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.

GRC LEGAL olarak dünya gündemini yakından takip ediyor ve güncelden seçkileri bu içeriğimizle bilgilerinize sunuyoruz.

Aşağıda yer alan haberler 2024 Şubat ayına aittir.

DPA x Uber

Hollanda Veri Koruma Otoritesi (Data Protection Authority, "**DPA**") Uber'e, sürücülerinin kişisel verilerine ilişkin gizlilik düzenlemelerini ihlal ettiği gerekçesiyle **10 milyon Euro** para cezası verdi.

DPA, Uber'in sürücülerinin kişisel verilerini ne kadar süreyle sakladığını ya da Avrupa Ekonomik Alanı (European Economic Area, "**EEA**") dışındaki, adını vermediği ülkelerdeki kuruluşlara gönderirken bu verileri nasıl güvence altına aldığını hüküm ve koşullarında belirtmediğini tespit etti.

Uber'in ayrıca kişisel verilere erişim taleplerini gereksiz yere karmaşık hale getirerek sürücülerinin gizlilik haklarını kullanma çabalarını engellediğini de sözlerine ekleyen DPA, Uber'in yine de işaret edilen sorunları düzeltmek için adımlar attığını belirtti.

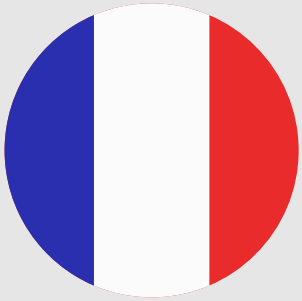
Bir Uber sözcüsü yaptığı açıklamada, "DPA, Uber'in sürücüler tarafından dile getirilen az sayıdaki 'düşük etkili' sorunu çözdüğünü kabul ederken, iddialarının büyük çoğunluğunu asılsız olarak reddetti" dedi. Sözcü, şirketin veri talep süreçlerini iyileştirmek için sürekli olarak çalıştığını da sözlerine ekledi.

Ceza, 170'ten fazla Fransız sürücünün bir Fransız insan hakları örgütüne şikâyette bulunması ve bu örgütün de Fransız Veri Koruma Otoritesine şikâyette bulunmasının ardından verildi. Ancak Uber'in Avrupa'daki merkezi Hollanda'da olduğu için şikâyet DPA'ya iletildi.

GRC LEGAL Yorumu

GDPR, kişisel verilerin üçüncü ülkelere aktarımını düzenleyerek kişisel verilerin EEA içerisinde sahip olduğu koruma düzeyinin korunmasını amaçlar. Bu kapsamda, kişisel verilerin yurtdışına aktarılmasına yönelik kriterler getirmiştir. Kişisel verileri üçüncü ülkelere aktarılan kişilerin GDPR hükümleri gereğince verilerinin hangi güvence önlemleri alınarak aktarımı sağlandığının belirtilmesi gerekir. Bu noktada DPA'nın bu yaptırımı, GDPR hükümlerinin üçüncü ülkelere veri aktarımı hususundaki hassaslığını göz önüne koymaktadır.

Fransız SA x Tagamedia



Fransız Denetim Otoritesi (French Supervisory Authority, "**Fransız SA**"), 2022 yılında ticari araştırma konusundaki öncelikli soruşturma konusunun bir parçası olarak, sektördeki profesyonellerin uygulamalarına, özellikle de veri komisyoncuları olarak bilinen bu ekosistemdeki birçok aracı da dahil olmak üzere verileri yeniden satanlara odaklandı.

Bu vesileyle, Fransız SA, esas olarak çevrimiçi rekabet siteleri ve ürün test internet siteleri işleten ve bu yolla potansiyel müşterilerden veri toplayan Tagadamedia hakkında soruşturma başlatmaya karar verdi.

Tagadamedia, yarışmalara veya ürün testlerine katılmak için internet sitelerinde sunduğu formlar aracılığıyla potansiyel müşterilerden veri topluyor. Bu veriler daha sonra ticari araştırma için şirketin ortaklarına gönderiliyor. Şirket veri işleme için rıza topladığını iddia etse de kullanılan formlar GDPR gerekliliklerine uygun olarak rıza toplanmasına izin vermiyor.

