele almalarının seçim sürecinde adaletsizlik yarattığına dair hiçbir kanıt bulamadı.

HRW, Macaristan'ın yasalarda, politikalarda ve uygulamalarda kişisel verilerin siyasi kampanyalar için kullanılmasına ilişkin eksiklikleri gidermesi gerektiğini söyledi. Öncelikli olarak yargı ve seçim ayağını temsil eden hükümet organlarının bağımsız ve tarafsızlığının sağlanması, bunların yasalarla desteklenmesi ve veri koruma otoritelerinin bağımsız ve tarafsız denetiminin güçlendirilmesi gerektiği belirtiliyor.

Meta x IDPC

İrlanda Veri Koruma Otoritesi (The Irish Data Protection Commissioner, "**IDPC**") tarafından, Meta'nın sahibi olduğu Instagram ve Facebook'a veri kazıma uygulamaları nedeniyle **265 milyon avro** para cezası verildi. Çoğu Büyük Teknoloji şirketinin Avrupa merkezi İrlanda'da olduğundan, IDPC'nin, GDPR uygulayıcısı olması kaçınılmaz olarak gündeme gelmişti.

Veri kazıma nedir?

Veri kazıma, bir internet sitesinden veri alma işlemi olarak ifade edilebilir. En basit anlatımıyla bir internet sitesinden bilgi kopyaladıktan sonra başka bir yere yapıştırmak da aslında bir manuel kazıma ("scraping") işlemidir. Genel çapta bakıldığında ise veri kazıma altyapıları aracılığı ile web sunucuları ve/veya uygulamalar arasındaki veri akışı dinlenebilir ve ilgili veriler dosyalardan kazınabilir.

Soruşturma, 2021 Nisan ayında bir bilgisayar korsanı forumunda çevrimiçi olarak yayınlanan ve isim, konum, doğum tarihi, telefon numarası ve e-posta adresi gibi kişisel verileri içeren Facebook'taki kişisel verilerin sızması ile açılmıştı.

Veri sızıntısının 106 ülkede 533 milyon kişiyi ilgilendirdiği, yalnızca Avrupa Birliği'nde ("European Union, "**AB**") ise **86 milyon kişiyi etkilediği** bildirildi. O dönemde Facebook, şirketin Ağustos 2019'da giderdiği bir güvenlik açığı nedeniyle toplu veri kazıma işleminin gerçekleştiğini ve bu nedenle sızan verilerin eski olduğunu belirtmişti.

Soruşturma Instagram'ın veri sızıntısı ile doğrudan ilgili olmayıp Facebook Arama Butonu ile Facebook ve Instagram Messenger'daki Rehber Eşleştirmesi üzerine yoğunlaştı. ***Bu araçların, kullanıcıların Facebook ve Instagram'daki arkadaşlarını/tanıdıklarını telefon numaralarına göre platform üzerinden bulmalarını sağladığı biliniyor.***

Aralık ayında alınan kararda, Mayıs 2018 ve Eylül 2019 dönemleri arasında ilgili sosyal ağların Avrupa'nın gizlilik kurallarını ihlal ettiği sonucuna varılarak bir dizi düzeltici/iyileştirici işlemin yanında **265 milyon avro para cezası** da uygulandı. Meta'nın sözcülerinden biri yaptığı açıklamada, şirketin sistemlerinde telefon numaralarını kullanarak özellikleri kazıma yeteneğini kaldırmak da dahil olmak üzere değişiklikler yaptığını, izinsiz veri kazımanın kabul edilemeyeceğini söyledi.

Meta'nın bu karara itiraz etmesi bekleniyor. Zira bu ceza, ***çocukların mahremiyetini ihlal ettiği gerekçesiyle Instagram'a verilen 405 milyon avroluk cezanın ardından Meta'ya verilen ikinci en büyük ceza*** olurken *(Detaylı Bilgi İçin: Dünyada Neler Oluyor Bülten'imizin Eylül ayına ait haberleri içeren dördüncü sayısına bakabilirsiniz.)*, **AB'nin şeffaflık gerekliliklerine uymadığı gerekçesiyle WhatsApp'a verilen 225 milyon avroluk cezayı da geride bıraktı.**

Bilindiği üzere Instagram ve WhatsApp ile ilgili geçmişte alınan bu kararlar, diğer Avrupa veri koruma otoritelerinin IDPC'nin vardığı sonuca itiraz etmesi ve daha ağır para cezaları talep etmesi nedeniyle uyuşmazlık çözüm mekanizmasından geçmişti; ancak bu karar ile ilgili henüz hiçbir otoriteden itiraz gelmedi.

