İÇİNDEKİLER

ÖNSÖZ
KISALTMALAR
BU EL KİTABI NASIL KULLANILIR

1. AVRUPA VERİ KORUMA HUKUKUNUN TARİHSEL GELİŞİMİ VE İÇERİĞİ
1.1.Verilerin korunması hakkı
Ana başlıklar
1.1.1. Avrupa İnsan Hakları Sözleşmesi
1.1.2. 108 Sayılı Avrupa Konseyi Sözleşmesi
1.1.3. Avrupa Birliği Veri Koruma Mevzuatı
1.2. Hakların dengelenmesi
Ana başlıklar
1.2.1. İfade özgürlüğü
1.2.2. Belgelere erişim
1.2.3. Sanat ve bilim özgürlüğü
1.2.4. Mülkiyetin korunması

2. VERİ KORUMA TERMİNOLOJİSİ
2.1. Kişisel veriler
Ana başlıklar
2.1.1. Kişisel veri kavramının temel unsurları
2.1.2. Özel nitelikli kişisel veriler
2.1.3. Anonim hale getirilmiş veya takma isim ile değiştirilmiş veriler
2.2. Veri işleme
Ana başlıklar
2.3. Kişisel verilerin kullanıcıları
Ana başlıklar
2.3.1. Veri sorumluları ve veri işleyenler
2.3.2. Veri alıcıları ve üçüncü kişiler
2.4. Rıza
Ana başlıklar
2.4.1. Geçerli rızanın unsurları
2.4.2. Rızayı her daim geri çekme hakkı

3. AVRUPA VERİ KORUMA HUKUKUNUN TEMEL İLKELERİ
3.1. Hukuka uygun işlenme ilkesi
Ana başlıklar
3.1.1. AIHS kapsamında haklı müdahalenin şartları
3.1.2. Avrupa Birliği Temel Haklar Şartı kapsamında hukuka uygun sınırlamaların şartları
3.2. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi
Ana başlıklar
3.3. Veri kalitesi ilkeleri
Ana başlıklar
3.3.1 Verilerde gereklilik ilkesi
3.3.2. Doğruluk ilkesi
3.3.3. Verilerin sınırlı muhafazası ilkesi

3.4. Adil işleme ilkesi
Ana başlıklar
3.4.1. Şeffaflık
3.4.2. Güven oluşturulması
3.5. Hesap verilebilirlik ilkesi
Ana başlıklar

4. AVRUPA VERİ KORUMA HUKUKUNUN KURALLARI
4.1. Hukuka uygun işlemeye dair kurallar
Ana başlıklar
4.1.1. Hassas olmayan verilerin hukuka uygun olarak işlenmesi
4.1.2. Özel nitelikli (hassas) kişisel verilerin hukuka uygun olarak işlenmesi
4.2. İşleme sürecinin güvenliğine dair kurallar
Ana başlıklar
4.2.1. Veri güvenliğinin unsurları
4.2.2. Gizlilik
4.3. Verilerin işlenmesinde şeffaflığa dair kurallar
Ana başlıklar
4.3.1. Bilgilendirme
4.3.2. Bildirim
4.4. Uyuma teşvik kuralları
Ana başlıklar
4.4.1. Ön denetim
4.4.2. Kişisel veri koruma memurları
4.4.3. Davranış kuralları

5. VERİ ÖZNELERİNİN HAKLARI VE BU HAKLARIN UYGULANMASI
5.1. Veri öznelerinin hakları
Ana başlıklar
5.1.1. Erişim hakkı
5.1.2. İtiraz hakkı
5.2. Bağımsız denetim
Ana başlıklar
5.3. Kanun yolları ve yaptırımlar
Ana başlıklar
5.3.1. Veri sorumlusuna yapılan talep
5.3.2. Denetim makamlarına yapılmış olan şikayetler
5.3.3. Mahkemeye yapılmış olan şikayetler
5.3.4. Yaptırımlar

6. SINIR ÖTESİ VERİ AKIŞI
6.1. Sınır ötesi veri akışının doğası
Ana başlıklar
6.2. Üye Devletler veya Akit Taraflar arasındaki serbest veri akışı
Ana başlıklar
6.3. Üçüncü ülkelere serbest veri akışı
Ana başlıklar
6.3.1. Yeterli koruma sağlandığı için serbest veri akışı
6.3.2. Özel durumlarda serbest veri akışı
6.4. Üçüncü ülkelere sınırlandırılmış veri akışı

Ana başlıklar
6.4.1. Sözleşme maddeleri
6.4.2. Bağlayıcı şirket kuralları
6.4.3. Özel uluslararası anlaşmalar

7. KOLLUK VE CEZA YARGILAMASI KAPSAMINDA VERİLERİN KORUNMASI
7.1. Kolluk ve ceza yargılaması kapsamında verilerin korunması
Ana başlıklar
7.1.1. Kolluk Tavsiye Kararı
7.1.2. Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi)
7.2. Kolluk ve cezai konularda verilerin korunmasına dair AB mevzuatı
7.2.1. Veri Koruma Çerçeve Kararı
7.2.2. Kolluk ve sınır ötesi adli işbirliği alanlarında veri korumasına yönelik diğer özel hukuki düzenlemeler
7.2.3. Europol ve Eurojust'ta Veri Koruma
7.2.4. AB düzeyindeki ortak bilgi sistemlerinde verilerin korunması

8. AVRUPA VERİ KORUMA HUKUKUNDA YER ALAN DİĞER DÜZENLEMELER
8.1. Elektronik Haberleşme
Ana başlıklar
8.2. İstihdam verileri
Ana başlıklar
8.3. Tıbbi veriler
Ana başlıklar
8.4. İstatistiksel amaçlar için verilerin işlenmesi
Ana başlıklar
8.5. Mali veriler
Ana başlıklar

İLAVE KAYNAKLAR
İÇTİHATLAR
AİHM İçtihatlarından Örnekler
Avrupa Birliği Adalet Divanı İçtihatlarından Örnekler
DİZİN

Kısaltmalar

108 Sayılı Avrupa Konseyi Sözleşmesi	Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 Sayılı Sözleşmesi
AB	Avrupa Birliği
AK	Avrupa Konseyi
ABAD	Avrupa Birliği Adalet Divanı
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AP	Avrupa Parlamentosu
AT	Avrupa Toplulukları
İHEB	Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi
BM:	Birleşmiş Milletler
CIS	
C-SIS	Merkezi Schengen Bilgi Sistemi (Central Schengen Information System)
EDPS	Avrupa Veri Güvenliği Gözetmeni (European Data Protection Supervisor)
Şart	Avrupa Birliği Temel Haklar Şartı
N-SIS	Ulusal Schengen Bilgi Sistemi (National Schengen Information System)
OECD	İktisadi Kalkınma ve İşbirliği Örgütü (Organisation for Economic Cooperation and Development)
PNR	Yolcu İsim Kaydı (Passenger Name Record)
SIS II	Schengen Bilgi Sistemi (Schengen Information System)
VIS	Vize Bilgi Sistemi (Visa Information System)
Çerçeve Karar	Ceza hukukunu ilgilendiren konularda polis ve adli makamlar arasındaki işbirliği çerçevesinde işlenen kişisel verilerin korunması hakkındaki 27 Kasım 2008 sayılı ve 2008/977/JHA sayılı Konsey Çerçeve Kararı
EDRIS:	Avrupa Acil Durum Afet Bilgi Sistemi (European Emergency Disaster Response Information System)
Eurojust:	Avrupa Yargı İşbirliği Kurumu
Europol:	Avrupa Polis Teşkilatı
Eurosur:	Avrupa Sınır Gözetim Sistemi
Eurostat:	Avrupa Birliği İstatistik Kurumu
EAW	Avrupa Tutuklama Emri
EEA	Avrupa Ekonomik Alanı
EFTA	Avrupa Serbest Ticaret Birliği
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı
ENU	Europol Ulusal Birimi
ESMA	Avrupa Menkul Kıymetler ve Piyasalar Otoritesi
eTen	Trans-Avrupa Telekomünikasyon Ağları

EuroPrise	Avrupa Gizlilik Mührü
Eu-LISA	Avrupa Büyük Ölçekli Bilişim Teknolojileri Sistemleri Ajansı
BCR	Bağlayıcı kurumsal kural
CCTV	Kapalı devre televizyon
CETS	Avrupa Konseyi Antlaşmaları Serisi
CRM	Müşteri ilişkileri yönetimi
FRA	Avrupa Birliği Temel Haklar Ajansı
GPS	Küresel konumlama sistemi
JSB	Ortak Denetim Birimi
NGO	Sivil toplum kuruluşu
PIN	Kişisel kimlik numarası
SEPA	Avrupa Tek Ödeme Alanı
SWIFT	Dünya Bankalararası Finansal Telekomünikasyon Toplumu
TEU	Avrupa Birliği Antlaşması
TFEU	Avrupa Birliği'nin İşleyişi Hakkında Antlaşma
UDHR	İnsan Hakları Evrensel Bildirisi

Bu el kitabı nasıl kullanılır

Bu el kitabı, Avrupa Birliği (AB) ve Avrupa Konseyi (AK) bağlamında verilerin korunması mevzuatına genel bir bakış sağlar.

El kitabı, verilerin korunmasında uzmanlaşmamış hukukçulara yardımcı olmak için tasarlanmıştır; bu çalışma verilerin korunmasına ilişkin yasal sorunlarla karşı karşıya kalabilecek avukatlar, hakimler ve uygulama alanındaki diğer meslek mensuplarının yanı sıra sivil toplam kuruluşları da dahil olmak üzere diğer kuruluşlarda çalışanlara (STKlar) yönelik olarak oluşturulmuştur.

El kitabı, veri koruması alanında AB hukuku ve AİHS düzenlemeleri açısından ilk referans noktasıdır ve bu alanın AB mevzuatı, AİHS, Avrupa Konseyinin düzenlemiş olduğu Kişisel Verilerin Korunması Sözleşmesi (108 Sayılı Avrupa Konseyi Sözleşmesi) ve diğer Avrupa Konseyi araçları kapsamında nasıl düzenlendiğini açıklar. Her bir bölüm geçerli olan yasal hükümleri ve iki ayrı hukuk sistemi altında (AB ve AK) önemli görülen mahkeme içtihatlarını içeren bir tabloyla başlamaktadır. Sonrasında bu iki hukuk düzenine ait yasal düzenlemeler her bir başlığa uygulanma şekillerine göre sırayla sunulmaktadır. Bu anlatım tarzı okuyucunun her iki hukuk sistemini birbiri ile karşılaştırabilmesine ve düzenlerin hangi noktada birleştiklerini, hangi noktada farklılaştıklarını görmesine imkân tanımaktadır.

Her bölümün başındaki tablolar o bölümde ele alınan konu başlıklarını genel hatlarıyla aktarmakta ve uygulanabilir yasal hükümler ve örneğin mahkeme içtihatları gibi diğer önemli belgeleri belirtmektedir. İlgili bölümün içeriğinin özlü bir biçimde aktarılması için gerekli görüldüğü durumlarda bu başlıkların sırası bölüm içerisindeki metnin yapısından az da olsa farklılık gösterebilir. Tablolar hem AB hem de AK hukukunu kapsamaktadır. Bu da kullanıcıların kendi durumlarına ilişkin önemli bilgilere ulaşmalarını ve özellikle de sadece AK düzenlemelerine tabi olanların bu bilgilere ulaşmalarını kolaylaştıracaktır.