İncelemeler sırasında şirket, Fransız SA'ya potansiyel müşterilerden veri toplamak için iki form örneği sundu. Ancak, bu formların sunumu özgür iradeye dayanan ve bilgilendirici bir açık rızanın alınmasına izin vermiyordu. **Aslında, kullanıcıların onay vermelerine izin veren düğmenin, kullanıcıların onay vermemelerine izin veren düğmenin aksine daha vurgulayıcı bir şekilde yer alması veya eksik metin ve küçültülmüş boyut olarak sunulması, kullanıcıları verilerinin ortaklara aktarılmasını kabul etmeye güçlü bir şekilde teşvik etti.**

Şirket, yaptırım prosedürü sırasında Fransız SA'ya yeni bir form sundu. Bu yeni formla alınan rıza da geçerli bir rıza alınmasına izin vermiyor, dolayısıyla işleme faaliyetini her türlü yasal dayanaktan yoksun bırakıyordu.

Bu vesileyle Fransız SA, GDPR'nin iki ihlalini tespit etti:

1- Verilerin işlenmesi için yasal bir dayanağa sahip olma yükümlülüğüne uyulmaması (GDPR Madde 6)
2- İşleme faaliyetlerine ilişkin bir kayıt uygulama yükümlülüğüne uyulmaması (GDPR Madde 30)

Fransız SA yaptığı ihlal tespiti gerekçesiyle Tagadamedia'ya **75.000 Euro** para cezası verdi.

GRC LEGAL Yorumu

Dünya genelinde veri koruma otoriteleri, açık rıza kavramına odaklanarak veri komisyoncularının uygun rıza alma yolunda ilerlemesini sağlamak adına sıkı denetimler yapıyor. Fransız SA tarafından Tagadamedia'ya verilen para cezası yapılan denetimlerin yansıyan bir görüntüsü.

Şirketin ceza almasına neden olan formlar incelendiğinde ***karanlık tasarım*** kavramı karşımıza çıkıyor. Karanlık tasarım, en basit ifade ile tasarım hileleridir. İnternet sitelerinde ve uygulamalarda kullanıcıların dikkatlerini farklı yere yoğunlaştırarak onları manipüle etmek amacıyla kullanılan bu hileli arayüzler, şirketlerin kendi çıkarları ve menfaatleri lehine işlettikleri en yaygın uygulamalardan biri haline gelmiştir. Tagadamedia tarafından yürütülen onay sürecinin karanlık tasarım faaliyetlerine dayandırılması kişilerin özgür iradesini sakatlamış ve hukuka aykırı bir açık rıza teminine sebebiyet vermiştir. *Daha detaylı bilgi için, konuyla ilgili olarak yayımlamış olduğumuz Karanlık Tasarım adlı çalışmamıza LinkedIn hesabımız üzerinden ulaşabilirsiniz.*

Hollanda Hükümeti x META

Hollanda hükümeti, sosyal medya platformunun veri güvenliğini nasıl ele aldığına dair ciddi endişeler nedeniyle Facebook'tan tamamen çekilmeyi düşünüyor. Bu konuda ana şirket Meta ile yapılan görüşmelerden istenen gelişmeler elde edilemedi. Hükümete yakın kaynaklar De Telegraaf'a, resmi bir bildirinin tüm hükümeti etkileyen bir Facebook yasağı için hazırlıkları özetlediğini söyledi.

Dijitalleşme Devlet Sekreteri Alexandra Van Huffelen gazeteye yaptığı açıklamada, hükümetin Facebook'un yıllardır gizliliğe duyarlı verileri nasıl ele aldığı konusunda endişeli olduğunu doğruladı. Van Huffelen, "2017'de Hollanda Veri Koruma Kurumu (“**AP**”), Facebook'un GDPR'ı iki alanda ihlal ettiğini tespit etti: kullanıcıları bilgilendirmek ve hassas verileri işlemek". Meta’nın daha sonra düzenlemeler yaptığını ancak bu sorunu çözemediğini ve yeni sorunların ortaya çıktığını sözlerine ekledi.