Meta, AB yasaları kapsamında veri korumaya yönelik ihlalleri nedeniyle yaklaşık **1 milyar avro** yaptırıma tabi tutuldu. Geçtiğimiz aylarda gelirlerinde keskin bir düşüş yaşayan ve son zamanlarda 11.000'den fazla personeli işten çıkarmak zorunda kalan Meta, veri koruma otoritelerinden darbe almaya devam ediyor.

Avrupa Birliği x NIS2

Avrupa Birliği Konseyinin AB genelinde siber güvenliği güçlendirme amacıyla imzaladığı NIS2 ("**Yönerge**") olarak adlandırılan yeni Yönerge, ağ ve bilgi sistemlerinin güvenliğine ilişkin mevcut direktifin yerini alacak. Çek Cumhuriyeti Bölgesel Kalkınma Bakanı Ivan Bartoš, *"Siber güvenlik kuşkusuz önümüzdeki yıllarda da önemli bir sorun olmaya devam edecek. Ekonomilerimiz ve vatandaşlarımız için riskler çok büyük. Bugün bu tehdide karşı koyma kapasitemizi arttırmak üzere bir adım daha attık."* açıklamalarında bulundu.

NIS2'nin; enerji, ulaştırma, sağlık ve dijital altyapı gibi direktif kapsamındaki tüm sektörlerde siber güvenlik risk yönetimi önlemleri ve raporlama yükümlülükleri için temel oluşturacağına inanılıyor.

Revize edilen direktif, siber güvenlik gerekliliklerini ve siber güvenlik önlemlerinin farklı üye devletlerde uygulanmasını uyumlaştırmayı amaçlıyor.

Başarmak sağlamak adına; düzenleyici bir çerçevede asgari kuralları belirleyerek her üye devletteki ilgili makamlar arasında etkili iş birliği için mekanizmalar ortaya koyuyor, siber güvenlik yükümlülüklerine tabi sektör ve faaliyetlerin listesini güncellerken uygulamayı sağlamak için çözüm yolları ve yaptırımlar öngörüyor.

Ayrıca Yönerge'nin, büyük ölçekli siber güvenlik olaylarının ve krizlerinin koordineli yönetimini destekleyecek olan **Avrupa Siber Krizler İrtibat Organizasyonu Ağı EU-CyCLONe**'yi de resmen kuracağı bildiriliyor.

Eski NIS direktifi kapsamında üye devletler hangi kuruluşların temel hizmetlerin işletmecisi olarak nitelendirilme kriterlerini karşılayacağını belirlemekten sorumluyken yeni NIS2 Yönerge'si, düzenlemeye tabi kuruluşların belirlenmesi için genel bir kural olarak bir **büyüklük sınırı kuralı** getiriyor. Bu diğer bir anlatımla, ***sektörlerde faaliyet gösteren veya Yönerge kapsamındaki hizmetleri sağlayan tüm orta ölçekli ve büyük kuruluşların direktif kapsamına gireceği anlamına geliyor.***

Yönerge'nin içerisinde savunma veya ulusal güvenlik, kamu güvenliği ve kolluk kuvvetleri gibi alanlarda faaliyet gösteren kuruluşlara bu Yönerge'nin uygulanmayacağı da açıklığa kavuşturuluyor. **Yargı, parlamentolar ve merkez bankaları da kapsam dışında tutuluyor.**

NIS2'nin merkezi ve bölgesel düzeydeki kamu idareleri için de geçerli olacağı belirtilirken ek olarak, üye devletlerin yerel düzeydeki bu tür kuruluşlar için de Yönerge'nin geçerli olmasına karar verebileceği vurgulanıyor. Üye devletlerin Yönerge'yi iç hukuklarına **adaptasyonu için 21 aylık bir uyum süreci** öngörülüyor.

Twitter x IDPC

IDPC'nin radarında veri kazıma uygulamaları var gibi görünüyor. "Meta x IDPC" haberimizde yer verdiğimiz veri kazıma uygulamaları, Twitter'ın da önüne geldi.

