KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ SEÇİLMİŞ GÜNCEL GELİŞMELER-36

* Avrupa Veri Koruma Kurulu (EDPB), 2002/58/EC sayılı e-Gizlilik Direktifi'nin 5/3 maddesi kapsamında değerlendirilebilecek takip teknolojilerine ilişkin açıklamalarda bulunulan ve 2023 yılı içerisinde kamuoyu görüşüne açılan Rehber'in son versiyonunu yayımladı[1]. E-Gizlilik Direktifi'nin 5/3 maddesinin farklı teknik çözümlere uygulanabilirliğinin ele alındığı Rehber'de, anılan maddenin çerezlerin yerini alabilecek veya yeni iş modelleri yaratabilecek yeni izleme yöntemlerine uygulanmasına ilişkin belirsizliklerin giderilmesi amaçlanmaktadır.

  Bu kapsamda Rehber içerisinde; "bilgi", "abonenin veya kullanıcının terminal ekipmanı", "halka açık iletişim ağı", "erişim sağlanması" ve "bilginin depolanması ve depolanan bilgi" kavramları analiz edilmekte ve URL-piksel takibi, yerel işleme, yalnızca IP adresine dayalı izleme, aralıklı ve aracılı nesnelerin interneti raporlaması ile benzersiz tanımlayıcılar gibi yaygın izleme tekniklerini içeren kullanım senaryolarına yer verilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), GDPR kapsamında bir veri işleme şartı olarak "meşru menfaat"in hangi durumlarda ne şekilde uygulanabileceğine ilişkin bir içerik paylaştı[2]. Genel olarak bakıldığında, bahse konu işleme şartına dayanılabilmesi için dikkate alınması ve bir arada bulunması gereken üç koşul şu şekilde belirtilmektedir:

  - Veri sorumlusunun veya üçüncü bir tarafın meşru menfaatinin olup olmadığı netleştirilmelidir. Bu menfaat, kuruluşun gerçek faaliyetlerle ilgili olmalı ve AB ya da üye devlet düzenlemelerine aykırı olmamalıdır. Ayrıca, veri işleme tarihinde geçerli, açık ve somut bir menfaat bulunmalıdır. Diğer bir ifadeyle bahse konu menfaat, varsayımsal bir şekilde belirlenmemelidir.

  - Bahse konu işlemenin, meşru menfaat için gerçekten gerekli olup olmadığı değerlendirilmelidir. Bu değerlendirme yapılırken, meşru menfaatin elde edilmesi için bireylerin temel hak ve özgürlüklerini daha az kısıtlayıcı yollarla amaca ulaşılıp ulaşılamayacağı dikkate alınmalıdır. İşleme, yalnızca belirlenen meşru menfaatin gerektirdiği ölçüde yapılmalı ve veri minimizasyonu ilkesine riayet edilmelidir.

  - Bireylerin temel hak ve özgürlüklerinin, söz konusu meşru menfaat karşısında üstün gelip gelmediği değerlendirilmelidir. Bu değerlendirme sırasında, bireylerin ilgili kuruluşla olan ilişkilerinden doğan makul beklentileri de göz önünde bulundurulmalı ve işlemenin etkisini sınırlandıran hafifletici önlemler alınmalıdır.

* G7 ülkelerinin dijital kimliğe ilişkin yaklaşımlarındaki ortak noktaların belirlendiği bir rapor OECD tarafından yayımlandı[3]. Önümüzdeki süreçte birlikte çalışabilirlik çalışmalarını desteklemesi amacıyla hazırlanan Rapor'da; konuya ilişkin kavramlar ve tanımlar, uluslararası teknik standartların kullanımı ve güvence düzeylerine yönelik yaklaşımlara yer verilmektedir.