Van Huffelen gazeteye verdiği demeçte, bu ve diğer ülkeler tarafından dile getirilen endişeler nedeniyle, "Hollanda hükümeti, **‘DPIA’** olarak adlandırılan Facebook Sayfalarının kullanımıyla ilgili gizlilik riskleri hakkında bir soruşturma yürüttü" dedi. Soruşturma ciddi eksiklikleri ortaya çıkardı.

Dışişleri Bakanı bunları Facebook ile görüştü, ancak bu henüz tatmin edici taahhütler veya iyileştirmelerle sonuçlanmadı. Meta, DPIA'da bulunan kusurlara dahi itiraz etti. Bu nedenle, Kasım ayında hükümet, AP'den Facebook'u kullanmaya devam etmenin güvenli olup olmadığı konusunda tavsiye istedi.

Bu tavsiyenin yakında gelmesi bekleniyor. Ancak Telegraaf'ın kaynaklarına göre, **hükümet Facebook'u yasaklamayı bekliyor ve şimdiden hazırlıklar yapıyor. Bakanlıklar, Facebook'tan çekilmenin kendileri için ne gibi sonuçları olacağını düşünüyor.**

Gazeteye göre, diğer sosyal medya platformları da bunu takip edebilir. **Van Huffelen kısa süre önce eski adı Twitter olan X'i kullanmayı bırakmaya karar verdi. Bunun kişisel bir karar olduğunu ve hükümet politikası olmadığını vurguladı.** Ancak gösterdiği nedenlerden biri, X'in iyileştirmelerinin tartışmaya ve uygulamaya açık olmamasıydı.

GRC LEGAL Yorumu

Çin platformunun oluşturduğu casusluk riskleriyle ilgili endişeler nedeniyle TikTok'u yasaklayan Hollanda hükümetinin, veri güvenliği endişeleri nedeniyle bu kez Facebook'u tamamen terk etme olasılığı ile gündemde olduğunu görmekteyiz.

Daha önce İrlanda Veri Koruma Komisyonu tarafından **1,3 milyar dolarlık** rekor cezaya çarptırılan ve kişisel veri güvenliği alanında 'sabıkalı' olarak nitelendirebileceğimiz Meta'nın GDPR ihlallerine devam ediyor olması Hollanda hükümetinin güvenlik kaygılarını haklı çıkarır niteliktedir. Meta'nın bu yöndeki gizlilik anlayışı göz önünde bulundurulduğunda Hollanda hükümetinin Facebook'u terk etme kararının, diğer ülkeler için de örnek teşkil etmesini temenni etmekteyiz.

Tüketici Savunucuları x Toyota

Tüketici savunucusu grubu olan "**Choice**", Toyota otomobillerinin konum verilerini, sürüş verilerini, yakıt seviyeleri ve hatta telefon numaraları ve e-posta adresleri gibi kişisel bilgileri topladığını ve potansiyel olarak paylaştığını söylüyor. **Choice, 'Bağlı Hizmetler' özelliğinin kişisel ve araç verilerini üçüncü taraflara gönderebileceğini ve sürücülere bileşenlerin çıkarılmasının garantiyi geçersiz kılma riski taşıdığını söyledi**.

Toyota, müşteri gizliliğini "son derece ciddiye aldığını" vurguladı, ancak **"Bağlı Hizmetler" özelliği olarak bilinen veri iletişim modülünün ("DCM") yalnızca devre dışı bırakılabileceğini, ancak araçlarından kaldırılamayacağını, aksi takdirde sürücülerin garantilerini geçersiz kılabileceğini ve Bluetooth ve hoparlörleri işlevsiz hale getirebileceğini kabul etti.**

Choice'un kıdemli kampanyaları ve politika danışmanı Rafi Alam, "Otomobil şirketleri, bu teknoloji özelliklerinin sürücü güvenliğini artırdığını söylüyor, ancak veri hackleme ve paylaşma dünyasında, tüketicilerin hoşuna gitsin ya da gitmesin, şirketlerin değerli bilgiler toplamasının başka bir yolu" dedi.

