## AVRUPA'DA KİŞİSEL VERİNİN YOLCULUĞU:

# GÜVENLİK Mİ ÖZGÜRLÜK MÜ?



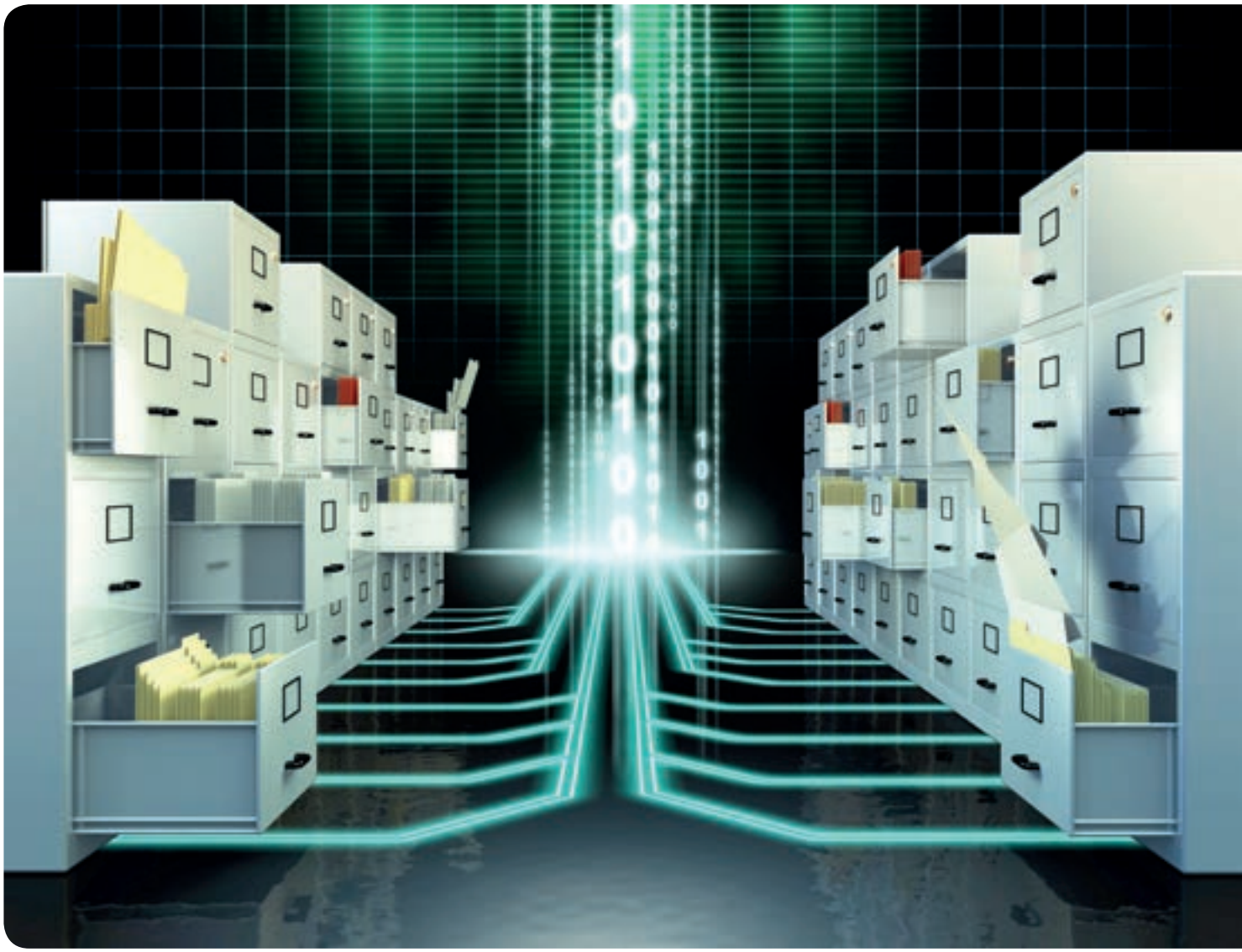
**İfade ve basın özgürlüğü ile kişisel verinin korunması arasındaki denge** günümüzde AB içinde bile henüz kurulabilmiş değil. Denge sorunu, önümüzdeki yıllarda da büyük tartışmaların konusu olmaya devam edeceğe benziyor.