* Avrupa İnsan Hakları Mahkemesi, "Yeni Teknolojiler"in ele alındığı kararlara ilişkin bilgi notunun güncellenmiş versiyonunu yayımladı[4]. Derleme kapsamında;

  - Kitaplar ve müzik eserlerinin telif hakkı,
  - Elektronik veriler,
  - E-posta,
  - Yüz tanıma teknolojisi,
  - GPS,
  - Radyo veya telekomünikasyona müdahale,
  - İnternet,
  - IP adresleri,
  - Mobil uygulamalar,
  - Cep telefonları,
  - Çevrim içi taciz,
  - Uydu antenleri,
  - Gizli kameraların kullanımı,
  - Video ile izleme başlıkları altında çeşitli karar özetlerine yer verilmektedir.

* Dünya Ekonomik Forumu, gelişmekte olan teknolojilerle ilişkili riskler ve fırsatların incelendiği, bu kapsamda siber dayanıklılığı artırmak adına veri odaklı iç görülerin paylaşıldığı ve çeşitli önerilerin sunulduğu bir çalışma yayımladı[5].

  Geleneksel "tasarımda güvenlik" *(security by design)* yaklaşımının, karmaşık ve gelişen tehdit ortamı karşısında yetersiz kalması nedeniyle "tasarımda dayanıklılık" *(resilience by design)* yaklaşımının benimsenmesine yönelik acil bir gereksinim bulunduğuna vurgu yapılan Çalışma'nın temel bulguları arasında şu hususlar yer almaktadır:

  - Genişleyen Teknolojik Ortam: Günümüzün dijital ekosistemini şekillendiren ve gelişmekte olan 200'den fazla teknoloji, bu teknolojilerin değerlendirilmesi ve buna uygun güvenlik stratejileri geliştirilmesinde geniş ve kapsayıcı bir yaklaşım gerektirmektedir.

  - Artan Saldırı Yüzeyi: Bağlı cihazların sayısının 2030 yılına kadar 32 milyarı aşacağı tahmin edilmekte olup bu durum, siber saldırıların potansiyel giriş noktalarının önemli ölçüde artmasına neden olmaktadır.

  - Yapay Zekâya Özgü Tehditler: Veri zehirlenmesi ve model manipülasyonu gibi yapay zekâya özgü saldırıların önlenmesi, stratejilerin güncellenmesi ve sürekli bir şekilde yenilenmesini gerektirmektedir.

  - Kuantum Hesaplama Riskleri: Kuantum teknolojisi, mevcut şifreleme yöntemleri için önemli tehditler oluşturduğundan, kuantum dirençli kriptografi çözümleri geliştirilmesine duyulan ihtiyaç artmaktadır.

  - Tedarik Zinciri Zafiyetleri: Bilgi ve iletişim teknolojileri tedarik zincirlerinin karmaşık ve küresel yapısı, bunları siber tehditler için birincil hedef hâline getirdiğinden, tüm zincir boyunca kapsamlı güvenlik önlemleri alınması gerekmektedir.

  - Düzenleyici Zorluklar: Teknolojik ilerlemelerin hızının, mevcut düzenleyici çerçevelerin önüne geçtiği dikkate alınarak inovasyonu ve güvenliği dengeleyen esnek, uyarlanabilir düzenlemelere ihtiyaç bulunmaktadır.

  - Yetkinlik Açığı: Gelişen teknolojiler konusunda uzmanlığa sahip siber güvenlik profesyonellerinin eksikliği, bu sistemlerin ortaya çıkardığı tehditlere yanıt vermede önemli zorluklara neden olmaktadır.

Bu kapsamda geliştirilen öneriler arasında ise;

- Yenilikçi çözümler oluşturmak üzere sürekli bir şekilde araştırma ve geliştirmeye yatırım yapılması,

- Siber güvenlik zorluklarının ele alınmasını sağlamak adına hükümet, endüstri ve akademi arasındaki iş birliğinin güçlendirilmesi,

- Güvenlik ve dayanıklılığın tasarıma entegre edilmesini teşvik eden ve uluslararası iş birliğini kolaylaştıran düzenleyici çerçeveler geliştirilmesi,

- Kapsamlı ve etkili siber dayanıklılık planlaması yapılması ve olay müdahale planlarının düzenli olarak test edilmesi,

- Gelişmekte olan teknolojilerin sorumlu bir şekilde geliştirilmesi ve kullanılmasına yönelik sağlam yönetişim yapıları kurulması,

- Siber güvenlik stratejilerinin, yeni teknolojilerin ortaya çıkardığı tehditlere göre uyarlanması gibi hususlar sayılmaktadır.