AB ülkeleri dışında, AK üyesi olan ve AIHS ve 108 Sayılı Avrupa Konseyi Sözleşmesine taraf olan ülkelerin uygulayıcıları kendi ülkeleri için gerekli olan bilgilere doğrudan AK'ye ait bölümlere giderek erişebilirler. AB ülkelerinde bulunan uygulayıcıların, her iki hukuk düzeniyle de bağlı oldukları için her iki bölümü de kullanmaları gerekecektir. Belirli bir konuda daha fazla bilgi arzu edenler için, el kitabının en sonunda bulunan 'ilave kaynaklar bölümüne bakmaları önerilir.

AK mevzuatı, Avrupa İnsan Hakları Mahkemesince (AİHM) verilmiş olan belirli kararlara yapılan kısa atıflar ile sunulmuştur. Bu kararlar, verilerin korunmasıyla alakalı mevcut çok sayıda AİHM kararı arasından seçilmiştir.

AB mevzuatı ise Avrupa Topluluğu Adalet Divanı (ATAD, 2009 öncesinde Avrupa Adalet Divanı olarak adlandırılan kurum) içtihatlarında belirtildiği üzere, antlaşmaların ve Avrupa Birliği Temel Haklar Şartı'nın ilgili maddelerinde kabul edilen yasal düzenlemelerden oluşmaktadır.

Bu el kitabında anlatılan veya atıfta bulunulan içtihatlar AİHM ve ATAD içtihadının önemli bir bölümüne dair örnekler sunmaktadır. El kitabının sonunda bulunan başvuru kılavuzu, okuyucuya mahkeme içtihadını çevrimiçi olarak arama konusunda yardımcı olması amacıyla yazılmıştır.

Buna ek olarak, Avrupa veri koruma mevzuatının özellikle de AİHM veya ATAD içtihadına konu olmamış alanlardaki uygulama şeklini somutlaştırmak adına farazi kurgulardan oluşan bazı pratik örnekler mavi kutucuklar içerisinde sunulmuştur. Gri renkte olan diğer kutucuklarda ise içtihat hukuku dışındaki kaynaklardan, örneğin mevzuattan örnekler sunulmaktadır.

Bu el kitabı, AİHS ve AB hukukundan oluşan iki farklı hukuk sisteminin rolüne dair kısa bir açıklama ile başlamaktadır (Bölüm 1). 2. Bölüm'den 8. Bölüme kadar olan kısımda sunulan konular ise şöyledir:

- veri koruma terminolojisi
- Avrupa veri koruma mevzuatının temel ilkeleri
- Avrupa veri koruma mevzuatının kuralları
- verileri işlenen kişinin hakları ve bu hakların uygulaması
- sınır ötesi veri akışı
- kolluk ve ceza yargılaması kapsamında verilerin korunması
- verilerin korunmasını düzenleyen diğer Avrupa mevzuatı

1.Avrupa Veri koruma hukukunun tarihsel gelişimi ve içeriği

AB	İşlenen konular	AK
Verilerin korunması hakkı		
Kişisel Verilerin Işlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi (Veri Koruma Direktifi), OJ 1995 L 281		AİHS, *Madde 8 (özel hayatın ve aile hayatının, konut ve haberleşme hakkının korunması)* *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Sözleşme)*
Hakların dengelenmesi		
ABAD, Birleştirilmiş davalar C-92/09 ve C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 2010	**Genel olarak**	
ABAD, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 2008	**İfade özgürlüğü**	AİHM, *Axel Springer AG v. Germany*, 2012 AİHM, *Mosley v. the United Kingdom*, 2011
	Sanat ve bilim özgürlüğü	AİHM, *Vereinigung bildender Künstler v. Austria*, 2007
ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 2008	**Mülkiyetin korunması**	
ABAD, C-28/08 P, *Avrupa Komisyonu v. The Bavarian Lager Co. Ltd*, 2010	**Belgelere erişim**	AİHM, *Társaság a Szabadságjogokért v. Hungary*, 2009

1.1 Verilerin korunması hakkı

Ana başlıklar

- AİHS Madde 8 uyarınca, kişisel verilerin toplanılması/kullanılması ve bu verilerin korunması hakkı, özel hayatın ve aile hayatının korunması, konut ve haberleşme hakkına saygı gösterilmesi hakkı kapsamında yer almaktadır.
- 108 sayılı AK Sözleşmesi, açık bir şekilde verilerin korunması ile ilgili düzenlenmiş olan uluslararası olarak bağlayıcı ilk metindir.
- AB mevzuatına göre, verilerin korunması ilk olarak VK Direktifi ile düzenlenmiştir.
- AB mevzuatında verilerin korunması temel hak olarak tanımlanmıştır.

Bir bireyin özel alanının üçüncü şahıslar ve özellikle devlet tarafından ihlaline karşı korunması hakkı uluslararası bağlamda ilk olarak 1948 Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi'nin (İHEB) 12. Maddesi kapsamında özel ve aile hayatına saygı başlığı altında düzenlenmiştir.[1] İHEB, Avrupa'daki diğer insan hakları belgelerinin gelişimini etkilemiştir.

1.1.1. Avrupa İnsan Hakları Sözleşmesi

Avrupa Konseyi, İkinci Dünya Savaşının sonunda, hukukun üstünlüğünü, demokrasiyi, insan haklarını ve sosyal kalkınmayı teşvik etmek amacı ile kurulmuştur. Bu amacı gerçekleştirmek için Avrupa Konseyi üyelerinin üzerinde anlaştıkları metin 1953 yılında AİHS olarak kabul edilmiştir ve bu sözleşme 1953 yılında yürürlüğe girmiştir.

Üye devletlerin AİHS'ye uluslararası düzlemde uyma yükümlülükleri vardır. Tüm AK üyesi devletler AİHS'yi kendi ulusal hukuk sistemlerine dahil etmişler veya ulusal mevzuat kapsamında yürürlüğe koymuşlardır. Bu sebeple de sözleşme hükümlerine uygun şekilde hareket etme yükümlülükleri bulunmaktadır.

Avrupa İnsan Hakları Mahkemesi (AİHM) tarafların AİHS kapsamındaki yükümlülüklerini yerine getirdiklerinden emin olmak amacı ile, 1959 yılında, Fransa'nın Strazburg kentinde kurulmuştur. AİHM, devletlerin AİHS altındaki yükümlülüklerini yerine getirip getirmediklerini, bireylerin, toplulukların, sivil toplum kuruluşların veya tüzel kişilerin şikayetlerini inceleyerek denetlemektedir. 2013 Yılında AK'ye üye 47 devletten, 28'i AB ülkelerinden oluşmaktaydı. Mahkemeye başvuran kişilerin bu ülkelerin vatandaşları olmaları zorunluluğu bulunmamaktadır. Ayrıca, AİHM, AK üyesi devletlerden birisinin başka bir üye devlet aleyhine açtığı davalara bakmakla da görevlidir.

Kişisel verilerin korunması hakkı, kapsamı ve hangi hallerde sınırlandırılabileceği AİHS Madde 8'de düzenlenmiş olan özel ve aile hayatına, konut ve haberleşmeye saygı gösterilmesi hakkı kapsamında yer almaktadır.[2]

AİHM geçmişteki içtihatları kapsamında birçok kez verilerin korunması konusu ile ilgili durumları incelemiştir. Özellikle de iletişimin dinlenmesi ve kayda alınması[3], farklı şekillerdeki

[1] Birleşmiş Milletler (BM), İnsan Hakları Evrensel Beyannamesi, 10 Aralık 1948.
[2] Avrupa Konseyi (AK), Avrupa İnsan Hakları Sözleşmesi, CETS No. 005, 1950.
[3] Örneğin: AİHM, *Klass and Others v. Germany*, No. 5029/71, 6 Eylül 1978; AİHM, *Uzun v. Germany*, No. 35623/05, 2 Eylül 2010.

gözetleme araçları [4] ve kişisel verilerin devlet kurumları[5] tarafından saklanmasına karşı korunması gibi başlıklar inceleme konusu olmuştur. Mahkeme, 8. maddenin üye devletlere yalnızca Sözleşmenin ihlaline yol açabilecek durumlardan kaçınma şeklinde bir yükümlülük değil, ayrıca aktif bir şekilde özel ve aile hayatına saygı gösterilmesinin sağlanması biçiminde pozitif bir yükümlülük de getirdiğini açıklığa kavuşturmuştur.[6] Bu mahkeme kararlarının birçoğuna ilgili bölümlerde ayrıntılı bir şekilde değinilecektir.

1.1.2. 108 Sayılı Avrupa Konseyi Sözleşmesi

Bilişim teknolojilerinin 1960'larda ortaya çıkışıyla, bireylerin korunabilmesi için (kişisel) verilerinin de korunmasına yönelik bir ihtiyaç ortaya çıkmıştır. 1970'lerin ortalarında, Avrupa Konseyi Bakanlar Komitesi, AİHS 8. maddeye atıfta bulunarak kişisel verilerin korunmasına ilişkin birçok ilke karar kabul etmiştir.[7] 1981 yılında Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 Sayılı Sözleşmesi (108 Sayılı Sözleşme) imzaya açılmıştır.[8] 108 Sayılı Sözleşme verilerin korunmasına dair bu zamana kadar düzenlenmiş olan en önemli ve bağlayıcı nitelikteki tek uluslararası hukuki belgedir.

108 Sayılı Avrupa Konseyi Sözleşmesi gerek özel gerekse kamu sektörü (örneğin yargı ve kolluk kuvvetleri) tarafından gerçekleştirilen bütün veri işlemelerini kapsar. Sözleşme verilerin toplanması ve işlenmesi sırasında gerçekleşebilecek ihlallere karşı bireyi korur ve aynı zamanda kişisel verilerin sınır ötesi akışını düzenlemeyi amaçlar. Kişisel verilerin toplanması ve işlenmesine ilişkin olarak sözleşmede, verilerin adil ve hukuka uygun bir şekilde toplanması ve işlenmesi, belirli ve sınırlı yasal amaçlar doğrultusunda saklanan verilerin bu amaçlara uygun olmayan kapsamda kullanılmaması veya gerekli olan süreden fazla bir süre saklanmaması ilkeleri benimsenmektedir. Ayrıca verilerin belirli, açık ve meşru amaçlar için işlenmiş ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmaları öngörülmüştür.

Verilerin toplanması ve işlenmesi sürecine yönelik getirilen bu güvencelere ek olarak, uygun yasal tedbirlerin bulunmadığı hallerde kişilerin ırkı, siyasi düşüncesi, sağlığı, dini, cinsel hayatı veya sabıka kaydı gibi özel nitelikli kişisel verilerinin işlenmesi yasaklanmıştır.

Sözleşme ayrıca kişilerin kendileri hakkında verilerin saklandığını bilme ve gerekiyorsa bu verilerin düzeltilmesini talep haklarına yer vermektedir. Kişilerin sözleşmede düzenlenen hakları ancak devlet güvenliği veya savunma tedbirleri kapsamında, üstün çıkarların bulunması durumunda kısıtlanabilir.

Sözleşme kapsamında verilerin sözleşmeye taraf devletler arasında serbest dolaşımı öngörülmekle birlikte, yasal düzenlemelerin eş değer koruma sağlamadığı ülkelere olan aktarımlarda bazı sınırlamalar getirilmiştir.

---

[4] Örneğin: AİHM, *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984; AİHM, *Copland v. the United Kingdom*, No. 62617/00, 3 Nisan 2007.

[5] Örneğin: AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987; AİHM, *S. and Marper v. the United Kingdom*, Nos. 30562/04 ve 30566/04, 4 Aralık 2008.

[6] Örneğin: AİHM, *I. v. Finland*, No. 20511/03, 17 Temmuz 2008; AİHM, *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008.