Günümüzde, artan bir hızla gelişen teknolojilerin ve küreselleşmenin etkilerinden, temel insan hakları da nasibini alıyor. Temel hakların korunmasına ilişkin hukuki düzenlemelerle teknolojik gelişmelerin etkileşimi, hem iş çevrelerinde hem de akademik çevrelerde en popüler tartışma konularından biri...

İlk kez 1948 İnsan Hakları Evrensel Beyannamesi'nin 12'nci Maddesi'nde belirtilmiş olan "özel hayatın korunması", gelişen teknolojilerden ve küreselleşmeden en çok etkilenen temel haklar arasında yer alıyor.[1] Bu noktada, özellikle kişisel verinin korunması sorun; bazı AB ülkelerinde vatandaşlara ilişkin özel bilgilerin başka devletlerin istihbarat örgütlerinin eline geçmesi ve halka mal olmuş kişilerin özel

**Ahmet CERAN**
*İKV Uzman Yardımcısı*





hayatlarına dair verilerin internete sızması gibi sansasyonel olaylarla, gündemin merkezine oturmuş durumda.

İçinde bulunduğumuz bilgi çağında kişisel veriler; sigortacılık, bankacılık, ulaştırma, sosyal medya, arama motorları, reklamcılık gibi çok çeşitli sektörlerden; kolluk kuvvetleri, sınır kontrol birimleri, nüfus müdürlükleri gibi kamu kuruluşlarına kadar geniş bir yelpazeye yayılmış iş kollarında kullanılıyor. Bulut bilişim (cloud computing) ve benzeri her gün gelişen teknolojilerle birlikte, "kişisel bir veri, internet aracılığıyla, Berlin'den işlenmek üzere Boston'a gönderilebilmekte ve Boston'da işlenen bu veri, depolanmak üzere Hindistan'ın silikon vadisi kabul edilen Bangalor'a çok kısa sürede ulaştırılabilmekte".[2]

Bu süreçler; sınırların belirsizleşmesi, kişilik haklarının zarar görmesi, ulusal denetimin zorlaşması, mevcut hukuki düzenlemelerin yetersiz kalması gibi sorunların ortaya çıkmasına neden olabiliyor. Öte yandan kişisel verinin korunması sorunu, AB hukukunun konusuna giren; temel haklar, kişilerin serbest dolaşımı, sınır kontrolü ve komşuluk politikaları, şirketler hukuku, organize suçlarla, terörle ve insan ticaretiyle mücadele gibi alanlarla doğrudan bağlantılı. AB'de tartışmaların merkezinde, kişisel verinin kullanımına ilişkin süreçlerde özgürlüklerin mi yoksa güvenliğin mi ön planda olacağı sorusu yer almakta.

## VERİ GÜVENLİĞİNE İLİŞKİN KAVRAMSAL VE HUKUKİ ÇERÇEVE

En temel tanımıyla kişisel veri; kişinin özel, profesyonel veya kamusal yaşamıyla bağlantılı her türlü bilgi olarak kabul ediliyor. İsim, fotoğraf, Twitter/Facebook/Whatsapp iletileri, e-posta adresi, tıbbi bilgiler gibi yaşamın her alanındaki çok farklı bilgi bu kapsama girebiliyor. Türk yetkili makamlar tarafından AB müktesebatıyla uyum doğrultusunda hazırlanan Kişisel Verilerin Korunması Kanun Tasarısı'nın 3'üncü Maddesi'nde kişisel veri; "Belirli



veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlanıyor.[3]

Kişisel veri, ilk kez BM İnsan Hakları Evrensel Bildirgesi ve Avrupa İnsan Hakları Sözleşmesi (AİHS) tarafından güvence altına alındı. Bununla birlikte, 1960'lardan itibaren bilgi teknolojilerinde yaşanan gelişmelerle, kişisel verinin korunmasına yönelik daha ayrıntılı uluslararası düzenlemelere ihtiyaç duyuldu ve Avrupa Konseyi'nin, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı Sözleşmesi" oluşturuldu. 108 sayılı Sözleşme, bu alanda bağlayıcılığı olan ilk düzenleme olarak dikkat çekiyor. Sözleşme'ye, Avrupa Konseyi üyesi olmayan Uruguay ve Fas gibi ülkeler de taraf konumunda. Sözleşme'nin hükümleri, taraf ülkelerdeki özel sektörün ve kamu sektörünün tamamını bağlıyor.[4]

İlgili uluslararası düzenlemeler kapsamında normal kişisel verilerin yanı sıra özel koruyucu önlemleri gerekli kılan üç adet veri türü bulunuyor.