Twitter'ın AB'deki faaliyetlerini denetlemekten sorumlu IDPC, ***milyonlarca Twitter kullanıcısının e-posta ve telefon numaraları da dahil olmak üzere profil bilgilerinin internete sızdırıldığı bir veri kazıma olayı hakkında açıklama talep etti ve Twitter'dan yanıt bekliyor.***

Twitter, Ağustos ayında bilgisayar korsanlarının sistemindeki bir güvenlik açığından yararlanarak telefon numaraları ve e-postalarla bağlantılı Twitter profillerini elde ettiklerini kabul etmiş ancak o dönemde bu açığı giderdiklerini belirtmişti.

Twitter etkilenen hesap sayısını doğrulamazken bilgisayar korsanlarına atıfta bulunan medya raporları, **5,4 milyon kullanıcının e-posta adresleri ve telefon numaraları** da dahil olmak üzere profil ayrıntılarının 24 Kasım gibi yakın bir tarihte bir bilgisayar korsanı forumunda ücretsiz olarak paylaşıldığını belirtti. Bir internet sitesine göre, aynı güvenlik açığından faydalanan ikinci bir Twitter profil hesabı dökümü, milyonlarca kullanıcının daha bilgilerini açığa çıkarmıştı. IDPC, her iki olayla ilgili raporlar hakkında cevap beklediğini söyledi.

Dublin'de halihazırda Twitter hakkında, Elon Musk'ın şirketin CEO'su olmasından önce açılmış iki soruşturma bulunuyor. IDPC'den Helen Dixon geçtiğimiz ay yaptığı açıklamada, ofisinin şirketin yöneticilerini devam eden soruşturmalar hakkında sorgulayacağını belirtmişti.

Twitter'dan herhangi bir cevap gelmezken bu olayın, Meta'ya verilen cezadan tam bir hafta sonra gündeme gelmesi ve neredeyse aynı şekilde gerçekleşmiş olması, benzer bir cezanın Twitter'a da gelebileceği ihtimalini oldukça kuvvetlendiriyor.

Meta x Rekor Para Cezası

Meta, yakında sahip olduğu üç sosyal ağ olan Facebook, WhatsApp ve Instagram için büyük bir faturayla karşı karşıya kalacak gibi görünüyor. Avrupa Veri Koruma Kurulu'nun (European Data Protection Board, "**EDPB**") üç platformu hedef alan kararlar vermesi bekleniyor ve ardından Meta'nın İrlanda'daki baş düzenleyicisi bir ay içinde nihai bir karar verecek.

Para cezasının ayrıntıları ve olası değeri o zamana kadar gizli tutulacak ancak Meta'nın mali tablolarına göre, **para cezalarının üçlü toplamı 2 milyar avroyu aşabilir**. Tahmin edilen bu ceza miktarının, **tek seferde bir şirket için hükmedilen GDPR kaynaklı en yüksek para cezasını teşkil etmesi bekleniyor.**

İrlanda'daki belgelere göre Meta, 2022 ve 2023'te AB gizlilik cezaları için **3 milyar avro** ayırdı. *Instagram, çocukların mahremiyetini ihlal ettiği için Eylül ayında 405 milyon avro para cezasına çarptırılmıştı ve Facebook şimdiye kadar veri ihlallerinden 282 milyon avro miktarında para cezasına ulaştı.*

Söz konusu bütçe ile bugüne kadar ödenmesi gereken para cezalarının hesabı yapıldığında Meta tarafından gelecekte gerçekleşebilecek **veri ihlalleri için 2 milyar avro bırakılıyor.** Sektör devleri söz konusu olduğunda bakış açısının ihlalin kaçınılmaz olduğu konusunda evrildiğini görüyoruz. *Dolayısıyla gelecekte tedbirlerin artması yerine cezalara ayrılan bütçelerin devleşmesi daha makul bir beklenti haline geliyor.*

Eleştirmenler ayrılan bütçeyi değerlendirirken Meta'nın dünya çapında 11.000 çalışanını ekonomik gerekçelerle işten çıkarmasını göz önünde bulunduruyor. Alınması beklenen üç para cezası, Meta'nın cebine zarar vermenin ötesinde, iş modelini de etkileyebilir.