* Avrupa Birliği genelinde siber güvenlik risklerine karşı daha dirençli bir ekosistem oluşturulması amacıyla hazırlanan ve 16.01.2023 tarihinde yürürlüğe giren 2022/2555 sayılı NIS2 Direktifinin, üye devletlerin iç hukuklarına aktarılması için belirlenen süre 17.10.2024 tarihinde sona ermiş olup yine bu tarihte Avrupa Komisyonu, NIS2 Direktifi kapsamında ilk uygulama kurallarının kabul edildiğini duyurmuştur[6].

* Avustralya Veri Koruma Otoritesi (OAIC), yapay zekâ ürünlerinden faydalanarak ürün veya hizmet sunan kuruluşlarca dikkat edilmesi gereken hususlara yönelik tavsiyelerin yer aldığı bir rehber yayımladı[7]. Kuruluşların, ticari olarak sunulan yapay zekâ ürünlerini kullanırken gizlilik yükümlülüklerine uymalarına yardımcı olunması amaçlanan Rehber'den çıkarılabilecek başlıca noktalar şu şekildedir:

  - Gizlilik yükümlülükleri, bir yapay zekâ sistemine girilen tüm kişisel bilgiler ve yapay zekâ tarafından üretilen çıktılar (kişisel bilgileri içeriyorsa) için geçerlidir. Ticari olarak sunulan bir yapay zekâ ürününü kullanmayı düşünen kuruluşların, ürünün amaçlanan kullanımlara uygun olduğundan emin olmak için gerekli özeni göstermeleri önem taşımakta olup bu kapsamda ürünün öngörülen kullanımlara yönelik test edilip edilmediği, insan gözetiminin süreçlere nasıl entegre edilebileceği, potansiyel gizlilik-güvenlik riskleri ve kimlerin bu verilere erişim sağlayabileceği gibi hususlar göz önünde bulundurulmalıdır.

  - Kuruluşların gizlilik politikaları ve bildirimleri, yapay zekâ kullanımına ilişkin açık ve şeffaf bilgiler içerecek şekilde güncellenmelidir. Ayrıca, şeffaflığın ve gizliliğin korunmasını sağlamak için yapay zekâ sistemlerinin kullanımı konusunda uygun politika ve prosedürler oluşturulmalıdır.

  - Kişisel bilgi üretmek veya çıkarımlarda bulunmak için yapay zekâ kullanıldığı durumda, kuruluşlar Avustralya Gizlilik İlkelerine (APP) uygun hareket etmelidirler. Diğer yandan, yapay zekâ modelleri tarafından üretilen çıkarımsal, hatalı veya yapay olarak oluşturulan bilgiler (halüsinasyon veya deepfake gibi), belirli veya makul ölçüde belirlenebilir bir bireyle ilgili olduğu durumda, bu bilgilerin işlenmesinde Avustralya Gizlilik İlkelerine riayet edilmelidir.

  - Kişisel bilgilerin bir yapay zekâ sistemine girilmesi durumunda bu bilgiler, yalnızca toplandıkları amaca uygun olarak kullanılmalıdır. Bunun dışındaki bir kullanım, ancak bireyin rızasının olması ya da ikincil kullanımın birey tarafından makul bir şekilde beklenebilir olması ve birincil amaçla ilişkili (hassas bilgiler için ise doğrudan ilişkili) olması durumunda mümkün olabilmektedir.