"Endişe verici bir şekilde, Toyota'nın Bağlı Hizmetler politikası, devre dışı bırakmazsanız, araştırma, ürün geliştirme ve veri analizi amacıyla kişisel ve araç verilerini toplayıp kullanacağını söylüyor" dedi. Ayrıca, **Toyota'nın politikalarının gerçekte neyin 'onay' olarak sayıldığı konusunda inanılmaz derecede belirsiz** olduğunu sözlerine ekledi.

Choice tarafından yapılan bir araştırmaya göre Matthew adlı bir müşteri, 68.000 dolarlık Toyota HiLux'u satın aldıktan birkaç ay sonra Bağlı Hizmetler özelliğinden haberdar olduğunu ve bu özelliğe kaydolmasını isteyen e-postalar almaya başladığını iddia etti.

Bu özellikten rahatsız olan müşteri bayiden arabasındaki teknolojiyi kaldırmasını (sadece devre dışı bırakmakla kalmayarak) istedi, ancak kendisine **bunun garantiyi geçersiz kılacağı ve sigortasını riske atacağı söylendiğini iddia etti**. Sonuç olarak arabayı teslim almadı ve siparişini iptal etti, ancak bayinin 2.000 dolarlık depozitosunu iade etmeyi reddettiğini iddia etti.

Alam, gizlilik sorunlarının otomobillerde yaygın bir endişe haline geldiğini, "hemen hemen her yeni araçta 'akıllı' bir bağlantı kurulu gibi göründüğünü" söyledi. Federal hükümetini, güvenlik önlemlerini güçlendirmeye ve acil olarak kişisel verilerin toplanması ve kullanılmasına ilişkin yasaklar getirmeye çağırdı. **Alam, "İnsanlar yeni bir araba satın almak için gizlilik haklarından vazgeçmek zorunda kalmamalı" dedi.**

GRC LEGAL Yorumu

Choice'un ortaya koyduğu bulgular; Toyota'nın gizlilik politikasının belirsiz olması, Bağlı Hizmetler özelliğinin devre dışı bırakılabilse de araçlardan tamamen kaldırılamaması ve bunun garantiyi geçersiz kılma ve Bluetooth ve hoparlörü işlevsiz bırakması gibi ciddi sorunları vurgulamaktadır. Nitekim, Bağlı Hizmetler özelliğinin araçtan tamamen kaldırılamaması ve diğer özelliklerin işlevsiz hale gelmesi durumlarının Toyota'nın temin ettiği hizmeti tüketicilerin kişisel verilerinin toplanması şartına bağladığı söylenebilecektir.

Toyota'nın tüketicilerin gizlilik haklarına gösterdiği duyarlılık göz önünde bulundurulduğunda ise, devre dışı bırakıldığı 'söylenilen' Bağlı Hizmetler özelliğinin verileri gerçekten toplamadığı hususunda ise endişeler giderek büyümektedir.

Fransa x Siber Saldırganlar

Fransız Veri Gizliliği İzleme Kuruluşu'nun açıklamasına göre, Fransa vatandaşlarının neredeyse yarısının verileri, sağlık bedeli ödeme hizmet sağlayıcılarında gerçekleşen büyük bir güvenlik ihlalinde ele geçirildi.

Fransız Veri Koruma Otoritesi (National Commission on Informatics and Liberty, "**CNIL**"), Ocak ayı sonunda ödeme kuruluşları olan Viamedis ve Almerys'in sistemlerinde ihlal yaşandığını ve **33 milyondan fazla** müşteriye ait verilerin çalındığını açıkladı. **Etkilenen veriler arasında doğum tarihleri, medeni hal, sosyal güvenlik numaraları ve sigorta bilgilerinin yer aldığı** ancak hiçbir banka bilgisinin, tıbbi verinin veya iletişim bilgisinin tehlikeye atılmadığı belirtildi.