Kararlar, Max Schrems'in şirketi milyonlarca Avrupalının verilerini işlerken uygun yasal zemine sahip olmamakla suçlayan şikayetlerinden kaynaklanıyor. **Nihai kararlar, Meta'nın verileri kullanıcılarla yaptığı bir sözleşmenin parçası olarak işlediği iddiasını geçersiz kılarsa, şirketin veriye dayalı reklam hedefleme modeli için başka bir yasal dayanak araması gerekecek.**

IDPC, Meta'nın geçen yıl yayınlanan karar taslağında kişiselleştirilmiş reklamlar sağlamak için *"kullanıcılarıylabir sözleşmeyi yerine getirmek için verilere ihtiyacı olduğu"* iddiasını büyük ölçüde destekledi. Ancak bu bakış açısı, İrlanda'yı meslektaşları arasında uzun süredir azınlıkta bırakıyor. Norveç Veri Koruma Kurumu, İrlanda yorumunun GDPR'ı "**anlamsız**" hale getireceğini söyledi. IDPC, şirketlerin sözleşmeyi yasal dayanak belirleyerek reklamları hedeflemek için verileri kullanmasını yasaklayan AB yönergelerine karşı oylamada da yalnızdı.

Sonuç olarak Meta'nın, kararlar akabinde veri işleme için yeni yasal dayanak arama ihtiyacı doğabilir. Avrupa'dan Amerika'ya veri aktarımı hakkında yüksek profilli bir davanın da devam edildiği düşünüldüğünde, uzun süre mercek altında olması ve adımlarının takip edilmesi kaçınılmaz görünüyor.

Apple x Siber Güvenlik

Apple, sivil özgürlük ve gizlilik savunucularının uzun süredir belirttikleri dahil olmak üzere, kişisel verileri bilgisayar korsanlarından korumaya yardımcı bir yol olarak sunduğu bir dizi güvenlik ve gizlilik iyileştirmesini duyurdu.

Apple uçtan uca şifreleme kullanarak bulutta ("**iCloud**") yedeklenen verilerin daha fazlasını korumayı seçmeyi mümkün kılarak kullanıcının dışında hiç kimsenin söz konusu bilgilere erişememesini sağlıyor. Değişikliklerin, gelişmiş bir devlet aktörünün şirket sunucularına sızmayı başardığı istisnai bir durumda dahi, kullanıcıların dijital hayatlarını bilgisayar korsanlarından korumalarına yardımcı olacağı söyleniyor.

Gizlilik savunucuları, bu değişikliklerin kolluk kuvvetlerinin ve devlet kurumlarının Apple'dan alabileceği kullanıcı verisi türleri üzerinde daha ani bir etkiye sahip olabileceğini söylüyor. Cahn, *"Bu tür bir koruma siber suçlulara karşı değil, şirketi verileri teslim etmeye zorlamak için hükümetin gücünü kötüye kullanan kişilere karşı koruma sağlaması açısından daha değerlidir"* dedi.

Apple uzun yıllardır polislerin bilgi almak için başvurdukları bir pozisyonda bulunuyor. Apple'ın Kolluk Uygulama Kılavuzları, soruşturmalarda nasıl yardım sağlayabileceklerine ilişkin yol gösteriyor ve yeni değişiklik ile gizlilik özelliğini kullanmayı seçenler için güvenli bir liman mevcut olacak.

Araştırmalarına yardımcı olması için kullanıcı verilerini güvence altına almak isteyen devlet kurumları için bir endişe kaynağı olan değişiklik ile ilgili FBI, kullanıcı verilerine ajans tarafından erişilmesinin önlenmesinden duyduğu hoşnutsuzluğu çoktan dile getirdi. FBI yaptığı açıklamada, Apple'ın kararından "derin endişe duyduğunu" ve ajansın bu bilgilere erişmek için başka bir yola veya alternatif çözümlere ihtiyacı olduğunu söyledi.

Apple gibi şirketler, insanlar hakkında ellerinde bulundurdukları çok büyük miktardaki bilgi nedeniyle hem bilgisayar korsanları hem de kolluk kuvvetleri için giderek daha çekici bir varlık haline geldi. Şirketin en son şeffaflık raporuna göre, Apple'ın topladığı veriler için hükümet ve kolluk kuvvetleri talepleri arttı.

Son yıllarda küresel siber saldırılar ve veri ihlallerinde ani bir artış yaşandı. Kimlik Hırsızlığı Kaynak Merkezi'nden (Identity Theft Resource Center) alınan bir rapora göre, 2022'nin ilk çeyreğinde, bir önceki yılın aynı çeyreğine göre %14 artışla kamuya açıklanmış 404 veri ihlali meydana geldi.