  - Otorite tarafından iyi uygulama örneği olarak; önemli ve karmaşık gizlilik riskleri taşımaları nedeniyle, hassas nitelikli bilgiler başta olmak üzere kişisel bilgilerin kamuya açık üretici yapay zekâ araçlarına girilmemesi önerilmektedir.

* Avustralya Veri Koruma Otoritesi (OAIC), üretici yapay zekâ modelleri veya sistemleri geliştiren taraflarca dikkat edilmesi gereken hususlara yönelik tavsiyelerin yer aldığı bir rehber yayımladı[8]. Kişisel bilgileri kullanarak üretici yapay zekâ modellerini eğiten veya ince ayar yapan kuruluşların gizlilik yükümlülüklerine uymalarına yardımcı olunması amaçlanan Rehber'den çıkarılabilecek başlıca noktalar şu şekildedir:

  - Geliştiriciler, üretici yapay zekâ modellerinin doğruluğunu sağlamak için, yüksek kaliteli veri kümelerini kullanmak ve uygun testleri yapmak da dâhil olmak üzere, makul adımları atmalıdırlar. Yapay zekâ kullanımının getirdiği risk düzeyine bağlı olarak, modellerin doğruluğunu sağlamak için gerekli önlemler alınmalıdır ve yüksek risk taşıyan kullanımlarda ek güvenlik önlemleri uygulanmalıdır.

  - Verilerin kamuya açık veya başka bir şekilde erişilebilir olması, bunların üretici yapay zekâ modelleri ya da sistemlerini eğitmek veya ince ayar yapmak için kullanılmasının hukuka uygun olduğu anlamına gelmemektedir. Geliştiriciler, kullanmayı veya toplamayı amaçladıkları verilerin (kamuya açık veriler de dâhil) kişisel bilgi içerip içermediğini değerlendirmeli ve gizlilik yükümlülüklerine uygun hareket etmelidirler. Bu yükümlülüklerin karşılanabilmesi için (örneğin, bilgilerin silinmesi gibi) atılması gereken ek adımlar bulunup bulunmadığı değerlendirilmelidir.

  - Geliştiriciler, hassas nitelik taşıyan bilgiler konusunda özellikle dikkatli olmalıdırlar. Bu çerçevede, bilgilerin bireyden rıza alınmaksızın web üzerinden kazınması veya üçüncü bir tarafın veri kümesinden elde edilmesinin hukuka aykırılık teşkil edebileceği ihtimali üzerinde durulmalıdır.

  - Geliştiriciler, hâlihazırda sahip oldukları kişisel bilgileri bir yapay zekâ modelini eğitmek amacıyla kullanmayı planladıklarında, bunun toplama amacına uygun olup olmadığını değerlendirmelidirler. İkincil kullanım için bireyden rıza alınmadığı durumda, bu kullanımın birey tarafından makul bir şekilde beklenip beklenemeyeceğinin ve ilk toplama amacı ile arasındaki ilişkinin boyutu (hassas bilgiler için ise doğrudan ilişkili olup olmadığı) dikkatli bir şekilde değerlendirilmelidir.

  - Yapay zekâ ile ilgili ikincil kullanımın, ilk toplama amacına uygunluğu ve bunun birey tarafından makul olarak beklenebilir olup olmadığı hususları açık bir şekilde ortaya konulamadığında, bu kullanım için rıza alınmalı ve/veya bireylere bu kullanımdan vazgeçme konusunda anlamlı ve bilgilendirilmiş bir seçenek sunulmalıdır.

* Avrupa Komisyonu, "Çocuklar için Daha İyi İnternet" *(Better Internet for Kids-BIK)* portalının yenilenen versiyonunun kullanıma sunulduğunu duyurdu[9]. Çevrim içi güvenliğe yönelik kapsamlı bir bilgi kaynağı sunan portal, dijital dünyada güvenli ve bilinçli bir şekilde hareket edebilmeleri amacıyla çocuklar, ebeveynler, eğitimciler ve politika yapıcılara rehberlik sağlamaktadır.

