Hazırlayan: Avukat Yalçın TORUN | Bülten Tarihi: 17 Mart 2026

Özel Nitelikli Kişisel Verileri Koruma Rejimi: Biyometrik Veriler ve Sağlık Verileri

Avukat Yalçın Torun

Torun Hukuk Bürosu — Kişisel Veriler ve Anayasa Hukuku Birimi

yalcintorun1966@gmail.com | https://yalcintorun.av.tr

Özet

Kişisel verilerin bir alt kümesi olarak hassas (özel nitelikli) veriler, olası zararın büyüklüğü nedeniyle güçlendirilmiş bir koruma rejimine tabidir. Bu makale, KVKK'nın 6. maddesi ve Avrupa Veri Koruma Tüzüğünün GDPR'ın 9. maddesi kapsamındaki hassas veri kategorilerini —özellikle biyometrik ve sağlık verilerini— kapsamlı biçimde incelemektedir. Biyometrik verinin tanımı, özellikleri ve bu verilerin doğrulama ile kimlik belirleme amacıyla kullanılmasının yarattığı riskler analiz edilmektedir. Sağlık verilerinin işlenmesinde hasta mahremiyeti ile kamusal sağlık çıkarları arasındaki denge ele alınmakta; elektronik sağlık kayıtlarının ve e-nabız sisteminin hukuki boyutları tartışılmaktadır. KVK Kurul kararları ve AİHM içtihadı bu hassas veri kategorilerinin pratiğe yansıması bağlamında sistematik biçimde değerlendirilmektedir.

Anahtar Kelimeler: Hassas kişisel veri, biyometrik veri, sağlık verisi, KVKK m. 6, GDPR m. 9, e-nabız, elektronik sağlık kaydı, genetik veri, KVK Kurul kararları, hasta mahremiyeti.

1. Giriş

Hassas kişisel veriler, potansiyel zararının büyüklüğü nedeniyle veri koruma hukukunda özel bir statüye sahiptir. Sağlık verilerinin ifşası iş kaybına, sosyal dışlanmaya veya ayrımcılığa yol açabilir; biyometrik verilerin çalınması ise geri dönüşü olmayan kimlik hırsızlıklarına zemin hazırlar. KVKK'nın 6. maddesi, bu özel statüyü tanıyarak özel nitelikli verilerin işlenmesini katı kurallara bağlamakta ve yalnızca sınırlı sayıda istisna gerekçelerle işlenmesine imkan sağlamaktadır. Diğer bir ifadeyle özel nitelikli kişisel verilerin işlenmesi yasaktır. KVKK'nun 6/3 fıkrasında mevcut sınırlı sayıdaki durumda özel nitelikli kişisel verilerin işlenmesi mümkündür.

Dijital dönüşümün hızlanmasıyla birlikte biyometrik veriler —parmak izi, yüz tanıma, ses tanıma, iris tarama— günlük hayatın her alanına sızmıştır. Akıllı telefonların kilit ekranı yüz tanımayla açılmakta; kurumsal güvenlik sistemleri parmak izi okumaya dayanmakta; sağlık verileri ise devlet ve özel sektör veri tabanlarında merkezi biçimde depolanmaktadır. Bu gelişmeler, özel nitelikli kişisel veri korumasının teorik çerçevesinin ötesinde somut pratik sorunlar doğurmaktadır.

2. Özel Nitelikli Veri Kategorileri

2.1. KVKK'da Özel Nitelikli Veri Kategorileri

KVKK'nın 6. maddesi on iki hassas veri kategorisi saymaktadır: Irk, etnik köken, siyasi düşünce, felsefi inanç, din ve mezhep, kılık ve kıyafet, dernek-vakıf-sendika üyeliği, sağlık ve cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleri ile biyometrik ve genetik veriler. Bu liste sınırlı sayı (numerus clausus) ilkesine tabidir; kanunda yer almayan bir veri kategorisi bu madde kapsamında işlenemez. Ancak öğretide bazı yazarlar, teknolojik gelişmeler karşısında listenin yetersiz kaldığını; konum verisi ve finansal profilleme gibi yeni veri kategorilerinin de özel nitelikli kişisel veri statüsüne alınmasının tartışılması gerektiğini savunmaktadır.