Apple'ın "iCloud için gelişmiş veri koruması" olarak adlandırdığı, iCloud'da saklanan kullanıcı bilgilerinin uçtan uca şifrelenmesi anlamına geliyor ve aşağıdaki detaylar paylaşılıyor:

Yıl sonundan önce ABD'de,
2023'te dünya çapında piyasaya sürülecek,

Piyasaya sürülmeden önce ilk olarak küçük bir test grubunun kullanımına sunulacak,

iCloud'a yedeklenen mesajlar, notlar ve fotoğraflar gibi bilgiler tamamen şifrelenecek,

Değişiklik tüm verileri kapsamayacak: kişiler, takvim bilgileri ve e-posta şifrelenmeyecek,

Kullanıcılar özelliği gönüllü olarak etkinleştirecek,

Şifreleme anahtarı ve şifrelenmiş verilere erişim sağlanması için kullanılan kod iCloud'da değil, cihazda saklanacak,

Varsayılan olarak tüm kullanıcılar için açık olmayan özellik, gizlilik savunucuları için bir tartışma konusu olmaya devam ediyor.

Cahn, *"iCloud için varsayılan olarak gizliliğe geçiş yapmanın en önemli adım olduğunu düşünüyorum. Ancak bu kadar çok e-posta programı ve takvim aracını devre dışı bırakmanın ne kadar zor olacağı göz önüne alındığında Apple'ı daha az eleştiriyorum"* dedi. **Apple ise sistemin, kullanıcıların şifreleme anahtarlarından ve bilgilere erişimi yeniden kazanmak ve kurtarmak için sorumlu olmasını gerektirdiği için varsayılan olarak ayarlanmadığını söylüyor.**

Son olarak şirket, insanların mesajlarının yalnızca amaçlanan alıcıya gittiğini ve bir bilgisayar korsanı tarafından ele geçirilmediğini doğrulamasına olanak tanıyan bir kod sistemi sunuyor. İşlem, şifreli mesajlaşma uygulaması Signal'in kullanıcılarına tanıdık gelebilir. Sistemi etkinleştiren iki kişi benzersiz kodlarını değiş tokuş edebilecek ve cihazları, farklı bir koda sahip birinin konuşmaya girip girmediğini otomatik olarak algılayacak.

Ürünlerin tanıtımının yapıldığı basın açıklamasında doğrulama özelliğini etkinleştiren kullanıcılar arasındaki konuşmalarda bir saldırgan, bulut sunucularını ihlal etmeyi ve bu şifreli iletişimleri dinlemek için kendi cihazlarını yerleştirmeyi başarırsa otomatik uyarılar açılacağı belirtildi.

Clubhouse x Garante

İtalya'nın Veri Koruma Otoritesi (Garante Per La Protezione Dei Dati Personali, "**Garante**"), Covid-19 karantinaları sırasında popüler hale gelen, 2020 yılında geliştirilen ve kullanıcıların sesli sohbet edebilmesi için sohbet odaları sağlayan ABD'li sosyal medya uygulaması Clubhouse'a, GDPR'ı ihlal ettiği gerekçesi ile 2 milyon avro para cezası verdi.

Garante tarafından yapılan basın açıklamasında, Alpha Exploration'a ait uygulamanın kullanıcı verilerinin kullanımında yeterince şeffaf olmadığı ve GDPR'ın çok sayıda hükmünü ihlal ettiği belirtildi. Açıklamada, uygulamanın kullanıcılara izinsiz olarak ses saklama ve paylaşma olanağı verdiği; uygun bir yasal dayanak olmaksızın hesap bilgilerini profilleyerek paylaştığı ve sosyal ağ tarafından yapılan kayıtların belirsiz saklama sürelerine sahip olduğu vurgulandı.

Garante, para cezasının yanı sıra uygulamaya, kullanıcıların bir sohbet odasına girmeden önce sohbetin kaydedilebileceğini öğrenmelerine olanak tanıyan bir özellik getirmesini ve kullanıcı olmayanları da kişisel verileriyle ilgili bilgilendirecek bir mekanizma oluşturmasını emretti. Clubhouse gizlilik bildirimine, veri saklama sürelerine ilişkin birtakım bilgileri de netleştirerek eklemesi yönünde talimat verildi.

Uygulamadan henüz bir cevap gelmemekle birlikte uygulamanın Fransız Veri Koruma Otoritesi'nin de soruşturma radarına girdiği bildirildi.