  Portala eklenen "Ebeveyn ve Bakıcılar Köşesi"; ekran süresi yönetimi, oyun bağımlılığı ve ebeveyn kontrolleri gibi konularda yol gösterici bilgiler sunarken, popüler uygulamalar ve sosyal medya platformlarına ilişkin çeşitli güncel kaynakları da içermektedir. "Gençlik Köşesi"nde ise gençlerin çevrim içi güvenlik konusundaki farkındalıklarının artırılması ve bu alanda aktif bir şekilde rol almalarının teşvik edilmesi amaçlanmaktadır.

  Diğer yandan bahse konu portalda, çocukların çevrim içi güvenliğine yönelik merkezi bir bilgi erişim noktası olarak hizmet veren "BIK Bilgi Merkezi" ile ilgili çeşitli bilgiler de paylaşılmaktadır.

* Birleşik Krallık Veri Koruma Otoritesi (ICO) tarafından yürütülen *"Children's Data Lives"* projesine ilişkin rapor yayımlandı[10]. Çocukların çevrim içi dünyadaki davranışları ve bu davranışların kişisel verilerin korunmasına ilişkin haklarla nasıl kesiştiği konusunda temel bir anlayış sunulması amaçlanan projede, çocukların veri mahremiyetine ilişkin farkındalıkları ile mahremiyetin korunmasına verdikleri önem araştırılmaktadır.

  9 ila 17 yaş arasındaki 30 çocuğun günlük yaşamlarının gözlemlendiği bu uzun vadeli proje kapsamında ulaşılan temel bulgulardan bazıları şu şekildedir:

  - Çocuklar kimi zaman, mahremiyetlerine önem verdiklerini düşündüren şekillerde davransalar dahi verilerinin korunmasına ilişkin sahip oldukları hakların nadiren farkındadırlar. Diğer yandan, çocukların yaşamlarının giderek daha fazla çevrim içi hâle gelmesi ile birlikte verilerini paylaşmaları sıradanlaştığından, çoğu zaman bu davranışı "veri paylaşımı" olarak görmemektedirler.

  - Yaş gruplarına göre çocukların davranışları farklılık göstermektedir. Örneğin, küçük yaş grubundaki çocuklar (9-11) teknolojiyi oyun ve eğlence aracı olarak görürken; daha büyük yaştaki çocuklar sosyal statüye ve arkadaş ağı oluşturmaya odaklanmaktadırlar. Bu şekilde bir sosyal motivasyon, belirli noktalarda gizliliğin korunmasını teşvik etse de beğeni, görüntülenme ve popüler uygulamalara erişim isteği gibi durumlar veri mahremiyeti ile çatışabilmektedir.

- Çocuklar açısından konum paylaşımı, aile ve arkadaşlar ile bir yakınlık göstergesi veya ilgi belirtisi olarak algılanmaktadır. Özellikle daha büyük yaştaki çocuklar için, ilişkileri sürdürmenin kabul görmüş ve hatta beklenen bir yönü hâline geldiği anlaşılmaktadır.

- Çocukların platformları kullanma isteği, gizlilik politikalarını göz ardı etmelerine neden olmaktadır. Diğer yandan, verilerine erişilmesi riski soyut bir durum olarak algılanmakta ve şirketlerle veri paylaşımı, genellikle uygulamalara veya hizmetlere erişmek ve bunları kullanmak için gerekli bir adım olarak düşünülmektedir. Ayrıca gizlilik politikalarının görünür olmaması, karmaşık bir şekilde hazırlanmış olması veya bazı platformların çocuklara hitap eden oyun benzeri tasarımlarının veri paylaşımını bir eğlence unsuru gibi göstermesi, çocukların kararları üzerinde etkili olabilmektedir.