2.2. Biyometrik Verinin Hukuki Niteliği

Biyometrik veri, bir kişiyi biyolojik veya davranışsal özellikleri aracılığıyla benzersiz biçimde tanımlamaya olanak veren teknik yöntemlerle işlenen fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin kişisel veridir. GDPR'ın 4/14. maddesi bu tanımı kullanmaktadır; KVKK m. 6 ise biyometrik veriyi tanımlamamakla birlikte onu özel nitelikli kategori olarak sınıflandırmaktadır. Biyometrik verinin en kritik özelliği, değiştirilemez niteliğidir: Parmak izi, iris yapısı veya yüz geometrisi, şifre ya da kart bilgisinin aksine değiştirilemez. Bu nedenle biyometrik veri ihlalinin sonuçları, diğer veri türlerine kıyasla çok daha kalıcı ve onarılması güç zararlar doğurmaktadır.

KVK Kurulu, yüz tanıma sistemiyle kişisel veri işlenmesine ilişkin çeşitli kararlarında biyometrik veri işlemenin zorunlu olmayan durumlarda gerçekleştirilmesini hukuka aykırı bulmuştur. Özellikle okul ve alışveriş merkezi girişlerinde yüz tanıma sistemlerinin kullanılması bu kapsamda değerlendirilmiş; alternatif ve daha az müdahaleci yöntemlerin tercih edilmesi gerektiği vurgulanmıştır. Bu kararlar ölçülülük ilkesinin biyometrik veri alanındaki tezahürü olarak değerlendirilebilir.

3. Sağlık Verilerinin Özel Koruma Rejimi

3.1. Sağlık Verisinin Önemi ve Koruma Gerekçesi

Sağlık verileri, olası ayrımcılık ve damgalama (stigmatization) potansiyeli nedeniyle hassas veri kategorileri içinde en kritik olanlardan biridir. Bir kişinin kronik hastalığı, psikolojik durumu, HIV statüsü veya genetik yatkınlıkları; iş hayatı, sigorta işlemleri, sosyal ilişkiler ve aile ortamı üzerinde yıkıcı etkiler doğurabilir. AİHM, Z - Finlandiya (1997) kararında sağlık verilerinin özel hayat hakkının en hassas alanlarından birini oluşturduğunu açıkça teyit etmiştir. Bu kararda AİHM HIV pozitif bir başvurucunun

tıbbi kayıtlarının mahkemece ifşa edilmesinin, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi (özel hayata saygı) kapsamında hak ihlali olduğuna hükmetmiştir. Tıbbi verilerin halka açık duruşmalarda veya üçüncü kişilerin erişimine açık şekilde korunmadan kullanılmasının, orantısız bir müdahale olduğuna karar verilmiştir. Bu karar, sağlık verilerinin gizliliğinin, hastanın kendi yararına veya personel güvenliği gibi "ağır basan bir gereklilik" olmadıkça korunması gerektiğini yerleşik hale getirmiştir. Türk hukukunda Hasta Hakları Yönetmeliği (m. 21-25), sağlık verilerinin gizliliğini özel olarak düzenlemektedir.