Meta x Kişiselleştirilmiş Reklam

The Wall Street Journal (“**WSJ**”) haberine göre, EDPB, Meta’nın kullanıcıları kişiselleştirilmiş reklamları kabul etmeye zorlayamayacağı yönünde karar verdi.

Meta’nın İrlanda’daki şirketi, Mayıs 2018’de GDPR yürürlüğe girdiğinde hüküm ve koşullara bir ekleme yaparak kullanıcılardan onay alma gerekliliğini ortadan kaldırabileceğine inanmış, IDPC de Meta’yı bu konuda desteklemişti. Dört buçuk yıl sonra EDPB’den çıkan kararda, IDPC’nin bu görüşü reddedildi.

Kararda, Meta’nın kişisel verileri reklam amaçlı kullanırken gizlilik politikasını ya da sözleşmeleri öne sürmesinin bir gerekçe olarak gösterilemeyeceği, kullanıcıların açık rızalarına başvurularak **evet/hayır** seçeneklerinin sunulması gerektiği belirtildi.

Henüz EDPB kararının kendisi yayınlanmamakla birlikte, IDPC’ye yöneltilen bozma kararı ışığında, IDPC’nin de nihai kararıyla birlikte, Ocak 2023 tarihinde yayınlanması bekleniyor. WJS’ye göre, kişiselleştirilmiş reklamların genel olarak durdurulmasına ek olarak Meta için büyük miktarda para cezası da talep edildi, miktar henüz bilinmiyor.

IDPC’nin prosedür süresince Meta’ya destek çıktığı, hatta Meta’nın çıkarları doğrultusunda EDPB Kılavuz İlkeleri’ni (EDPB Guidelines) etkilemeye çalıştığı iddia ediliyor. Bununla birlikte diğer Avrupa veri koruma otoriteleri de IDPC’nin görüşünü reddetmekte ısrarcı.

Meta’nın Ocak 2023’te çıkacak karara itiraz edebileceği de gündemde ancak EDPB kararından sonra itirazların sonuç bulması oldukça düşük bir ihtimal gibi gözüküyor. Özellikle kullanıcıların son dört buçuk yıldır verilerinin rızaları dışında kullanılmasına karşın harekete geçebileceği düşünülüyor.

Google x CJEU

AB’nin en üst mahkemesi Avrupa Adalet Divanı (The Court of Justice of the European Union, “**CJEU**”), Avrupa’da bulunan kişilerin, bilgilerinin açıkça yanlış olduğunu kanıtlamaları halinde Google’ın kendileri hakkındaki arama sonuçlarını silmelerini sağlayabileceklerine hükmetti.

Dava, iki yatırım yöneticisinin Google'dan, isimlerine dayanarak yapılan ve grubun yatırım modelini eleştiren bazı makalelere bağlantı veren bir aramanın sonuçlarını kaldırmasını talep etmesiyle başladı.

İddiaya göre makalelerdeki bilgiler yanlış olmasına rağmen Google, bu bilgilerin doğruluğu ile ilgili kesin bilgisinin olmadığını savunarak talebi reddetti.

CJEU verdiği kararla, yatırım yöneticilerinin GDPR kapsamında **"unutulma hakkı"** olarak adlandırılan hakkı başarılı bir şekilde kullanabilmelerinin önünü açtı. Mahkeme, kararına eşlik eden basın açıklamasında; *"Arama motorlarından yanlış sonuçları temizlemek isteyen kişiler, kendileri hakkında söylenenlerin yanlış olduğuna dair yeterli kanıt sunmak zorundadır. Ancak bu kanıtın, örneğin bir yayıncıya karşı açılmış bir davadan gelmesi gerekmez. Yalnızca kendilerinden makul olarak talep edilebilecek kanıtları sunmaları yeterlidir."* açıklamalarında bulundu.

OECD x Hükümetler Arası Anlaşma

OECD ülkeleri 14 Aralık'ta, ulusal güvenlik ve yasaların uygulanması amaçlarıyla kişisel verilere erişilirken özel hayatın gizliliği ve diğer insan hak ve özgürlüklerinin korunmasına yönelik ortak yaklaşımlara ilişkin ilk hükümetler arası anlaşmayı kabul etti. Diğer ülkelerin de katılımına açık olan 38 OECD ülkesi ve AB tarafından imzalanan Bildirge büyük bir siyasi taahhüdü işaret ediyor.