[7] AK, Bakanlar Komitesi (1973), Res(73) 22 Sayılı, *Özel sektördeki faaliyet gösteren elektronik veri bankaları karşısında bireylerin mahremiyetinin korunması üzerine alınan İlke Kararı*, 26 Eylül 1973;
AK, Bakanlar Komitesi (1974), Res(74) 29 Sayılı, *Kamu sektöründeki faaliyet gösteren elektronik veri bankaları karşısında bireylerin mahremiyetinin korunması üzerine alınan İlke Kararı,* 20 Eylül 1974.

[8] AK, Kişisel Verilerin Otomatik İşlenmesi Açısından Bireylerin Korunması Sözleşmesi, CETS No. 108, 1981.

108 Sayılı Avrupa Konseyi Sözleşmesi'nin öngördüğü temel ilkeleri ve kuralları geliştirmek adına yasal anlamda bağlayıcı olmayan çok sayıda tavsiye kararı Avrupa Konseyi Bakanlar Kurulu tarafından kabul edilmiştir. (Bkz. Bölüm 7 ve 8).

Tüm AB üye ülkeleri 108 Sayılı Avrupa Konseyi Sözleşmesi'ni onaylamışlardır. Sözleşme 1999 yılında değiştirilerek Avrupa Birliği'nin de sözleşmeye taraf olmasının yolu açılmıştır.[9] 2001 yılında 108 Sayılı Avrupa Konseyi Sözleşmesi'ne ek protokol kabul edilmiş ve üçüncü taraf devletlere, yani sözleşmeye üye olmayan devletlere yönelik sınır ötesi veri akışına ve zorunlu olarak kurulacak olan ulusal veri koruma denetim mercilerine dair madde eklemeleri yapılmıştır.[10]

Genel Görünüş

108 Sayılı Avrupa Konseyi Sözleşmesi'nin yenilenmesine dair bir kararı takiben, halkın katılımı ile 2011'de yapılan müzakere sonucunda iki temel amaç kabul edilmiştir: dijital alanda gizliliğin korunmasını güçlendirmek ve sözleşmenin izleme mekanizmasını kuvvetlendirmek.

108 Sayılı Avrupa Konseyi Sözleşmesi, Avrupa dışında kalan ülkeler de dahil olmak üzere AK üyesi olmayan ülkelerin üyeliğine açıktır. Sözleşmenin evrensel bir standart haline gelme potansiyeli ve bütün ülkelere açık niteliği küresel düzeyde veri korumayı teşvik için bir temel noktası oluşturabilir.

Mevcut durumda 108 Sayılı Avrupa Konseyi Sözleşmesi'ne taraf olan 46 üye devletten 45'i AK üyesidir. Uruguay, AB üyesi olmayan ilk devlet olarak 2013 yılında sözleşmeye taraf olmuştur. Fas ise Avrupa Konseyi Bakanlar Kurulu tarafından sözleşmeye taraf olması için davet edilmiştir ve katılımı resmileştirme sürecini yürütmektedir.

1.1.3. Avrupa Birliği Veri Koruma Mevzuatı

AB hukuku antlaşmalardan ve ikincil mevzuattan oluşmaktadır. Avrupa Birliği Antlaşması ve Avrupa Birliğinin İşleyişi Hakkında Antlaşma tüm AB üye ülkeleri tarafından kabul edilmiştir ve bu antlaşmalar 'birincil AB hukuku' olarak tanımlanmaktadır. İkincil AB hukuku olarak adlandırılan belgeler ise AB kurumlarının kurucu antlaşmalardan aldıkları yetkiye dayanarak oluşturdukları ikincil nitelikteki tüzükler, yönergeler ve kararlardır.

Verilerin korunmasına ilişkin temel AB düzenlemesi AP ve AK'nin 95/46/EC sayılı ve 24 Ekim 1995 tarihli Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi'dir.[11] Kabul edildiği tarihte birçok üye devletin ulusal hukukunda konuyla ilgili kanunlar halihazırda bulunmaktaydı. Malların, sermayenin, hizmetlerin ve kişilerin iç pazarda serbest dolaşımı verilerin dolaşımının serbestliğini beraberinde getirmişti. Bu serbestinin bütünüyle sağlanabilmesinin yolu da üye ülkelerin güvenebileceği yeknesak ve yüksek düzeyde bir veri korunmasının varlığından geçmekteydi.

VK Direktifi'nin amacı ulusal düzeydeki veri koruma kanunlarının yeknesaklaştırılması[12] olduğundan, direktif o dönemde var olan ulusal veri koruma kanunlarına nazaran daha belirleyici bir yapıda düzenlenmiştir. Avrupa Birliği Adalet Divanı'nca (ABAD), VK

[9] AK Bakanlar Komitesi, *Avrupa Birliği Toplulukların Katılmasına İzin veren, Kişisel Verilerin Otomatik İşlenmesi Açısından Bireylerin Korunması Sözleşmesine* (ETS No. 108) yapılan değişiklikler, Strazburg, 15 Haziran 1999; değişiklikler yapılmış olan 108 Sayılı Sözleşme'nin 23 (2). maddesi.

[10] AK, *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması, Denetim Otorotileri ve Sınır Ötesi veri Akışlarıyla İlgili Sözleşmesine Ek Protokol*, CETS No. 181, 2001.

[11] Veri Koruma Direktifi, OJ 1995 L 281, s. 31.

[12] Örneğin, Veri Koruma Direktifi, Gerekçe 1, 4, 7 and 8.

Direktifi'nin amacı [...] bireylerin kişisel verilerin işlenmesiyle alakalı hak ve özgürlüklerinin korunmasının tüm üye devletlerde eşit düzeyde olmasını sağlamaktır. [...] Ulusal kanunların birbirlerine yakınlaştırılmaları, kesinlikle korumanın azaltılması sonucunu doğurmamalıdır, tam tersine, AB içinde yüksek derecede bir koruma düzeyi sağlamalıdır. Buna göre, [...] bu ulusal yasaların uyumlaştırılması asgari uyum ile sınırlı kalmamalıdır ve bütünleyici bir yakınlaştırma hedeflenmelidir.[13] Sonuç olarak, AB üyesi ülkelerin direktifi uygularken sınırlı miktarda manevra yapma özgürlükleri bulunmaktadır.

VK Direktifi, 108 Sayılı Sözleşme'nin içinde yer alan özel hayatın gizliliği hakkına dair ilkeleri somutlaştırmak ve genişletmek üzere tasarlanmıştır. Direktifin kabul edildiği 1995 yılında, AB üye ülkelerini oluşturan 15 üye devletin aynı zamanda 108 Sayılı Avrupa Konseyi Sözleşmesi'ne taraf olmaları sebebiyle bu iki düzenleme arasında çelişkili düzenlemeler bulunması olasılığı ihtimal dışı kalmıştır. Üstelik VK Direktifi, 108 Sayılı Avrupa Konseyi Sözleşmesi'nin yeni koruma mekanizmalarının yaratılmasına imkân veren 11. maddesine dayanmaktadır. Özellikle, veri koruma kurallarına uyumu geliştirmesi için getirilen bağımsız denetim mekanizmasının Avrupa veri koruma hukukunun verimli işleyişi açısından önemli bir katkı olarak ortaya çıkmıştır. (Bu mekanizma 108 Sayılı Avrupa Konseyi Sözleşmesi'ne Ek Protokol düzenlemesiyle 2001 yılında AK hukukuna dahil edilmiştir.)

VK Direktifi'nin bölgesel uygulaması AB üyesi 28 devletin de sınırlarını aşmakta ve Avrupa Ekonomik Alanı'nda (EEA)[14] bulunan İzlanda, Lihtenştayn ve Norveç'i kapsamaktadır.

Lüksemburg'da bulunan Avrupa Birliği Adalet Divanı (ABAD), üye devletlerin VK Direktifi kapsamındaki yükümlülüklerini yerine getirip getirmediğini denetleme ve üye devletlerde etkili ve yeknesak uygulanmasını sağlamak için direktifin geçerliliği ve yorumlanmasına dair ön kararlar verme yetkisine sahiptir. VK Direktifi'nin uygulanabilirliği açısından önemli bir istisna gerçek kişilerin yalnızca kişisel veya hanehalkına yönelik amaçlarla kişisel verileri işlemesi durumu, yani "ev istisnası" olarak bilinen durumdur.[15] Genellikle bu tür işlemeler bireyin özgürlüklerinin bir parçası olarak görülmektedir.

VK Direktifi'nin kabul edildiği tarihte yürürlükte olan birincil AB hukukuyla uyumlu olarak, direktifin maddi kapsamı iç pazara dair hususlarla sınırlandırılmıştır. Uygulama kapsamı dışında kalan önemli konular arasında kolluk ve ceza yargılaması konularındaki iş birliği yer almaktadır. Bu alanlarda verilerin korunmasına dair düzenlemeler başka yasal belgelerde yer almaktadır. Bölüm 7'de bunlara detaylı olarak değinilecektir.

VK Direktifi sadece AB üye devletlerini muhatap alabildiği için, kişisel verilerin AB kurum ve kuruluşları tarafından işlenmesi aşamasındaki korumayı sağlamak üzere ek bir yasal düzenlemeye ihtiyaç duyulmuştur. Birlik kurumları ve birimleri tarafından kişisel verilerin işlenmesi bakımından bireylerin korunması ve bu tür verilerin serbest dolaşımı hakkında 18 Aralık 2000 tarihli ve (AT) 45/2001 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü[16] bu konuları düzenlemiştir.

---

[13] ABAD, Birlikte Görülen C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ve Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011, par. 28-29.

[14] 1 Ocak 1994'te yürürlüğe girmiş olan Avrupa Ekonomik Alanı Sözleşmesi, OJ 1994 L 1.

[15] Veri Koruma Direktifi, Madde3 (2) ikinci kısım.

[16] Kişisel verilerin Topluluk kurumları ve organları tarafından işlenmesiyle ilgili olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı hakkında 18 Aralık 2000 tarihli ve (AT) 45/2001 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü, OJ 2001 L 8.

Buna ek olarak, VK Direktifi kapsamında düzenlenmiş olan alanlarda bile, diğer meşru çıkarları dengeleme noktasında gereken belirginliğe erişebilmek için daha detaylı veri koruma hükümlerine sıklıkla gerek duyulmaktadır. Bunun iki örneği olarak Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına ilişkin 2002/58/EC sayılı Direktif ve 2006/24 sayılı Veri Saklama Direktifi[17] verilebilir.[18] Diğer örnekler 8. Bölüm'de ele alınacaktır. Bu hükümler VK Direktifi ile uyumlu olmalıdır.

Avrupa Birliği Temel Haklar Şartı

Avrupa Toplulukları tarafından düzenlenmiş olan temel antlaşmalarda insan haklarına ve bu hakların korumasına yönelik bir referans bulunmamaktaydı. Zamanla, Avrupa Birliği Adalet Divanı önüne gelen davalar yeni bir yaklaşım oluşturmaya başladı. Bireylerin insan haklarını korumak amacı ile temel haklara AB'ye ait genel ilkeler altında yer verildi. Avrupa Birliği Adalet Divanına göre bu genel ilkeler ulusal anayasalarda ve uluslararası insan hakları antlaşmalarındaki ve özellikle de AİHS'sinde bulunan insan haklarının temelini yansıtmaktadır. Avrupa Birliği Adalet Divanı kendine AB mevzuatının tümünü bu temel ilkeler ile uyumlu hale getirmeyi görev edinmiştir.