Viamedis, ilgili verilerin sağlık çalışanlarını hedef alan bir **kimlik avı saldırısıyla** ele geçirildiğini ve çalınan kimlik verilerinin sisteme erişim sağlamak için kullanıldığını belirtirken Almerys veri ihlalinin nasıl gerçekleştirildiğine ilişkin bir açıklama yapmadı. Ancak ilgili ihlallerin sağlık hizmeti sağlayıcıları tarafından kullanılan bir portal aracılığıyla benzer bir şekilde gerçekleştirildiği tahmin ediliyor.

CNIL, GDPR'da öngörüldüğü üzere veri ihlalinden etkilenenlerin bilgilendirilmesini sağlamak amacıyla Viamedis ve Almerys ile birlikte çalıştıklarını ancak ülkenin neredeyse yarısını etkileyen ihlal bildiriminin gerçekleştirilmesinin zaman alacağını belirtti. Ayrıca herhangi bir kuruluşun ilgili ihlallerde kusurlu olup olmadığının tespiti amacıyla soruşturma açıldığını açıkladı. Fransız yetkililer ise ele geçirilen verilerin kimlik avı veya sosyal mühendislik saldırılarında kullanılmak üzere diğer ihlallerden elde edilen verilerle birleştirilebileceği konusunda uyarılarda bulunmaya devam etmekte.

Bilgi Köşesi

Sosyal mühendislik, bilgisayar sistemlerine veya ağlara doğrudan teknik bir saldırı gerçekleştirmek yerine, insanları manipüle ederek bilgi veya erişim elde etmeye çalışılan bir saldırı türüdür. Saldırganlar genellikle insanların doğal eğilimlerini, meraklarını, güven duygularını veya diğer duygusal zaaflarını kullanarak bilgi almaya veya insanların belirli eylemleri gerçekleştirmelerini sağlamaya çalışırlar. Örneğin, sahte bir e-posta göndererek kişisel bilgileri ele geçirebilir, telefonla arayarak gizli bilgileri çalabilir veya yanlış bir web sitesine yönlendirerek kimlik avı saldırıları gerçekleştirebilirler.

GRC LEGAL Yorumu

Fransa'da yaşanan büyük ölçekli veri ihlali, hizmet sağlayıcılarının almaları gereken kişisel veri/bilgi güvenliği önlemlerinin ne kadar önemli olduğunu bir kez daha gözler önüne sermektedir. Öyle ki ilgili ihlal sağlık hizmet sağlayıcıların sistemlerinde gerçekleşmiş olup oldukça kritik ve hassas verileri kapsamakta; ciddi mahremiyet endişelerine yol açmaktadır. Özellikle bu tür hassas veri işleyen kuruluşların, veri koruma önlemlerini en üst seviyede tutmaları ve güvenlik açıklarını sıkı bir şekilde izlemeleri hayati önem taşımaktadır.

Hong Kong x DeepFake

Hong Kong'da yaşanılan ve **şimdiye kadar gerçekleştirilen en iddialı deepfake dolandırıcılığı** olduğu tahmin edilen olayda; saldırganlar adı açıklanmayan bir şirket çalışanını, CFO'nun ve diğer personellerin simülasyonlarının yer aldığı sahte bir video konferans aracılığıyla 25 milyon dolar transfer etmeye ikna etti. Her ne kadar deepfake ses içeren dolandırıcılık türünün giderek yaygınlaştığı bir gerçek olsa da skandala sebep olan bu olay birden fazla kişinin sahte temsillerinin kullanıldığı ilk vaka olma özelliğini taşıyor.

Vakada sahte temsillerine yer verilen çalışanların tümünün kamuya açık bilgileri, sesleri ve görüntülerinin mevcut olduğu; hedef alınan çalışanın ilk başta dolandırıcılıktan şüphelendiği ancak sonuçta **toplamda 25 milyon dolar değerinde on beş banka transferi** yaptığı biliniyor.