3.2. E-Nabız Sistemi ve Sağlık Veri Güvenliği

Türkiye'de Sağlık Bakanlığı tarafından işletilen e-nabız sistemi, vatandaşların sağlık kayıtlarına elektronik ortamda erişim imkânı tanımaktadır. Milyonlarca Türk vatandaşının sağlık verilerinin merkezi bir veri tabanında toplanması, olağanüstü nitelikte bir özel nitelikli veri deposu oluşturmaktadır. Sisteme erişim yetkisinin kapsamı, kimlerin hangi koşullarda veri görüntüleyebileceği ve veri güvenliğinin nasıl sağlandığı konularında KVKK uyumluluğuna ilişkin sistemin incelenmesi gerekmektedir. Özellikle TSK ve Jandarmaya personel alımlarında yapılan muayenelerde Ruh sağlığı uzmanı hekimlerin adaylardan E nabız sitemini doktorların erişimine açmalarını istedikleri ve geçmişe yönelik kayıtları sorguladıkları bilinmektedir. Medula sistemi ise reçetelere ve hastalara yazılan kayıtlara ulaşmayı olanak sağlayan diğer bir sistemdir. . KVK Kurulu, kamu kurumlarının sağlık verisi işleme uygulamalarına ilişkin çeşitli denetimler gerçekleştirmiş; ancak bu alanda kapsamlı ve bağımsız bir denetime ihtiyaç duyulduğu açıkça ortadadır.

4. Sonuç

Özel nitelikli kişisel veriler, özellikle biyometrik ve sağlık verileri, dijital dönüşümün hızlandırdığı bir ortamda giderek daha fazla tehdit altındadır. KVKK'nın 6. maddesi bu verilere güçlendirilmiş bir koruma sağlamakla birlikte uygulamadaki eksiklikler hâlâ giderilmemiştir. KVK Kurulu'nun biyometrik veri kararları olumlu bir yönelimi yansıtmakta; ancak e-nabız gibi kamu sektörü veri tabanlarının bağımsız denetimine ilişkin kaygılar sürmektedir. Yeterlilik kararı süreci de dahil olmak üzere AB standartlarına tam uyum için bu kategorilerin özel korumasının güçlendirilmesi zorunludur.

Dipnotlar

1. KVKK m. 6: Özel nitelikli kişisel veriler ve işleme koşulları.
2. GDPR m. 9: Özel kategorilerdeki kişisel verilerin işlenmesi.
3. GDPR m. 4/14: Biyometrik veri tanımı.
4. AİHM, Z - Finlandiya, Başvuru No. 22009/93, 25 Şubat 1997, para. 95.
5. KVK Kurulu Kararı, 2019/78 sayılı Karar — Biyometrik veri işleme.
6. Hasta Hakları Yönetmeliği, m. 21-25 — Sağlık verilerinin gizliliği.
7. 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında KHK.
8. AİHM, S. ve Marper - Birleşik Krallık, Başvuru No. 30562/04, 4 Aralık 2008.
9. KVKK m. 12: Veri güvenliğine ilişkin yükümlülükler.
10. EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices, 2020.

Kaynakça

AİHM. Z - Finlandiya, Başvuru No. 22009/93, 25 Şubat 1997.

AİHM. S. ve Marper - Birleşik Krallık, Başvuru No. 30562/04, 4 Aralık 2008.

EDPB. Guidelines 3/2019 on Video Devices. Brussels: EDPB, 2020.

Dinçkol, Bihterin V. Kişisel Verilerin Korunması Hukukunun Temel Esasları. İstanbul: Beta, 2021.

Kaya, Cemil. Kişisel Verilerin Korunması Hukuku. Ankara: Turhan Kitabevi, 2020.

KVK Kurul Kararları (biyometrik veri). kvkk.gov.tr.

6698 sayılı KVKK m. 6. Resmî Gazete, 7 Nisan 2016, Sayı: 29677.

Hasta Hakları Yönetmeliği. Resmî Gazete, 1 Ağustos 1998, Sayı: 23420.

Solove, Daniel J. Understanding Privacy. Cambridge: Harvard UP, 2008.

Türkiye Cumhuriyeti Anayasası. Resmî Gazete, 9 Kasım 1982, Sayı: 17863.

Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.

Öztürk, Mustafa. KVKK Şerhi. Ankara: Seçkin, 2022.

Bu makale, Torun Hukuk Bürosu Akademik Makale Serisi kapsamında hazırlanmıştır.