Avrupa Birliği çıkarmış ve yürütmekte olduğu politikalarının vatandaşlarının insan haklarını etkileyebileceğini kabul ederek ve vatandaşlarının AB'ye daha 'yakın' olmalarını sağlamak amacı ile, 2000 yılında Avrupa Birliği Temel Haklar Şartı'nı ilan etmiştir. Bu Şart ulusal anayasal gelenekleri ve uluslararası yükümlülükleri göz önünde bulundurarak, Avrupa Birliği'ne üye ülkelerin vatandaşlarının bireysel, sosyal ve ekonomik haklarını düzenlemiştir. Şart altı bölümden oluşmaktadır; onur, özgürlükler, eşitlik, dayanışma, vatandaş hakları ve adalet.

Temelinde, Şart politik bir belge olarak tasarlanmıştır ancak 1 Aralık 2009'da yürürlüğe giren Lizbon Anlaşması ile yasal bağlayıcılık kazanmış ve birincil AB hukuku olarak tanımlanmıştır.[19]

Avrupa Birliğinin İşleyişi Hakkındaki Antlaşma'nın (ABİHA) 16. maddesi uyarınca, verilerin korunması ile alakalı konular AB'nin genel düzenleme yetkisine sahip olduğu bir alan olarak belirlenmiştir.[20]

Şart, 7. madde uyarınca özel ve aile yaşamına saygı gösterilmesi hakkını garantiye almakla yetinmemekte, 8. maddesinde verilerin korunması hakkını da düzenlemekte ve bu korumanın seviyesini AB hukukunda yer alan bir temel hak seviyesine çıkartmaktadır. AB kurumlarının yanı sıra üye devletler de AB mevzuatını uygularken bu hakkı gözetmek ve korumak ile sorumlu tutulmuşlardır (Şart'ın 51. maddesi). VK Direktifi'nin yürürlüğe girmesinden birkaç yıl sonra düzenlenen Şart'ın 8. maddesi o dönemde var olan AB veri koruma hukukunu toparlayan bir düzenleme olarak ele alınmalıdır. Bu sebeple de Şart sadece 8. maddenin 1. fikrasında veri koruma hakkından bahsetmekle kalmayıp aynı zamanda 8. maddenin 2. fikrasında kilit veri koruma ilkelerine de atıf yapmaktadır. Son olarak 8. maddenin 3. fikrası bu ilkelerin uygulamasının bağımsız bir makam tarafından denetlenmesini düzenlemiştir.

[17] Avrupa Birliği Parlamentosu ve Konseyi, 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi, OJ 2002 L 201.

[18] 2006/24/AB Sayılı Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması veya Kamu Haberleşme Ağları Çerçevesinde Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Direktif, telekomünikasyon sektöründe kişisel verilerin korunmasına yönelik 2002/58/AT Direktifini değiştirmektedir, OJ 2006 L 105, 8 Nisan 2014 hükümsüz kalmıştır.

[19] AB (2012), Temel Haklar Şartı, OJ 2012 C 326.

[20] Bakınız Avrupa Birliği Antlaşması, OJ 2012 C 326; (2012), Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, OJ 2012 C 326.

Genel Görünüş

2012 yılı Ocak ayında, Avrupa Komisyonu mevcut veri koruma mevzuatının hızlı teknolojik gelişmeler ve küreselleşme ile birlikte modernize edilmesi gerektiğini belirtmiştir. AK'nin reform paketinde VK Direktifi'nin yerine geçirilmesi hedeflenen bir Genel Veri Koruma Tüzüğü[21] önergesi yer almaktadır. Ayrıca kolluk ve cezai konularda adli işbirliği hususlarını kapsayan yeni bir Genel Veri Koruma Direktifi[22] de önerilmektedir paket kapsamında. Bu el kitabının yayınlandığı sırada reform paketi üzerindeki tartışma devam etmekteydi.

1.2. Hakların dengelenmesi

Ana başlıklar

- Verilerin korunması hakkı mutlak bir hak değildir; diğer haklar ile dengelenmelidir.

Avrupa Birliği Temel Haklar Şartı madde 8'de düzenlenmiş olan kişisel verilerin korunmasına dair temel hak *'mutlak bir hak olarak yorumlanmamalı ve ancak toplumdaki fonksiyonuna bağlı olarak dikkate alınmalıdır'*.[23] Bu sebeple de Şart'ın 52. maddesinin 1. fıkrası, söz konusu sınırlamaların kanunla düzenlenmiş olması; hak ve özgürlüklerin özüne dokunmaması ve ölçülülük ilkesine uygun olması; gerekli olması ve AB tarafından kabul edilen kamu yararı amaçlarına veya diğer bireylerin hak ve özgürlüklerinin korunması ihtiyacına uygun olması koşuluyla 7. ve 8. maddede düzenlenen hakların sınırlanmasının mümkün olabileceğini kabul etmektedir.[24]

Verilerin korunması AİHS madde 8 (özel ve aile hayatına sayı gösterilmesi hakkı) ile güvence altına alınmaktadır ve Şart'da da olduğu üzere bu hak diğer yarışan hakların kapsamına saygı çerçevesinde uygulanmalıdır. AİHS'nin 8. maddesinin ikinci fıkrasına göre verilerin korunmasına dair hakkın kullanılmasına, kanuna uygun olarak yapılması ve demokratik bir toplumda […] diğerlerinin hak ve özgürlüklerinin korunması için gerekli olması durumu hariç, bir kamu otoritesi tarafından müdahalede bulunulması yasaklanmıştır.

Sonuç olarak, AİHM ve ABAD birçok kez, AİHS 8. maddesinin ve Şart' ın 8. maddesinin uygulanması kapsamında verilerin korunması hakkının diğer haklar ile dengelenmesinin gerekliliğine değinmiştir.[25] Bu dengenin nasıl kurulması gerektiği, aşağıdaki bölümlerde bulabileceğiniz üzere, birçok örnek ile detaylı bir şekilde açıklanmıştır.

---

[21] Avrupa Komisyonu (2012), *Kişisel verilerin işlenmesi bakımından gerçek kişilerin korunması ve bu kişisel verilerin serbest dolaşımına ilişkin Tüzük önerisi*, COM(2012) 11 final, Brüksel, 25 Ocak 2012.

[22] Avrupa Komisyonu (2012), *Kişisel verilerin işlenmesi bakımından gerçek kişilerin korunması ve bu kişisel verilerin serbest dolaşımına, cezai suçların önlenmesine, soruşturulmasına, tespit edilmesine veya kovuşturulmasına veya para cezalarının infaz edilmesine ilişkin Direktif önerisi,* COM(2012) 11 final, Brüksel, 25 Ocak 2012.

[23] Örneğin, ABAD, Birlikte Görülen C-92/09 ve C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Kasım 2010, par. 48.

[24] *A.e.*, par. 50.

[25] AİHM, *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 ve 60641/08, 7 Şubat 2012; ABAD, Birlikte Görülen C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011, par. 48; ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 Ocak 2008, par. 68. Bakınız Avrupa Konseyi (2013), Kişisel Verilerin korunmasına ilişkin Avrupa İnsan Hakları Mahkemesi'nin İçtihat Hukuku, DP (2013): www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_ FINAL.pdf.

1.2.1. İfade özgürlüğü

Verilerin korunması hakkı ile muhtemel bir çatışma yaşayabilecek haklardan biri ifade özgürlüğü hakkıdır.

İfade özgürlüğü hakkı, ifade ve bilgilenme özgürlüğü altında Avrupa Birliği Temel Haklar Şartı madde 11'de düzenlenmiştir. Bu hak kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin kanaat özgürlüğünü ve haber ve görüş alma ve de verme özgürlüğünü de kapsar. Bu madde AİHS'deki madde 10'a karşılık gelmektedir. Şart'ın 52. maddesinin 3. fıkrası uyarınca, AİHS ile güvence altına alınan haklara tekabül eden hakları içermesi durumunda, "bu hakların anlamı ve kapsamı AİHS'deki düzenleme ile aynı olacaktır". Bu sebeple, Şart'ın 11. maddesinde güvence altına alınan hakka kanuna uygun olarak getirilebilecek sınırlandırmalar AİHS'nin 10. maddesinin 2. Fıkrasında yer alan sınırlandırmalardan daha geniş olamayacaktır. Yani bu sınırlamaların kanunla düzenlenmiş olmaları ve demokratik bir toplumda, diğerlerinin itibarının ve haklarının korunması için gerekli olmaları gerekecektir. Bu kavram veri koruma hakkını da kapsamaktadır.

Kişisel verilerin korunması ve ifade özgürlüğü arasındaki ilişki, 'Kişisel verilerin işlenmesi ve ifade özgürlüğü' başlığı altında VK Direktifi'nin 9. maddesinde düzenlenmiştir.[26] Bu madde uyarınca üye devletler verilerin korunması ve dolayısıyla da direktifin 2, 4 ve 5. bölümlerinde düzenlenen özel hayatın gizliliği temel hakkına ilişkin belirli istisnaları veya sınırlamaları düzenlemekle sorumludurlar. Bu istisnalar, özel hayatın gizliliği hakkının ifade özgürlüğünü düzenleyen kurallarla uzlaştırılması gerektiği ölçüde, ancak ve ancak ifade özgürlüğü kapsamında yer alan gazetecilik veya sanatsal, edebi ifade amaçlı sınırlamalar şeklinde düzenlenebilir.

Örnek: '**Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ve Satamedia Oy'**[27] kararında ABAD'ın VK Direktifi'nin 9. maddesini ve verilerin korunması hakkı ile basın özgürlüğü hakkı arasındaki ilişkiyi yorumlaması istenmiştir. Mahkeme, 1.2 milyon gerçek kişinin yasal olarak Fin vergi makamlarından elde edilmiş vergi verilerinin Markkinapörssi ve Satamedia tarafından yayınlanmasını incelemek durumunda kalmıştır. Mahkemenin özellikle yorumlaması gerektiği konu, vergi makamları tarafından sunulan kişisel verilerin, cep telefonu kullanıcılarının diğer gerçek kişilere ait vergi verilerine erişmeleri amacıyla işlenmesinin yalnızca gazetecilik amacıyla gerçekleştirilmiş bir eylem sayılıp sayılamayacağıdır. Mahkeme Satakunnan'ın faaliyetlerinin VK Direktifi'nin 3. maddesinin 1. fıkrasına göre 'kişisel verilerin işlenmesi'ni teşkil ettiğini belirledikten sonra, direktifin 9. maddesini yorumlamıştır.

İlk olarak, ifade özgürlüğünün her demokratik toplumdaki önemine işaret etmiştir ve bu özgürlüğe ilişkin olan gazetecilik gibi kavramların geniş şekilde yorumlanması gerektiği sonucuna varmıştır. Daha sonra iki temel hak arasında bir denge sağlamak amacı ile, verilerin korunması hakkına yönelik istisnaların ve sınırlamaların sadece gerekli olduğu takdirde uygulanmasını öngörmüştür. Bu koşullar altında, ABAD, Markkinapörssi ve Satamedia tarafından yürütülen ve ulusal mevzuat gereği kamusal alanda yer alan belgelerden elde edilen bilgileri içeren faaliyetlerin, eğer bu faaliyetlerin amacı, iletim için kullanılan mecradan bağımsız olarak, bilgilerin, kanaatlerin veya fikirlerin kamuya açıklanması ise 'gazetecilik faaliyetleri' olarak sınıflandırılabileceğine karar vermiştir.

[26] Veri Koruma Direktifi, Madde 9.

[27] ABAD, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,* 16 Aralık 2008, par. 56, 61 ve 62.