***Hassas Veriler:*** Özel koruyucu önlemleri gerekli kılan üç veri türünden biri olan hassas veriler; ırksal kökeni, siyasi görüşleri, dinsel ya da diğer inançları açığa çıkaran kişisel veriler; kişinin sağlığı ya da cinsel yaşamıyla ilgili olan veriler ve cezai mahkûmiyetlere ilişkin verileri kapsıyor. Bu veriler otomatik yollarla işlenemez.[5]

***Anonim Veri:*** kişisel verinin bütün tanımlayıcı ögelerinin ortadan kaldırılmasıyla geriye kalan veri türü oluyor. Bir kişisel veri, belli bir amaç doğrultusunda kullanıldıktan sonra, bu veri bilimsel, istatiksel amaçlarla sadece anonim halde muhafaza edilebilir.

***Takma Adlı Veri (Pseudonymous Data):*** Bilginin, veri sahibiyle ilişkilendirilebilmesi için ek bilgilere ihtiyaç duyulan veri türü olarak tanımlanıyor. Bu tür verilerin işlenmesi sürecinde, verinin sadece dolaylı yollarla tanımlanabilir kalmasını sağlama görevi, veriyi işleyen kişiye aittir.[6]

OECD, tüm bu farklı türlerine rağmen, bütün kişisel verilerin korunmasına ve veri akışının kontrol altına alınmasına yönelik olarak 1980 yılında sekiz yönlendirici ilke belirledi. Günümüzde konuya ilişkin bütün ulusal ve uluslararası mevzuat, OECD'nin bu yönlendirici ilkelerini dikkate alıyor. OECD yönlendirici ilkeleri, tablo I'de yer alıyor.[7]

## AVRUPA'DA KİŞİSEL VERİ KORUNABİLİYOR MU?

Kişisel verinin korunması bütün Avrupa'da emredici (jus cogens) nitelikte temel haklar arasında kabul ediliyor. Fakat sınırları içinde bir günde 250 milyon bireyin aktif olarak internet kullandığı AB[8], kendi içinde ve üçüncü ülkelerle veri akışının tam kontrolünü sağlamakta ciddi zorluklarla karşılaşıyor. İkinci Dönem Barroso Komisyonu'nun Adalet, Temel Haklar ve Vatandaşlıktan Sorumlu Üyesi Viviane Reding, 1997'de Avrupa'da internet kullanımı oranının %1 olduğunu, günümüzde ise bilginin birkaç saniyede, AB içinde ve yeryüzünün diğer coğrafyalarında dolaşabildiğini ifade ediyordu.[9] Öyle ki, konu Avrupa liderlerinin, kendi iç kamuoylarında dahi eleştirilmelerine neden olabiliyor. Örneğin, 2013 yılında Alman vatandaşlarının internet üzerindeki

### Sınır Ötesi Veri Akışlarına İlişkin **OECD Yönlendirici İlkeleri**

| | |
|---|---|
| Sınırlandırma İlkesi | Verinin sadece yasalara uygun ve adil yollarla, verinin öznesinin bilgisi dahilinde toplanması. |
| Veri Kalitesi İlkesi | Verinin doğru, eksiksiz ve güncel olması. |
| Amacın Belirli Olması İlkesi | Verinin toplanmasının ardından, kullanım amacının değiştirilememesi. |
| Kullanımın Sınırlandırılması İlkesi | Verinin sadece verinin öznesinin rıza gösterdiği amaçlar doğrultusunda veya resmi yetkili makamların hükmü doğrultusunda kullanılması. |
| Koruyucu Tedbirler İlkesi | Kişisel verinin, izinsiz erişim, kullanım ve izinsiz değişiklikler gibi risklere karşı korunması. |
| Açıklık İlkesi | Kişisel verinin korunmasına ilişkin gelişmelere, politikalara ve uygulamalara açık olunması. |
| Bireysel katılım İlkesi | Kişinin, kendisine ilişkin veriyi kontrol altında tutanlarla etkileşime geçebilmesi. |
| Hesap Verebilirlik İlkesi | Kişisel veriyi kontrol altında tutanların, ilgili mevzuatla ve yukarıdaki ilkelerle uyumlu olması, bu doğrultuda şeffaflık sağlayabilmesi. |



kişisel verilerinin İngiltere ve ABD istihbarat örgütleri tarafından ele geçirilmesi ve kullanılması tartışmaları, seçim döneminde Almanya Şansölyesi Angela Merkel'in karşısına çıkan en zorlu karşı propaganda hamleleri arasında yer almıştı.[10]