Özel Sektör Kuruluşları Tarafından Tutulan Kişisel Verilere Devletin Erişimine İlişkin OECD Bildirgesi (OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, "**Bildirge**"), ulusal güvenlik ve kolluk kuvvetlerinin kişisel verilere mevcut yasal çerçeveler kapsamında erişimini açıklığa kavuşturarak küresel ekonominin dijital dönüşümünde sınır ötesi veri akışlarına olan güveni artırmayı amaçlamaktadır.

OECD Genel Sekreteri Mathias Cormann, *"Bugünün dijital çağında sosyal medya kullanımından uluslararası ticarete ve küresel sağlık konularında işbirliğine kadar her şey için sınırlar arasında veri aktarabilmek esastır. Ortak ilkeler ve güvenceler olmaksızın, kişisel verilerin yetki alanları arasında paylaşılması, özellikle ulusal güvenlik gibi hassas alanlarda mahremiyet endişelerini artırıyor."* dedi.

Dönüm noktası niteliğindeki bu anlaşma, OECD ülkelerinin ortak standartları ve güvenceleri desteklediğini resmen kabul ediyor. **Bireylerin dijital ekonomiye olan güveni ve vatandaşlarının kişisel verileriyle ilgili olarak hükümetler arasında karşılıklı güven için gerekli güvencelerle, hukukun üstünlüğüne sahip demokrasiler arasında veri akışının sağlanmasına yardımcı olacağına inanılıyor.**

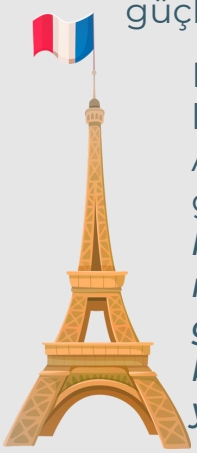
Devletin kişisel verilere erişimine yönelik demokratik değerler ve hukukun üstünlüğü ile tutarsız herhangi bir yaklaşımı reddeden Bildirge, kolluk kuvvetleri ve ulusal güvenlik gibi hassas alanlarda ortak ilkelerin bulunmamasının veri akışlarında gereksiz kısıtlamalara yol açabileceğine dair artan endişelerden kaynaklanmış.

Bildirge, OECD'nin mevcut ve üçüncü aşamasında büyüme ve refah için veri yönetişimine odaklanan ve ülkelerin karşılaştığı kritik veri yönetişimi zorluklarına kanıta dayalı çözümler sunan **Dijitale Geçiş** projesini tamamlıyor.

Apple x CNIL

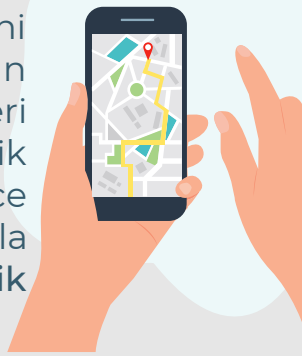
Fransız Veri Koruma Otoritesi'nin (Commission Nationale de l'Informatique et des Libertes, "**CNIL**") Raportör'ü Francois Pellegrini, Apple'ın gizlilik kurallarını ihlal ettiği gerekçesiyle 6 milyon euro para cezasına çarptırılması tavsiyesinde bulundu.

CNIL'in yaptırım kararı verirken raportör tavsiyeleri ile bağlı olmadığı bilinse de genellikle Otorite'nin kararları üzerinde raportörün görüşleri son derece önemli bir ağırlığa sahip olduğu belirtilmekte; bu kapsamda Pellegrini'nin geçen yıl "**France Digitale Lobi**" tarafından yapılan bir şikâyet sonucu yetkili kurum tarafından yürütülen soruşturma akabinde verdiği bu tavsiyenin, CNIL'den çıkacak bir yaptırım kararı olasılığını güçlendirir nitelikte olacağı düşünülüyor.