Ayrıca mahkeme, bu faaliyetlerin basın faaliyetleri ile sınırlı olmadığını, aynı zamanda kar amaçlı olarak da faaliyette bulunabileceğini belirtmiştir. Ancak, Mahkeme somut olayda böyle bir faaliyetin söz konusu olup olmadığı konusunda verilecek kararı ulusal mahkemeye bırakmıştır.

AİHM ifade özgürlüğü hakkı ile verilerin korunması hakkının uzlaştırılması ile ilgili olarak dönüm noktası niteliğinde birçok karar vermiştir.

Örnek: **'Axel Springer AG v. Almanya'**[28] davasında AİHM, ünlü bir oyuncunun tutuklanması ve mahkumiyeti ile alakalı haber yapmak isteyen bir gazetenin sahibine yönelik olarak yerel mahkeme tarafından getirilmiş olan yayın yasağının AİHS'nin 10. maddesini ihlal ettiği kararına varmıştır. AİHM daha önceki içtihatları kapsamında belirlediği ve ifade özgürlüğü ve özel hayatın gizliliği hakkı arasındaki dengeyi sağlarken esas alınması gereken kriterleri vurgulamıştır:

- İlk olarak, yayınlanan haberin kamunun yararına ve ilgisine mazhar olup olmadığı kriteri; ünlü bir kişinin tutuklanması ve mahkumiyeti kamuya açık yargısal bir gerçektir ve bu sebeple de kamu yararınadır;
- İkinci olarak, ilgili kişinin kamusal bir figür olup olmadığı kriteri; somut olayda söz konusu oyuncu kamusal bir figür sayılmaya yetecek derecede tanınmış bir kişiliktir;
- Üçüncü olarak, bilginin nasıl elde edildiği ve güvenilir olup olmadığı kriteri; bilgiler savcılık tarafından sağlanmıştır ve haberlerde yer alan bu bilgilerin doğruluğu taraflar arasında tartışma konusu olmamıştır.

Bu nedenle, AİHM, ilgili şirkete getirilen yayın yasağının meşru bir amaç olan özel hayatın gizliliğinin korunmasıyla ölçülü olmadığına karar vermiştir. Mahkeme AİHS'nin 10. maddesinin ihlal edildiği sonucuna varmıştır.

Örnek: **'Von Hannover v. Almanya (No.2)'**[29] davasında AİHM, kocasıyla beraber gittiği kayak tatilinde çekilen fotoğraflarının yayının durdurulmasına yönelik ihtiyati tedbir talebi reddedilen Monako Prensesi Caroline'in AİHS'nin 8. maddesinde yer alan özel hayatına saygı gösterilmesi hakkının ihlal edilmemiş olduğuna hükmetmiştir. Söz konusu fotoğraf Prens Rainier'in sağlığının kötüye gitmesine dair bir haber eşliğinde verilmiştir. AİHM, ulusal mahkemelerin, yayıncı şirketlerin ifade özgürlüğü hakkı ile başvuru sahibinin özel hayata saygı gösterilmesi hakkını dikkatli bir şekilde dengelediği sonucuna varmıştır. Ulusal mahkemelerin Prens Rainier'in sağlık durumunu çağdaş topluma mal olmuş bir olay olarak görmesi mantıksız olarak görülmemiş ve söz konusu haber ışığında değerlendirildiğinde fotoğrafın kamu yararına ilişkin bir tartışmaya en azından bir dereceye kadar katkıda bulunduğu AİHM tarafından kabul edilmiştir. Mahkeme AİHS'nin 8. maddesinin ihlal edilmediği sonucuna varmıştır.

AİHM içtihatlarına göre, hakların dengelenmesi hususunda en önemli kriterlerden biri söz konusu ifadenin, konuşulmasında kamu yararı olan bir tartışmaya katkıda bulunup bulunmadığıdır.

[28] AİHM, *Axel Springer AG v. Germany [GC]*, No. 39954/08, 7 Şubat 2012, par. 90 ve 91.
[29] AİHM, *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 ve 60641/08, 7 Şubat 2012, par. 118 ve 124.

Örnek: **'Mosley v. Birleşik Krallık'**[30] davasında ulusal bir haftalık gazete başvuruda bulunan ile ilgili mahrem fotoğraflar yayınlamıştır. Bunun üzerine başvuru sahibi, şikayet konusu gazetenin bir kişinin özel hayatının gizliliğini ihlal edebilecek mahiyette yayınlar yapılmadan önce ilgili kişiye ön bildirim yapılması yönünde bir prosedürü bulunmadığından fotoğrafın yayınlanması öncesinde ihtiyati tedbir yoluna gitmesinin de imkansız hale getirildiğini, bu sebeplerle AİHS'nin 8. maddesinin ihlal edildiğini öne sürmüştür. Fotoğrafların yayınlanması eğitimden çok eğlence amacı güttüğü için, tartışmasız olarak AİHS'nin 10. maddesinin sağladığı korumadan yararlanmış olsa da paylaşılan bilgilerin özel ve mahrem mahiyette olduğu ve yayınlanmalarında kamu yararı olmadığı durumlarda AİHS'nin 8. maddesinde aranan şartlara uyulması gerekceği açıktır. Ancak yayın öncesi bir sansür gibi işleyebilecek bu tip sınırlamalar ele alınırken ayrı bir özen gösterilmesi gerekmiştir. AİHM ön bildirim şartının yaratabileceği caydırıcı etkiyi, böyle bir ön bildirim sürecinin etkililiği ve bu alanda oluşabilecek keyfiyetin genişliğiyle alakalı şüpheleri göz önüne alarak, yasal açıdan bağlayıcı nitelikte bir ön bildirim şartının AİHS'nin 8. maddesi kapsamında gerekli olmadığına karar vermiştir.

Örnek: **'Biriuk v. Litvanya'**[31] davasında başvuruda bulunan, günlük yayınlanan bir gazeteden kendisinin AIDS'li olduğuna dair bir haber yayınladığı için tazminat talebinde bulunmuştur. Bu bilginin yerel hastanedeki sağlık görevlileri tarafından doğrulandığı iddia edilmiştir. AİHM ilgili haberin yayınlanmasında kamu yararı bulunmadığını ve kişisel verilerin, özellikle de tıbbi bilgilerin korumasının AİHS'nin 8. maddesinde güvence altına alındığı üzere bir bireyin özel ve aile hayatına saygı gösterilmesi hakkı açısından temel nitelikte olduğunu vurgulamıştır. Ayrıca, Mahkeme gazetede yayınlanan makalede verilen bilgiye göre hastane görevlileri tarafından sağlandığı iddia edilen bilgilerin tıbbi gizlilik yükümlülüklerini açıkça ihlal ettiğine dikkat çekmiştir. Sonuç olarak, devlet başvuranın özel hayatının gizliliği hakkını güvence altına almakta başarısız olmuştur ve 8. maddenin ihlal edildiği sonucuna varılmıştır.

1.2.2. Belgelere erişim

Şart'ın 11. maddesi ve AİHS'nin 10. maddesi gereğince bilgi edinme hakkı bilgi vermeyi olduğu kadar bilgi alma hakkını da korur. Demokratik bir toplumun işleyişinde devlet yönetiminin şeffaflığı giderek önem kazanmaktadır. Son 20 yılda, kamu otoriteleri tarafından tutulan belgelere erişim hakkı her AB vatandaşının ve bir üye ülkede ikamet eden herhangi bir gerçek kişinin veya bir üye ülkede kayıtlı işyeri bulunan herhangi bir tüzel kişinin önemli bir hakkı olarak kabul edilmiştir.

Avrupa Konseyi mevzuatı kapsamında, Resmi Belgelere Erişim Sözleşmesi'ni (205 sayılı AK Sözleşmesi) kaleme alanlara ilham veren Resmi Belgelere Erişim Tavsiye Kararı'ndaki ilkelere atıfta bulunulabilir.[32] **Avrupa Birliği mevzuatına göre**, belgelere erişim hakkı, AP'nin, AK'nin ve Avrupa Komisyonu'nun belgelerine kamunun erişimiyle alakalı 1049/2001 sayılı Tüzük ile korunma altına alınmıştır.[33] Şart'ın 42. maddesi ile Avrupa Birliğinin İşleyişine İlişkin Antlaşmanın 15. maddesinin 3. fıkrası bu erişim hakkını 'AB kurumları, kuruluşları, ofisleri ve ajansları'nı kapsayacak şekilde genişletmiştir. Şart'ın 52. maddesinin 2. fıkrası

[30] AİHM, *Mosley v. the United Kingdom*, No. 48009/08, 10 Mayıs 2011, par. 129 ve 130.

[31] AİHM, *Biriuk v. Lithuania*, No. 23373/03, 25 Kasım 2008.

[32] Avrupa Konseyi, Bakanlar Komitesi (2002), Üye Devletlere Resmi Belgelere Erişim ile ilgili Öneri, 21 Şubat 2002; Avrupa Konseyi, Resmi Belgelere Erişim Sözleşmesi, CETS No. 205, 18 Haziran 2009. Sözleşme henüz yürürlüğe girmemiştir.

[33] 1049/2001(AB) Sayılı, Avrupa Birliği Parlamentosu, Konseyi ve Komisyonu'nun belgelerine erişim ile ilgili, Avrupa Birliği Parlamentosu ve Konsey Tüzüğü, 30 Mayıs 2001, OJ 2001 L 145.

gereğince bu hak aynı zamanda Avrupa Birliği'nin İşleyişine İlişkin Antlaşma'nın 15. maddesinin 3. fikrasında belirtilmiş olan şartlara ve sınırlamalara göre uygulanacaktır. Bir belgeye erişilmesi başkalarının kişisel verilerini ifşa edeceksei bu durumda belgelere erişim hakkının verilerin korunması hakkı ile çatışabileceğini söyleyebiliriz. Bu sebeple bilgi ve belgelerin erişime sunulması talepleri değerlendirilirkeni bu bilgi ve belgeler içerisinde kişisel verileri yer alanlar bakımından verilerin korunması hakkı ile belgelere erişim hakkı arasında bir denge gözetilmelidir.

Örnek: **'Avrupa Komisyonu v. Bavarian Lager'**[34] davasında, ABAD AB kurumlarının belgelerine erişim ve 1049/2001 sayılı ve 45/2001 sayılı Tüzükler arasındaki ilişki bağlamında kişisel verilerin korunmasının kapsamını tanımlamıştır. 1992 yılında kurulmuş olan Bavarian Lager, Almanya'dan Birleşik Krallığa başta birahaneler ve barlar için olmak üzere şişelenmiş Alman birası ithalatı yapmaktadır. Ancak Birleşik Krallık mevzuatının fiilen ulusal üreticilere öncelik tanıması sebebiyle birtakım sorunlarla karşı karşıya kalmıştır. Bavarian Lager'in şikâyeti üzerine, Avrupa Komisyonu Birleşik Krallığın AB mevzuatı uyarınca yükümlülüklerini yerine getirmediğine kanaat getirmiş ve gerekli işlemleri başlatmıştır. Bunun sonucunda tartışma konusu ulusal hükümler değiştirilmiş ve AB hukuku ile uyumlu hale getirilmiştir. Sonrasında Bavarian Lager, Avrupa Komisyonu'ndan, Komisyon temsilcilerinin, İngiliz yetkililerin ve Ortak Pazar Bira Üreticileri Konfederasyonu'nun (CBMC; Confédération des Brasseurs du Marché Commun) katılımı ile gerçekleşen bir toplantının tutanağını talep etmiştir. Komisyon toplantıya ilişkin bazı belgelerin ifşasını kabul etmiş, ancak toplantıda bulunan 5 kişinin ismini, 2 kişinin talebi üzerine, kalan 3 kişiye de ulaşılamadığı gerekçesiyle belgelerden silmiştir. Komisyon, Bavarian Lager'in toplantı tutanaklarının eksiksiz halini talep ettiği yeni başvurusunu, Veri Koruma Tüzüğü'nde güvence altına alınan kişilerin özel hayatının gizliliğine atıfta bulunarak, 18 Mart 2014 tarihli kararı ile reddetmiştir. Bavarian Lager Komisyon'un bu kararından tatmin olmamış ve İlk Derece Mahkemesi'nde dava açmıştır. Mahkeme Komisyon'un kararını 8 Kasım 2007 tarihli kararıyla (T-194/04 Bavarian Lager v. Commision dosyası) iptal etmiş ve bir kurum veya kuruluşun temsilcisi olarak bir toplantıya katılan söz konusu kişilerin isimlerinin ifşa edilmesinin bu kişilerin özel hayatın gizliliğini ihlal etmediğine ve bu kişilerin özel hayatlarını herhangi bir şekilde tehlikeye atmadığına karar vermiştir.