- Gerekli kontrolleri ayarlama ve çocukları izleme sorumluluğunun çoğu ebeveynlere aittir. Bu araştırmada yer alan ebeveynlerin, çocuklarının çevrim içi güvenliği konusundaki endişelerinin (kandırılma, uygunsuz içeriklere maruz kalma, çevrim içi zorbalığa uğrama gibi), çocuklarının verilerinin kötüye kullanılması olasılığı ile ilgili endişeleri gölgede bıraktığı görülmektedir. Öte yandan, çocuklarının sosyal hayatta zorluk çekebileceği kaygısı ile bazı ebeveynlerin, çocuklarının platformlara erişimini sağlamak için yaş sınırlamalarını aşmalarına dahi göz yumabildikleri görülmektedir.

* 30.10.2024 tarih ve (mükerrer) 32707 sayılı Resmî Gazete'de yayımlanan "2025 Yılı Cumhurbaşkanlığı Yıllık Programı"nda belirtilen hususlar arasında, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Avrupa Birliği Veri Koruma Tüzüğü (GDPR) ile uyumlaştırılmasına yönelik çalışmaların tamamlanacağı (Tedbir 359.2.)da yer almaktadır[11].

* Kişisel Verileri Koruma Kurulunun 17.10.2024 tarih ve 2024/1793 sayılı kararı ile, veri sorumlusu ve veri işleyenlerin bildirim yükümlülüklerini internet üzerinden daha hızlı ve etkin bir biçimde yerine getirebilmeleri amacıyla hazırlanan "Standart Sözleşme Bildirim Modülü" vasıtasıyla bildirimlerin yapılabilmesine karar verilmiş olup; söz konusu modül ilgililerin kullanımına sunulmuştur[12]. Standart Sözleşme Bildirim Modülü ekranları ile ilgili detaylı bilgilerin yer aldığı Kılavuza da ilgili Modül üzerinden ulaşılabilmektedir[13].

* Norveç'te sosyal medya kullanım yaşının 15'e çıkarılması planlanıyor[14]. Sosyal medya kullanımına ilişkin olarak ülkede hâlihazırda asgari yaş sınırı 13 olsa da Norveç Medya Otoritesi tarafından yapılan araştırmaya göre, 9 yaşındaki çocukların yarısından fazlası, 10 yaşındaki çocukların %58'i ve 11 yaşındaki çocukların %72'si sosyal medyayı kullanıyor.

  Bu kapsamda, Hükümet'in çocukların yaş sınırlamalarını aşmasını önlemek amacıyla ek güvenlik önlemleri almayı planladığı; bunlar arasında, sosyal medya platformlarının kullanıcıların kişisel verilerini işleyebilmesi için kullanıcının en az 15 yaşında olmasını gerektirecek şekilde kişisel verilerin korunması mevzuatında değişiklik yapılması ve sosyal medya için bir yaş doğrulama bariyeri geliştirilmesi gibi unsurların yer aldığı belirtilmektedir.

* Dünyanın en büyük yayınevlerinden birisi olan Penguin Random House'un (PRH), telif hakkıyla korunan çalışmalarının büyük dil modelleri ve diğer yapay zekâ araçlarını eğitmek için kullanılmasını önlemek amacıyla telif hakkı sayfalarındaki ifadeleri güncellediği bildirildi[15]. Yeni ifade, tüm yeni eserlere ve yeniden basılan eserlere dahil edilecek.

  PRH tarafından küresel olarak tüm baskılarda kullanılacak olan telif hakkı beyanında; *"...Bu kitabın hiçbir bölümü, yapay zekâ teknolojileri veya sistemlerinin eğitilmesi amacıyla hiçbir şekilde kullanılamaz veya çoğaltılamaz. 2019/790 sayılı Dijital Tek Pazar Direktifi'nin 4(3) maddesi uyarınca, PRH bu eseri metin ve veri madenciliği istisnasından açıkça kapsam dışı bırakır."* ifadesi yer alıyor.