AB hukuku çerçevesinde, kişisel verinin korunmasına ilişkin AİHS ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin ötesinde de birtakım adımlar atıldı. İlk olarak 1995 yılında kabul edilen 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında Yönerge" ile Birlik dâhilinde verinin koruması alanında yüksek bir standart oluşturmaya çalışıldı. Verinin Korunması Yönergesi, yüksek seviyede veri güvenliği sağlanmadığı takdirde, AB iç pazarında malların; kişilerin ve hizmetlerin etkin serbest dolaşımının mümkün olamayacağı ana fikri üzerine inşa edilmiş durumda.

Bu doğrultuda Yönerge, 108 sayılı Avrupa Konseyi Sözleşmesi'ne ek olarak, AB ülkelerinde bağımsız denetim organları kurulmasını öngörüyor. Öte yandan, gelişen teknolojilerin ve küreselleşmenin etkileriyle birlikte mevcut düzenlemelerin güncelliğini yitirmesi ve Birlik içerisinde veri güvenliğinin ideal ölçüde sağlanamaması, reform tartışmalarını gündeme getiriyor. Avrupa Komisyonu'nun "Eurobarometer" adlı anket çalışmasının sonuçlarına göre, Avrupalılar'ın % 90'ı, kişisel veriye ilişkin Avrupa çapında eşit koruma talep ediyor.[11]

Devam eden reform tartışmalarıyla birlikte, Avrupa Komisyonu 2012 yılında, Avrupa Parlamentosu'na ve AB Konseyi'ne, 1995 Verinin Korunması Yönergesi'nin modernize edilmesine ve internet çağına ayak uydurulmasına yönelik bir teklif sundu. Teklifin öne sürdüğü, bütün AB'de geçerli tek bir "Verinin Korunması Tüzüğü"nün oluşturulmasıyla birlikte, önemli mali tasarruflar ve kolaylıklar sağlanması, ihlal hallerinde veri sahibinin anında uyarılması ve veri öznesinin talebi üzerine verinin

| ABAD'ın C-131/12 Sayılı Kararında **Öne Çıkan** Konular |
|---|
| Kişisel verinin korunmasına ilişkin AB hukuku, Google ve benzeri arama motorlarına uygulanabilir mi? |
| Arama motorları, kişisel veriyi kontrol altında tutuyor. Dolayısıyla ilgili AB hukuku, arama motorlarına da uygulanabiliyor. |
| Kişisel verinin korunmasına ilişkin AB hukuku, Google'ın veri sunucuları AB dışında, ABD'de bulunsa dahi, Google İspanya ofisine yönelik olarak uygulanabilir mi? |
| Veri sunucusu (server) fiziksel olarak AB dışında bulunsa dahi, arama motorunun AB ülkelerinde şubesi var ise veriyi depolayan şirket, ilgili AB organının yer bakımından yargı yetkisine giriyor. |
| Kişilerin, arama motorları aracılığıyla ulaşılabilen kişisel verilerinin silinmesini talep etme (right to be forgotten) hakkı var mıdır? |
| Bilginin; hatalı, eksik, ilgisiz ve aşırı olduğu durumlarda, kişilerin arama motorlarından veya diğer veri depolayıcılarından, verilerinin silinmesini talep etme hakkı (right to be forgotten) bulunuyor. |
| Kişinin, kendisine ilişkin veriyi kontrol altında tutanlarla etkileşime geçebilmesi. |
| Kişisel veriyi kontrol altında tutanların, ilgili mevzuatla ve yukarıdaki ilkelerle uyumlu olması, bu doğrultuda şeffaflık sağlayabilmesi. |

böylelikle AB dâhilindeki iş çevrelerine 2,3 milyar euro değerinde tasarruf sağlanması bekleniyor.

Avrupa Komisyonu'nun istatistiklerine göre, günümüzde verinin korunmasına ilişkin gereksiz evrak işleri ve harcamalar, işletmelere yıllık 130 milyon euroya varan ek masraf olarak geri dönüyor. Dolayısıyla yeni tüzükle birlikte her üye ülkede durağı bulunan tek bir veri güvenliği sistemi kurulmasıyla, gereksiz bürokratik süreçlerin önüne geçilmesi bekleniyor. Fakat bu noktada ne tür verinin kişisel veri kabul edileceği, bireyin güvenliğinin mi yoksa verinin serbest dolaşımının mı ön plana çıkarılacağı ve ne tür rızanın, kişisel verinin dolaşımı için yeterli olacağı soruları ekseninde AB ülkeleri ve AB kurumları çapında yoğun tartışmalar sürüyor. Güvenlik/özgürlük sarkacında devam eden bu tartışmaların, yakın gelecekte kolay bir çözüme ulaşacağı da tahmin edilmiyor.