Komisyon'un temyizi üzerine ABAD, İlk Derece Mahkemesi'nin verdiği kararı iptal etmiştir. ABAD, Belgelere Erişim Tüzüğü'nün 'kişisel verileri belirli durumlarda kamuya açıklanabilecek bir kişinin korunması için getirilmiş özel ve güçlendirilmiş bir sistem' kurduğunu belirtmiştir. ABAD'a göre, Belgelere Erişim Tüzüğü'ne dayanılarak kişisel verileri de içeren belgelere erişim talebinde bulunulması halinde Veri Koruma Tüzüğü'nün hükümleri bir bütün olarak uygulama alanı bulacaktır. Sonrasında ABAD, Komisyon'un Ekim 1996 tarihli toplantıya dair tutanakların eksiksiz olarak verilmesi yönündeki talebin reddine karar vermekte haklı olduğuna karar vermiştir. Toplantıda bulunan beş katılımcının rızalarının yokluğu göz önüne alındığında, ilgili isimlerin silinmiş olduğu bir tutanağı paylaşan Komisyon'un aleniyet yükümlülüğünü yerine getirdiği ifade edilmiştir.

Ayrıca, ABAD'a göre, "Bavarian Lager, söz konusu kişisel verilerin aktarılmasını meşru kılacak veya bu yönde bir gerekliliğin bulunduğuna ikna edecek herhangi bir gerekçe göstermediği için Komisyon'un ilgili tarafların çıkarları arasındaki dengeyi tespit etmesi mümkün olmamıştır. Bu bağlamda, Veri Koruma Tüzüğü kapsamında şart koşulduğu üzere

[34] ABAD, C-28/08 P, *Avrupa Komisyonu v. The Bavarian Lager Co. Ltd.*, 29 Haziran 2010, par. 60, 63, 76, 78 ve 79.

verileri açıklanacak kişilerin meşru çıkarlarının zarara uğratılabileceğine dair bir çıkarımda bulunmak da mümkün olmamıştır.

Bu karar uyarınca, verilerin korunması hakkına belgelere erişim kapsamında yapılacak bir müdahalenin belirli ve meşru bir sebebi bulunmalıdır. Belgelere erişim hakkı veri koruma hakkını otomatik olarak hükümsüz bırakamaz.[35]

AİHM'nin aşağıdaki kararında bir erişim talebinin hususi bir yönü ele alınmaktadır.

Örnek: **'Tarsasag a Szabadságjogokért v Macaristan'**[36] davasında insan hakları alanında faaliyet gösteren bir sivil toplum kuruluşu Anayasa Mahkemesi'nden devam eden bir dava hakkındaki belgelere erişim talep etmiştir. Anayasa Mahkemesi, söz konusu davayı mahkeme önüne getiren milletvekiline rıza verip vermeyeceği konusunda danışmaksızın davacı tarafın rızası olmadan bilgilerin üçüncü kişilere aktarılamayacağı gerekçesiyle erişim talebini reddetmiştir. Ulusal mahkemeler de bu kapsamdaki kişisel verilerin korunmasının, kamusal bilgilerin erişilebilirliği de dahil diğer meşru amaçlar tarafından geçersiz hale getirilemeyeceği gerekçesiyle bu ret kararını onamışlardır. Başvuran somut olayda bir "toplumsal denetçi" olarak hareket etmiştir ve bu açıdan medyaya tanınan güvencelerin benzerlerine sahiptir. AİHM basın özgürlüğü ile alakalı kararlarında istikrarlı bir şekilde kamunun, kamu yararına yönelik meseleler hakkında bilgi alma hakkının bulunduğunu ifade etmiştir. Başvuran tarafından talep edilen bilgiler 'hazır ve ulaşılabilir' niteliktedir ve herhangi bir veri toplama işlemini gerektirmemektedir. Böyle durumlarda, devletin başvuran tarafından talep edilen bilgilerin aktarımına engel olmama yükümlülüğü bulunmaktadır. Özetle AİHM, kamu yararına yönelik bilgilere erişimi engellemek amacıyla tasarlanan engellerin, medyada ya da bağlantılı alanlarda çalışanların hayati önem taşıyan "toplumsal denetçilik" rollerini yerine getirme konusundaki heveslerini kırabileceğini değerlendirmiştir. AİHM 10. maddenin ihlal edildiğine hükmetmiştir.

AB mevzuatı kapsamında, şeffaflığın önemi kesin bir biçimde vurgulanmıştır. Şeffaflık ilkesi Avrupa Birliği Antlaşması'nın 1. ve 10. maddesinde ve Avrupa Birliği'nin İşlemesine ilişkin Antlaşma'nın 15. maddesinin 1. fikrasında yer bulmuştur.[37] 1049/2001 sayılı Avrupa Komisyonu Tüzüğü'nün gerekçesinin 2. maddesi uyarınca şeffaflık, vatandaşların karar oluşturma sürecine katılımlarının geliştirilmesini, idarenin meşruiyetinin artırılmasını ve demokratik toplum içerisinde yer alan vatandaşlar için daha verimli ve güvenilir olmasını sağlamaktadır.[38]

Bu gerekçelendirmeden hareketle, ortak tarım politikaların finansmanına dair 1290/2005 sayılı Konsey Tüzüğü ve bu tüzüğün uygulanmasında dair detaylı düzenlemeler getiren 259/2008 sayılı Komisyon Tüzüğü kapsamında tarım sektörüne özgülenmiş belirli bazı AB fonlarının lehtarlarına ilişkin bilgilerin ve her bir lehtara ayrılan fon miktarlarının yayınlanması şartı öngörülmüştür.[39] Bahsedilen bilgilerin yayınlanması, kamu fonlarının idare tarafından uygun

[35] Bakınız: Avrupa Veri Koruma Denetçisi tarafından yayınlanan (2011), 'Bavarian Lager' kararından sonra kişisel veriler içeren metinlere kamusal erişim hakkı, Brüksel 24 Mart 2011: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/ Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

[36] AİHM, *Társaság a Szabadságjogokért v. Hungary*, No. 37374/05, 14 Nisan 2009; par. 27, 36–38.

[37] AB (2012), Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın Konsolide Versiyonları, OJ 2012 C 326.

[38] ABAD, C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communities*, 6 Mart 2003, par. 39; ve ABAD, C-28/08 P, *Avrupa Komisyonu v. The Bavarian Lager Co. Ltd.*, 29 Haziran 2010, par. 54.

[39] Ortak Tarım Politikası'nın Finansmanı Hakkında, 1290/2005 (AB) Sayılı Konsey Tüzüğü, 21 Haziran 2005, OJ 2005 L 209;

kullanımının kamu tarafından denetlenmesine katkıda bulunacaktır. Çok sayıda lehtar bu bilgilerin yayınlanmasının ölçülülük ilkesini ihlal ettiği yönünde itirazlar ileri sürmüştür.

Örnek: **'Volker ve Markus Schecke ve Hartmut Eifert v. Land Hessen'**,[40] davasında ABAD'ın, AB tarımsal destek fonundan yararlananların isimlerinin ve aldıkları yardımın miktarının yayınlanmasının ölçülülük ilkesine uygun olup olmadığını değerlendirmesi gerekmiştir. Verilerin korunması hakkının mutlak bir hak olmadığını belirten ABAD, iki AB tarımsal fonundan yararlanan kişilerin isimlerinin ve bu kişilerin hangi miktarda yardım aldıklarının bir internet sitesinde yayınlanmasının genel bağlamda kişilerin özel hayatına ve özel olarak da kişisel verilerin korunması hakkına müdahale teşkil ettiğini ifade etmiştir.

Mahkeme Şart'ın 7. ve 8. maddelerine yönelik bu müdahalenin kanuna düzenlenmiş bir sınırlama olduğuna ve bu sınırlamanın AB tarafından kabul edilen bir kamu yararı gözetilerek, yani kamu fonlarının kullanımında şeffaflığın artırılması amacıyla yapıldığına karar vermiştir. Ancak, somut olaya yönelik olarak Mahkeme, bu iki tarımsal fondan yararlanan kişilerin isimlerinin ve aldıkları miktarın yayınlanmasının orantısız bir önlem olduğuna ve Şart'ın 52. Maddesinin 1. fıkrası uyarınca da haklı gösterilemeyeceğine karar vermiştir. Sonuç olarak Mahkeme, AB mevzuatının Avrupa tarımsal fonlarından yararlananların bilgilerinin yayınlanmasına dair hükümlerini kısmen hükümsüz kılmıştır.

1.2.3. Sanat ve Bilim Özgürlüğü

Kişisel verilerin korunması hakkı ve özel hayata saygı gösterilmesi hakkı ile dengelenmesi gereken bir diğer önemli hak ise Şart'ın 13. maddesinde açıkça korunan sanat ve bilim özgürlüğüdür. Bu hak temel olarak ifade ve düşünce özgürlüğü hakkının bir parçasıdır ve Şart'ın 1. maddesiyle (İnsan onuru) bağlantılı olarak uygulanmalıdır. AİHM sanat ve bilim özgürlüğünün AİHS'nin 10. maddesi kapsamında korunduğunu belirtmektedir.[41] Şart'ın 13. maddesi ile güvence altına alınan bu hak AİHS'nin 10. maddesinin izin verdiği sınırlandırmalara da tabi olabilir.[42]

Örnek: **'Vereinigung Bildender Künstler v. Avusturya'**[43] davasında, Avusturya mahkemeleri, başvurucu konumundaki derneğin, kamuya mal olmuş kişilerin başlarının fotoğraflarını çeşitli cinsel pozisyonlarda gösteren bir tabloyu sergilemeye devam etmesini yasaklamışlardır. Söz konusu tabloda fotoğrafı kullanılan Avusturyalı bir milletvekili başvuru sahibi derneğe karşı dava açmış ve tablonun sergilenmesinin durdurulması için ihtiyati tedbir talebinde bulunmuştur. Yerel mahkeme söz konusu milletvekilinin talebini kabul etmiş ve resmin sergilenmesinin tedbiren durdurulmasına karar vermiştir. AİHM, AİHS'nin 10. maddesinin devleti veya halkın bir kısmını rencide eden, şok etkisi yaratan veya rahatsız eden fikirlerin aktarılması bakımından da geçerli olduğunu tekrar hatırlatmıştır.

Sanatsal çalışmaları oluşturan, icra eden, dağıtan veya sergileyen kişiler fikirlerin ve kanaatlerin yayılmasına katkıda bulunmaktadır ve devletin de bu kişilerin ifade özgürlüklerine tecavüz etmeme yükümlülüğü söz konusudur. Söz konusu tabloda kişilerin

ve *Avrupa Birliği Tarımsal Garanti Fonu (EAGF) ve Avrupa Birliği Kırsal Kalkınma Tarım Fonundan (EAFRD) kaynaklanan fonlarından faydalanan kişilerin bilgileri'nin yayınlanmasına ilişkin 259/2008 (AB) Sayılı Konsey Tüzüğü*, 18 Mart 2008, OJ 2008 L 76.