* Kaliforniya'da yaşlı bir adam, yapay zekâ ile oğlunun sesinin taklit edilmesi sonucu, oğlunun korkunç bir kazaya karıştığını ve hapisten kefaletle çıkmak için paraya ihtiyacı olduğunu düşünerek dolandırıcılara 25.000 dolar kaptırdı[16]. Telefonda duyduğu sesin, oğlunun sesiyle tamamen aynı olduğunu iddia eden adam, panikle harekete geçerek dolandırıcıların taleplerini yerine getirdi.

  Bu olay, yapay zekâ kullanılarak yapılan dolandırıcılıklara karşı dikkatli olmanın ve acil para talepleri karşısında durumun doğruluğunu farklı kanallardan teyit etmenin önemini bir kez daha göstermektedir.

* Polonya'da, bünyesinde çalışan gazetecileri işten çıkaran ve yapay zekâ tarafından oluşturulan "sunucular" kullanarak yayın hayatına devam edeceğini açıklayan "OFF Radio Krakow", gelen tepkiler üzerine bu karardan vazgeçildiğini duyurdu[17]. Radyo istasyonunun editörü tarafından yapılan açıklamada, yapay zekâ tarafından oluşturulan sunucuların kullanımının esasen bir "deney" olduğu ve üç ay sürmesi planlanan bu deneyin yoğun tepkiler nedeniyle yalnızca bir hafta sürebildiği belirtildi.

  Bu karar alınmadan önce, yakın zamana kadar radyo istasyonunda program yapmış olan bir gazeteci, çalışanların yapay zekâ ile değiştirilmesine karşı çıkan açık bir mektup yayımlamış ve bunun "herkesi etkileyen tehlikeli bir emsal" teşkil ettiğine dikkat çekmişti. Medya sektörü ve yaratıcı endüstrilerde yıllar boyu tecrübe kazanmış kişilerin makinelerle değiştirilmesi riskine vurgu yapan bu çağrı, ülke genelinde büyük yankı uyandırmış ve 23.000'den fazla kişi tarafından imzalanmıştı.

İLGİLİ LİNKLER

[1]https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en, 16.10.2024.

[2]https://www.linkedin.com/posts/eu-edpb_summary-legitimate-interest-when-and-how-activity-7256583210472501248-40WA?utm_source=share&utm_medium=member_desktop, 28.10.2024.

[3]https://www.oecd.org/en/publications/g7-mapping-exercise-of-digital-identity-approaches_56fd4e94-en.html, 15.10.2024.

[4]https://www.echr.coe.int/documents/d/echr/FS_New_technologies_ENG, Ekim 2024.

[5]https://www.weforum.org/publications/navigating-cyber-resilience-in-the-age-of-emerging-technologies-collaborative-solutions-for-complex-challenges/, 16.10.2024

[6]https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342, 17.10.2024.

[7]https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products, 23.10.2024.

[8]https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models, 23.10.2024.

[9]https://digital-strategy.ec.europa.eu/en/news/something-bik-has-happened, 22.10.2024.

[10]https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/children-s-data-lives-research/, Ekim 2024.

[11]https://www.resmigazete.gov.tr/eskiler/2024/10/20241030M1-1.pdf, 30.10.2024.

[12]https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu, 25.10.2024.

[13]https://standartsozlesme.kvkk.gov.tr/sharedFolder/kullanim-kilavuzu.pdf?v=190123456, Ekim 2024.

[14]https://www.theguardian.com/world/2024/oct/23/norway-to-increase-minimum-age-limit-on-social-media-to-15-to-protect-children, 23.10.2024.

[15]https://www.thebookseller.com/news/penguin-random-house-underscores-copyright-protection-in-ai-rebuff, 18.10.2024.

[16]https://nypost.com/2024/10/18/us-news/scammers-swindle-elderly-california-man-out-of-25k-by-using-ai-voice-technology-to-claim-his-son-was-in-horrible-accident-needed-money-for-bail-absolutely-his-voice/, 18.10.2024.

[17]https://apnews.com/article/poland-media-radio-ai-bba6beb01d523c6727d650c69da14960, 28.10.2024.