## ABAD KARARI: AVRUPA İNSANI UNUTULMAK İSTİYOR

Kişisel verinin korunmasına ilişkin her konuda geniş çaplı anlaşmaya varılamasa bile 13 Mayıs 2014 tarihinde AB'nin gündemine oturan önemli bir AB Adalet Divanı (ABAD) kararı alındı. Daha önce de belirtilmiş olduğu üzere, kişisel verinin paylaşımı ve dolaşımı ancak kişinin rızasının olduğu hallerde veya hukukun zorunlu kıldığı hallerde mümkün. Ayrıca, verinin paylaşımına neden olan amaç gerçekleştiğinde, OECD ilkeleri gereği kişisel veri başka bir amaç doğrultusunda kullanılamıyor. Öte yandan, kişisel verinin korunması, kişisinin kendisine dair kişisel veriye her şartta ulaşabilmesini ve kendisine ilişkin verinin silinmesini talep edebilmesini de kapsıyor.

Costeja González isimli İspanyol vatandaşı, kendisiyle bağlantısı kalmayan verilerin, Google'ın arama sonuçlarından silinmesine yönelik olarak 2010 yılında İspanyol yargı mercilerine başvurdu. İspanyol mahkemeleri de davayı ABAD'a sevk etti. ABAD, 13 Mayıs 2014 tarihinde davaya (C-131/12) ilişkin üç konuda, AB içtihat hukukunun geleceğini doğrudan etkileyecek önemli kararlar aldı (Bkz. Tablo II).[12]

ABAD kararında da ifade edildiği üzere, bu hak her durumda geçerli değil. İfade özgürlüğü, basın özgürlüğü ile kişisel verinin korunması arasındaki denge günümüzde AB içinde henüz kurulabilmiş değil ve büyük tartışmaların konusu olmaya da devam ediyor. Bu alanda özgürlük ve güvenlik dengesinin kurulabilmesi için her vakanın kendi iç dinamiklerine göre değerlendirilmesi ve yeni kararlarla gelişen bir içtihat hukukunun, modernize edilmiş mevzuatın oluşturulması gerekiyor.


***KAYNAKÇA:***

*1) Madde 12, BM İnsan Hakları Evrensel Beyannamesi, TBMM İnsan Haklarını İnceleme Komisyonu, http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf, Erişim Tarihi: 20.11.2014*

*2) Avrupa Komisyonu, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", Press Release, 25 Ocak 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm, Erişim Tarihi:20.11.2014*

*3) Kişisel Verilerin Korunması Kanun Tasarısı, Adalet Bakanlığı, http://www.kgm.adalet.gov.tr/tasariasamalari/basbakanlik/Kanuntas/kisiselveriler.pdf, ErişimTarihi:20.11.2014*

*4) European Union Agency for Fundamental Rights, Handbook on European data protection law, Publications Office of the European Union, 2014, p.17.*

*5) Songül Atak, "Avrupa Konseyi'nin Kişisel Verileri Açısından Sağladığı Temel Güvenceler", TBB Dergisi, Sayı 87, 2010.*

*6) Leyla Keser vd., Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, TEPAV, 2014, ss.62-63.*

*7) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, Erişim Tarihi: 21.11.2014.*

*8) Avrupa Komisyonu, "How does the data protection reform strengthen citizens' rights?", Data Protection Facts Sheet, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf, Erişim Tarihi:22.11.2014.*

*9) Avrupa Komisyonu, "Commission proposes a comprehensive reform ofdata protection rules to increase users' control of their data and to cut costs for businesses", Press Release, 25 Ocak 2012.*

*10) "Angela Merkel calls for EU-wide agreement on data protection", Financial Times, 2013, http://www.ft.com/intl/cms/s/7a4b26d8-eca6-11e2-a0a4, Erişim Tarihi: 22.11.2014*

*11) Avrupa Komisyonu, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, p.2, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, Erişim Tarihi 23.11.2014.*

*12) Avrupa Komisyonu, Factsheet on the "Right to be forgotten" ruling, C-131/12, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, Erişim Tarihi: 23.11.2014.*