[40] ABAD, Birlikte Görülen C-92/09 ve C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 Kasım 2010, par. 47–52, 58, 66–67, 75, 86 ve 92.

[41] AİHM, *Müller and Others v. Switzerland*, No. 10737/84, 24 Mayıs 1988.

[42] Temel Haklar Şartı'nın gerekçesi, OJ 2007 C 303.

[43] AİHM, *Vereinigung bildender Künstler v. Austria*, No. 68345/01, 25 Ocak 2007; özellikle bakınız: par. 26 ve 34.

yalnızca başlarının fotoğraflarının kullanıldığını ve resimdeki vücutların gerçeği yansıtma veya buna dair tahminde bulunma amacı bile taşımayacak derecede gerçek dışı ve abartılı bir biçimde boyanmış olduğunu göz önüne alan AİHM, söz konusu tablonun tasvir edilen şahsın özel hayatına ait detaylara yönelik olmaktan ziyade şahsın bir siyasetçi olarak toplumdaki duruşunu hedef aldığını, bu sebeple de tasvir edilen şahsın eleştirel bağlamda daha hoşgörülü davranması gerektiğini ifade etmiştir.

Mahkeme somut olaydaki tüm menfaatleri tartarak, tablonun sergilenmesinin yasaklanmasına yönelik sınırsız bir yasağın orantısız olacağını belirlemiştir. Sonuç olarak Mahkeme AİHS'nin 10. maddesinin ihlal edildiği kanaatine varmıştır.

Bilime ilişkin olarak, Avrupa veri koruma mevzuatı bilimin toplumdaki özel değerinin farkındadır. Bu nedenle, kişisel verilerin kullanımına yönelik bu alandaki sınırlandırılmalar azaltılmıştır. Gerek VK Direktifi gerekse 108 Sayılı Sözleşme verilerin ilk toplanma amaçları kapsamında gereksiz hale gelmesi durumunda bilimsel araştırmalar için saklanabilmesine izin vermektedir. Hatta verilerin bilimsel araştırma için tekrar kullanımları uygun olmayan bir amaç olarak değerlendirilmeyecektir. Bilimsel araştırmalardan elde edilecek fayda ve verilerin korunması hakkının uzlaştırılması için gerekli tedbirleri alma görevi de ulusal hukuka verilmiştir (Bkz. Bölüm 3.3.3 ve 8.4).

1.2.4. Mülkiyetin korunması

Mülkiyetin korunması hakkı Şart'ın 17. maddesinin 1. fıkrasında ve AİHS'nin Birinci Protokol'ünün 1. maddesinde düzenlenmiştir. Mülkiyet hakkının önemli bir unsuru Şartın 17. maddesinin 2. fıkrasında bahsedildiği üzere fikri mülkiyetin korunmasıdır. AB hukuk düzeninde fikri hakların, özellikle de telif haklarının etkili bir biçimde korunmasına dair birçok direktif bulunmaktadır. Fikri mülkiyet sadece fikir ve sanat eserlerinin mülkiyetini değil, patent, marka ve bunlara bağlı hakları da kapsamaktadır.

ABAD içtihadında açıkça ifade edildiği üzere temel bir hak olan mülkiyet hakkının korunması ile diğer temel hakların -özellikle verilerin korunması hakkının- korunması arasında bir denge kurulması gerekmektedir.[44] Telif haklarını koruma amacıyla faaliyet gösteren kurumların, internet hizmet sağlayıcılardan, dosya paylaşım platformlarını kullanan kişilerin kimliklerini ifşa etmelerini talep ettiği davalar olmuştur. Söz konusu platformlar internet kullanıcılarının, müzik parçalarını, bu parçalar telif hakları ile korunuyor olsalar bile para ödemeden indirmelerini sıklıkla mümkün kılmaktadır.

[44] AİHM, *Ashby Donald and others v. France,* No. 36769/08, 10 Ocak 2013.

Örnek: **'Promusicae v. Telefonica de Espana'** davası,[45] Telefonica isimli İspanyol internet erişim sağlayıcı şirketin, müzik sektöründeki bazı yapımcı ve yayıncılardan oluşan Promusicae isminde kâr amacı gütmeyen bir kuruluş tarafından kendisine yöneltilen ve erişim sağlama hizmeti verdiği bazı kişilere dair kişisel verileri paylaşması yönündeki talebi reddine ilişkindir. Promusicae'nin bu verilerin paylaşılmasını talep etmekteki gerekçesi, faydalanma hakkı Promusicae üyelerine ait olan bazı fonogramlara erişim sağlayan bir dosya transfer programını kullanan belirli kişilere yönelik adli işlemleri başlatabilmesi için bu bilgilere ihtiyacı olmasıdır.

İspanya Mahkemesi davayı ABAD'a taşımış ve bu kişisel verilerin paylaşımının adli süreç kapsamında ve telif haklarının etkili bir biçimde korunabilmesi adına AB hukuku çerçevesinde mümkün olup olmadığını sorgulamıştır. Şart'ın 17. Ve 47. maddesi bağlamında 2000/31, 2001/29 ve 2004/48 sayılı Direktiflere de atıfta bulunmuştur. Mahkeme, üye devletlerin, telif haklarının etkin bir biçimde korunmasını sağlayabilmek adına açılacak davalar kapsamında kişisel verilerin ifşa edilmesine yönelik bir yükümlülük getirmesi halinde yukarıdaki üç direktifin ve 2002/58 sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi'nin buna bir engel teşkil etmeyeceğini ifade etmiştir.

Bu sebeplerle de ABAD, söz konusu davanın, çeşitli temel hakların, yani özel hayata saygı gösterilmesi hakkı ile mülkiyetin korunması ve etkili kanun yolu haklarının sağladığı güvencelerin uzlaştırılmasına yönelik bir ihtiyaç olup olmadığı sorusu etrafında döndüğüne işaret etmiştir.

Mahkeme, üye devletlerin yukarıda anılan direktifleri ulusal alanda uygularlarken bu direktifleri, Topluluğun yasal düzeni tarafından korunan çeşitli temel haklar arasında bir denge kurulmasını sağlayacak şekilde yorumlamaları gerektiğine hükmetmiştir. Bunun da ötesinde, bu direktiflerin öngördüğü tedbirleri uygularken de üye devletlerin yetkilileri ve mahkemelerinin kendi ulusal mevzuatlarını bu direktiflerle uyumlu bir şekilde yorumlamaları ve bu direktiflerin temel haklarla veya Topluluk hukukunun diğer genel ilkeleriyle -örneğin ölçülülük ilkesiyle- çelişecek bir yoruma başvurmamaları gerektiği belirtilmiştir. [46]

2. Veri koruma terminolojisi

AB	İşlenen konular	AK
Kişisel Veriler		

[45] ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 Ocak 2008, par. 54 ve 60.
[46] *A.e.*, par. 65 ve 68; ve ayrıca bakınız: ABAD, C-360/10, *SABAM v. Netlog N.V.*, 16 Şubat 2012.

VK Direktifi, Madde 2 (a) ABAD, Birleştirilmiş davalar C-92/09 ve C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 Kasım 2010 ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 Ocak 2008	**Hukuki tanım**	108 Sayılı Sözleşme, Madde 2 (a) AİHM, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 Mart 2013
VK Direktifi, Madde 8 (1) ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003	**Özel nitelikli kişisel veriler (hassas veriler)**	108 Sayılı Sözleşme, Madde 6
VK Direktifi, Madde 6 (1) (e)	**Anonim hale getirilmiş veya takma isim ile değiştirilmiş veriler**	108 Sayılı Sözleşme, Madde 5 (e) 108 Sayılı Sözleşme, Explanatory report, Madde 42
Verilerin işlenmesi		
VK Direktifi, Madde 2 (b) ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003	**Tanımlar**	108 Sayılı Sözleşme, Madde 2 (c)
Veri kullanıcıları		
VK Direktifi, Madde 2 (d)	**Veri sorumlusu**	108 Sayılı Sözleşme, Madde 2 (d) Profilleme Tüzüğü, Madde 1 (g) *
VK Direktifi, Madde 2 (e) ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003	**Veri işleyen**	Profilleme Tüzüğü Madde 1 (h)
VK Direktifi, Madde 2 (g)	**Veri alıcısı**	108 Sayılı Sözleşme, Ek Protokol, Madde 2 (1)

VK Direktifi, Madde 2 (f)	**Üçüncü kişi**	
Rıza		
VK Direktifi, Madde 2 (h) ABAD, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011	**Geçerli rızanın tanımı ve şartları**	Tıbbi Veriler Tavsiye Kararı, Madde 6, ve çeşitli müteakip tavsiye kararları

Not: * Avrupa Birliği Konseyi Bakanlar Komitesi (2010), Rec(2010)13 Sayılı, Üye Devletlerin, profilleme bağlamında, kişisel verilerin otomatik olarak işlenmesine ilişkin olarak bireylerin korunması hakkındaki Tüzüğü, (Profilleme Tüzüğü*), 23 Kasım 2010.*

2.1. Kişisel veriler

Ana başlıklar

- Kimliği belirli veya belirlenebilir bir kişiye, yani veri öznesine ilişkin her türlü veri kişisel veridir.
- Veri öznesinin belirlenmesi için makul bir çaba ile ek bilgiye ulaşmak mümkün ise o kişi belirlenebilir sayılır.
- Belirli bir kişinin belirli bir kimliğe sahip olduğunun ve/veya belirli faaliyetleri yürütmeye yetkili kılınmış olduğunun ispatlanması kimlik doğrulama kavramı ile ifade edilir.
- 108 sayılı Sözleşme ile Veri Koruma Direktifi'nde sayılan özel nitelikli veri kategorileri (hassas veri olarak bilinir) bulunmaktadır. Bunlar daha yüksek bir koruma seviyesine ihtiyaç duymaları sebebiyle ayrı bir yasal rejime tabidirler.
- Herhangi bir tanımlayıcı bilgi içermeyecek hale getirilmiş veriler anonim hale getirilmiş veri olarak tanımlanır; tanımlayıcı bilgileri şifrelenmiş veriler ise takma isim ile değiştirilmiş veri haline gelirler.
- Anonim hale getirilmiş verilerin aksine, takma isim ile değiştirilmiş veriler kişisel veridirler.

2.1.1. Kişisel veri kavramının temel unsurları

AB ve AK mevzuatı altında, kişisel veri kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır.[47] Yani, kimliği ayan beyan ortada olan veya ek bilgi temini yoluyla kimliği saptanabilecek bir kişi hakkındaki bilgi. Böyle bir kişinin verilerinin işlenmesi durumunda da bu kişiye 'veri öznesi" denir.

Kişi

Verilerin korunması hakkı özel hayata saygı gösterilmesi hakkından doğmuştur. Özel hayat kavramı insan varlığına ilişkin bir kavramdır. Bu sebeple de gerçek kişiler bu korumadan asli olarak yararlanan kişilerdir. 29. Madde Çalışma Grubu'nun verdiği Görüş'e göre Avrupa veri koruma hukuku yalnızca canlı varlıkları korumaktadır.[48]

[47] Veri Koruma Direktifi, Madde2 (a); 108 Sayılı Sözleşme, Madde2 (a).
[48] Madde 29 Çalışma Kurultayı (2007), *Kişisel Veri kavramı üzerine görüş 4/2007*, WP 136, 20 Haziran 2007, s. 22.