Ayrıca konuya ilişkin şimdiye kadar yapılan açıklamalar doğrultusunda; hedef alınan çalışanın, şirketin CFO'su olduğunu iddia eden dolandırıcıdan **kimlik avı e-postası aldığı**, ilgili e-postanın içeriğinde gizli bir işlem yapılacağının belirtildiği, çalışanın şüphelenmesi üzerine dolandırıcı tarafından kontrol edilen sahte video grup sohbetine alınarak ikna edildiği ve sahte video grup sohbetinde CFO ile şirket çalışanlarının simülasyonunun bulunduğu, gerçeğin ise ancak bir hafta sonra çalışanın işlemler hakkında şirketin merkez ofisine başvurmasıyla ortaya çıktığı bilinmekte.

Olayla ilgili kamuoyuna açıklama yapan Hong Kong polisi, kendi yetki alanlarında deepfake dolandırıcılık faaliyetlerinin arttığını belirterek 2023 yılında yüz tanıma sistemini kandırmak amacıyla deepfake videolarının kullanıldığı en az 20 dolandırıcılık vakası bulunduğunu, habere konu dolandırıcılık vakası ile ilgili henüz herhangi bir tutuklama yapılmadığını ve soruşturmanın devam ettiğini ifade etti.

Bilindiği üzere, yapay zekâ halihazırda her türlü siber suçu ve dolandırıcılığı geliştirmek için kullanılıyor. Bazı saldırganlar dolandırıcılık mesajları ve e-postalarında kurbanların şüphelenmesine sebep olan hatalarını ChatGPT gibi yapay zeka araçları ile düzeltirken bazı saldırganlar ise yapay zekayı kötü amaçlı kod yazması için eğitiyor. **Hong Kong deepfake dolandırıcılığının da gösterdiği gibi, şu ana kadarki en büyük ilerleme sahte ses alanında yaşandı.**

Artık, yalnızca birkaç konuşma cümlesinden birinin sesinin ikna edici bir kopyasını oluşturabilecek araçlar mevcut; bu durum özellikle tanınmış kişiler veya şirket temsilcileri için büyük tehlike arz ediyor. **Microsoft'un yeni VALL-E aracı, bir sesi üç saniye kadar kısa bir sürede kopyalayabiliyor.** Bu gelişmeler, suçluların aile üyesi gibi davranarak acil durum olduğu iddiasıyla para istenilen telefon görüşmesi dolandırıcılıklarında da patlamaya yol açtı.

Yüz tanıma sistemlerinin de deepfake dolandırıcılıklarına karşı özellikle savunmasız olduğu görülüyor; öyle ki biyometrik yüz tanımanın gelecekte uygulanabilirliğini sorgulanıyor. Gartner firması tarafından yakın zamanda yapılan bir analiz, yapay zekâ destekli deepfake saldırıları nedeniyle çok çeşitli biyometrik doğrulama sistemlerinin 2026 yılına kadar güvenilmez hale geleceğini ve kuruluşların %30'unun verimsizlik nedeniyle bu yöntemleri terk edeceğini öngörüyor.

GRC LEGAL Yorumu

Geçtiğimiz aylarda Kurum'un da yayımlamış olduğu bilgi notu ile tanımına açıklık getirilen deepfake uygulamasının, Hong Kong'da yaşanılan skandaldan da anlaşıldığı üzere dünya çapında büyük yankılar yarattığı görülmektedir. Bu doğrultuda gerek özel yaşamlarında bireylerin gerekse de şirketlerin, deepfake uygulamalarına karşı bilinçlenmeleri büyük çaplı veri ihlallerinin önüne geçilebilmesi adına önem arz edecektir.

Özellikli olarak şirketler nezdinde nitelikli maddi kayıplara yol açabilecek deepfake saldırılarına karşı şirketlerin siber güvenlik operasyonlarını ve şirket içi iletişim kanallarını güçlendirmeleri etkili bir adım olacaktır. Buna ek olarak, para ve bilgi transferleri gibi önemli işlemler için çoklu onay seviyeleri uygulanmalı ve bireylerin deepfake gerçeğini gözeterek şüpheli talepleri sorgulamaktan çekinmemeleri adına eğitilmeleri hayatidir.