Fransa'daki dijital girişimcilerin ve risk sermayedarlarının büyük bir kısmını temsil eden bu Lobi, şikâyet dilekçesinde iPhone üreticisi Apple'ın eski işletim yazılımı iOS 14'ün Avrupa Birliği gizlilik gereklilikleri ile örtüşmediğine yer vermişti. *iOS 14 kapsamında kullanıcılardan, telefonlarında yüklü mobil uygulamaların reklamlarını yapmak ve hedefli reklamcılık faaliyeti gerçekleştirmek amacıyla izinsiz bir şekilde veri toplandığı, önden bir izin/rıza süreci işletilmeden hedefli reklam kampanyalarının yürütüldüğü savunuldu.*

Apple'ın "**App Tracking Transparency**" (Uygulama Takip Şeffaflığı) adını verdiği gizlilik güncellemelerinin, kullanıcılara uygulamaların diğer şirketlere ait uygulama ve web sitelerindeki etkinlikleri izlemesini önleme seçeneği sunduğu biliniyor. Pellegrini açıklamasında, Apple'ın önceki işletim sistemi sürümü iOS 14.6'nın kişisel verilerin toplanması noktasında kullanıcılardan izinleri doğru bir süreç yönetimi ile almadığını, bu izinlerin otomatik olarak verilmiş şekilde kullanıcı önüne verildiğini ve sadece kapatma/izin vermeme seçeneklerinin sunulduğunu, dolayısıyla **Avrupa Birliği'nin ePrivacy Direktifi (ePrivacy Directive) gizlilik hükümlerine aykırılık bulunduğunu dile getirdi.**



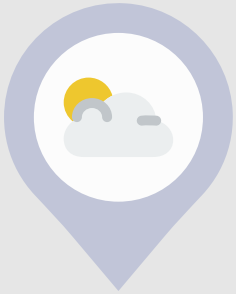
Apple’ın işletim sisteminin bir sonraki sürümü iOS 15’te ise bu tür ir ön izin mekanizmasının oluşturulduğu bildirildi. Apple’ın gizlilik departmanından sorumlu müdürü Gary Davis, Raportör’ün vardığı sonuçlara itiraz ederek firmanın kullanıcı gizliliği konusunda son derece hassas olduğunu belirtti. Davis, **“İhlalin ciddi bir boyutta olmamasının dile getirilmesi bile cezanın azaltılması gerektiğine işaret ediyor.”** diyerek ceza miktarının kamuoyuna açıklanmamasını talep ederken CNIL’ın ne zaman bir karara varacağı hakkında ise henüz bir bilgi bulunmuyor.

Microsoft x 2023

Fransa, Almanya, İspanya ve İsviçre dahil olmak üzere Avrupa ülkelerinde bir düzineden fazla veri merkezi işletmekte olan Microsoft Corp (MSFT.O) yaptığı açıklamada, 1 Ocak'tan itibaren AB bulut müşterilerinin bölgedeki verilerinin bir kısmını işleyip depolayabileceğini söyledi.

AB'nin 2018'de GDPR’ı yürürlüğe koymasından bu yana büyük işletmeler, müşteri verilerinin uluslararası akışı konusunda giderek daha fazla endişe duymaya başladı. Avrupa Komisyonu, verileri ABD'ye aktarılan Avrupalı kullanıcıların gizliliğini korumak için öneriler üzerinde çalışıyor.

AB veri sınırının aşamalı olarak kullanıma sunulması, Azure, Microsoft 365, Dynamics 365 ve Power BI platformu gibi tüm temel bulut hizmetleri için geçerli olacaktır. Microsoft'un Baş Gizlilik Sorumlusu Julie Brill, *"Bu projeye derinlemesine daldıkça, daha aşamalı bir yaklaşım benimsememiz gerektiğini öğrendik. İlk aşama müşteri verileri olacak. Sonraki aşamalarda log kaydı verilerini, hizmet verilerini ve diğer türdeki verileri sınıra taşıyacağız."* dedi ve ikinci fazın 2023'ün sonunda, üçüncü fazın ise 2024'te tamamlanacağını belirtti.



Büyük şirketler için veri depolama o kadar büyük hale geldi ve o kadar çok ülkeye dağıldı ki, verilerinin nerede olduğunu ve GDPR gibi kurallara uyup uymadığını anlamaları zorlaşıyor. Brill, *"Müşterilerimizin kendilerini daha güvende hissetmelerini sağlamak ve düzenleyicileriyle verilerinin nerede işlendiği ve depolandığı konusunda net görüşmeler yapabilmek için bu çözümü oluşturuyoruz"* dedi.

Microsoft daha önce, hükümetin müşteri verilerine ilişkin taleplerine itiraz edeceğini ve GDPR'ı ihlal ederek verilerini paylaştığı herhangi bir müşteriyi mali olarak tazmin edeceğini söylemişti.