AİHM'nin AİHS madde 8'e dair içtihatları da bize göstermektedir ki özel ve mesleki hayata dair meseleleri birbirinden tamamen ayırmak her zaman kolay değildir.[49]

Örnek: **'Amann v. İsviçre'**[50] davasında, yetkililer başvurana gelen iş amaçlı bir telefon aramasını dinlemişlerdir. Sonrasında yetkililer, bu telefon görüşmesine dayanarak başvuran hakkında bir araştırma yürütmüşler ve başvurana dair bir ulusal güvenlik kaydı açarak başvuranı fişlemişlerdir. Dinleme konusu telefon görüşmesi iş hayatına yönelik bir görüşme olmasına rağmen AİHM, bu görüşmeye dair saklanan verilerin başvuranın özel hayatına ait olduğuna hükmetmiştir. AİHM özel hayat kavramının dar şekilde yorumlanmaması gerektiğine, zira özel hayata saygı kavramının diğer insanlarla ilişkiler kurabilme ve bunları ilerletebilme hakkını da kapsadığına işaret etmiştir. Mahkeme sonrasında, mesleki veya işle alakalı faaliyetlerin özel hayat kavramının dışında tutulmasını haklı gösterecek herhangi bir sebep olmadığını ifade etmiştir. Bu şekilde geniş bir yorum 108 Sayılı Sözleşme'nin yorumuyla da uyuşmaktadır. AİHM ayrıca başvuranın davasına konu olan dinlemenin de hukuka uygun olmadığını, zira ulusal hukukun verilerin toplanması, kaydedilmesi ve saklanması ile alakalı olarak yeterince belirli ve detaylı hükümler içermediğini ifade etmiştir. Bu sebeple Mahkeme AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Eğer mesleki hayata dair konular da veri korumasından yararlanabiliyorsa, yalnızca gerçek kişilere koruma sağlanması hususu sorgulanır hale gelmektedir. AİHS kapsamında düzenlenen haklar sadece gerçek kişileri değil herkesi kapsamaktadır. AİHM'in içtihatları arasında tüzel kişilerin AİHS madde 8 kapsamında haklarının ihlal edildiği gerekçesiyle yaptıkları başvurulara dair kararlar bulmak mümkündür. Ancak Mahkeme, bu başvuruyu özel hayata saygı gösterilmesi hakkından ziyade konut ve haberleşme hakkına saygı gösterilmesi hakkı kapsamında ele almıştır:

Örnek: **'Bernh Larsen Holding AS ve Diğerleri v. Norway'**[51] davası üç Norveçli şirketin vergi idaresinin bir kararına karşı yaptıkları bir şikâyete dairdir. Söz konusu kararda, bu üç şirket tarafından ortak olarak kullanılan bir sunucudaki bütün verilerin bir kopyasının vergi denetçilerine verilmesi emredilmektedir.

AİHM başvuran şirketlere yüklenen böylesi bir yükümlülüğün AİHS madde 8 uyarınca başvuran şirketlerin konut ve haberleşme hakkını ihlal ettiğine karar vermiştir. Ancak, Mahkeme vergi dairesinin kötü niyetli kullanımı engellemek için, etkili ve yeterli önlemler aldığını tespit etmiştir: şirketler yeterli süre önceden haberdar edilmişlerdir; sunucuya müdahale sırasında orada bulunmalarına ve görüş bildirmelerine olanak tanınmıştır; vergi teftişi sonlandığında veriler imha edileceğine dair bir güvence sağlanmıştır. Bu koşullar altında, başvuran şirketlerin konut ve haberleşme hakkı ve şirket çalışanlarının gizliliğini korumaktaki çıkarları ile vergi teftişinin etkili bir şekilde yapılmasının sağlanmasına yönelik kamu yararı arasında adil bir denge kurulmuştur. Sonuç olarak, AİHM, AİHS madde 8'in ihlal edilmediğine karar vermiştir.

[49] Örneğin: AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 Mayıs 2000, par. 43; AİHM, *Niemietz v. Germany*, 13710/88, 16 Aralık 1992, par. 29.
[50] AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, par. 65.
[51] AİHM, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 Mart 2013. Bakınız, AİHM, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 Temmuz 2008.

108 Sayılı Sözleşme gereği, koruma birincil olarak gerçek kişilerin verilerinin korunmasına yöneliktir ancak, eğer üye ülkeler tercih ederlerse örneğin şirketler ve dernekler vb. tüzel kişiler de koruma kapsamına alınabilir.

Veri Koruma Direktifi tüzel kişilere ait verilerin işlenmesiyle alakalı olarak bu kişilerin korunmasına yönelik bir düzenleme içermemektedir. Ulusal yasakoyucular bu konuda yasal düzenleme yapmakta serbesttir.[52]

Örnek: **'Volker ve Markus Schecke ve Arazi Hessen v Hartmut Eifert'**[53] davasında ABAD, tarımsal yardımlardan yararlananların kişisel verilerinin yayınlanmasına atıfta bulunarak, tüzel kişilerin Şart'ın 7. ve 8. maddesi kapsamında koruma talep edebilmelerinin tüzel kişinin ticari ünvanının ifşasının bir veya birden fazla gerçek kişinin kimliğinin tespitine yol açacak olması durumunda söz konusu olabileceğine karar vermiştir. […] Şart'ın 7. ve 8. maddelerinde düzenlenen kişiler verilerin işlenmesi bağlamında özel hayata saygı gösterilmesi hakkı belirli ya da belirlenebilir bir bireye ait her türlü veriyi içermektedir .[54]

Bir kişinin belirlenebilirliği

AB ve AK mevzuatı gereğince, aşağıdaki şartların varlığı halinde bilginin bir kişiye ait veri içerdiği kabul edilir:

- Bilginin içeriğinde kişinin kimliği açıkça belirli olması; veya
- kimlik açıkça belirli olmasa da, verilen bilgilerde kişinin, az bir araştırma ile kimliğine ulaşılabilecek şekilde tasvir edilmiş olması.

Her iki bilgi türü de Avrupa veri koruma hukuku tarafından aynı şekilde koruma altına alınmıştır. AİHM defaatle AİHS'deki kişisel veri kavramının, özellikle de belirli veya belirlenebilir kişilere ait olma şartı bakımından 108 Sayılı Sözleşme ile aynı olduğunu belirtmiştir.[55]

Kişisel veriye dair yasal tanımlar kişinin hangi koşullar altında belirli sayılacağına dair açıklamalarda bulunmamaktadır.[56] Kimliğin belirlenmesi için kişiyi diğer bütün kişilerden ayırt edilebilir ve bir birey olarak tanınabilir bir biçimde tasvir eden unsurların gerekeceği aşikardır. Bir kişinin ismi bu tasvir edici unsurlara dair en temel örnek olarak gösterilebilir. İstisnai durumlarda diğer belirleyici unsurlar da kişinin ismine benzer bir etki yaratabilir. Örneğin, kamuoyuna mal olmuş kişiler -örneğin Avrupa Komisyonu'nun Başkanı- bakımından o kişinin bulunduğu mevkiden bahsetmek yeterli olabilir.

Örnek: **'Promusicae'**[57] davasında ABAD, Promusicae'nin belirli bir internet dosya paylaşım platformunu kullanan belirli bazı kullanıcıların isim ve adreslerini içeren bilgilerin iletilmesini istemesinin kişisel verilerin, yani kimliği belirli veya belirlenebilir gerçek kişilere ait bilgilerin paylaşılması anlamına geldiği konusunda anlaşmazlık bulunmadığını ifade etmiştir. Promusciae'nin ileri sürdüğü ve Telefonica'nın da itiraz etmediği üzere, Telefonica tarafndan saklanan bu bilgilerin iletimi, 2002/58 sayılı Direktif'in 2. maddesinin ilk paragrafı

[52] Veri Koruma Direktifi, Gerekçe 24.
[53] ABAD, Birlikte Görülen C-92/09 and C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 Kasım 2010, par. 53.
[54] *A.e.,* par. 52.
[55] Bakınız AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, par. 65.
[56] Bakınız AİHM, *Odièvre v. France* [GC], No. 42326/98, 13 Şubat 2003; ve AİHM, *Godelli v. Italy*, No. 33783/09, 25 Eylül 2012.
[57] ABAD, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 Ocak 2008, par. 45.

ve 95/46 sayılı Direktif'in 2. maddesinin b bendi birlikte değerlendirildiğinde, kişisel verilerin işlenmesi olarak değerlendirilmektedir.

Birçok isim eşsiz olmadığı için, kişinin kimliğini belirlemek ve başka birisiyle karıştırılmadığından emin olmak için ek belirleyici unsurlara ihtiyaç duyulabilir. Doğum tarihi ve yeri sıklıkla kullanılmaktadır. Buna ek olarak, vatandaşların daha iyi bir şekilde ayırt edilebilmesini sağlayabilmek için bazı ülkelerde kişiselleştirilmiş numaraların da kullanıldığı bilinmektedir. İçinde yaşadığımız teknolojik çağda parmak izleri, dijital fotoğraflar veya iris taramaları gibi biyometrik verilerin kimlik tespitindeki önemleri giderek artmaktadır.

Veri koruma hukukunun uygulama alanı bulabilmesi için veri öznesinin yüksek düzeyde tespitine gerek bulunmamaktadır; kişinin belirlenebilir olması yeterli görülmektedir. Kişinin belirlenebilir olması, bilginin bir parçasından doğrudan veya dolaylı olarak tespit edilebilir olması anlamına gelmektedir.[58] Veri Koruma Direktifi'nin Gerekçe bölümünün 26. maddesine göre buradaki temel ölçüt, tanımlama için gereken makul yolların bulunma ve bu yolların, 3. kişiler de dahil olmak üzere, öngörülebilir kullanıcılar tarafından kullanılma ihtimalinin yüksekliğidir. (Bkz. Bölüm 2.3.2.)

Örnek: Yerel bir otorite bölgedeki sokaklarda hız yapan arabalara dair veri toplamaya karar verir. Hız sınırını aşanların cezalandırılmasını sağlamak amacıyla, arabaların fotoğraflarını çeker ve fotoğrafın çekildiği zaman ve yeri otomatik olarak kaydederek bu verileri yetkili makama iletir. Verileri kaydedilen bir kişi, yerel otoritenin böyle bir veri toplama faaliyeti için veri koruma hukuku kapsamında herhangi bir yasal dayanağının olmadığını öne sürerek şikâyette bulunur. Yerel otorite kişisel veri toplamadığını savunur. Araba plakalarının anonim kişilere dair veriler olduğunu söyler. Yerel otoritenin araç siciline erişerek araç sahibinin veya sürücünün kimliğini tespit etme gibi bir yasal yetkisi bulunmamaktadır.

Öne sürülen bu gerekçe Veri Koruma Direktifi'nin Gerekçe bölümünün 26. maddesi ile örtüşmemektedir. Veri toplamanın amacının açık bir şekilde hız sınırını ihlal edenleri tespit etmek ve cezalandırmak olduğu göz önüne alındığında, kimlik tespitinin de yapılmaya çalışılacağı öngörülebilir bir durumdur. Yerel otoritelerin doğrudan kimlik tespiti yapabilecekleri bir yolları bulunmasa da bu yollara sahip bir merci olan polise bu verileri ileteceklerdir. Gerekçe'nin 26. maddesinde de verinin ilk kullanıcısından sonraki aşamada veriyi teslim alanların bireyi tespit etmeye teşebbüs edebilecekleri bir durum açıkça öngörülmektedir. Gerekçe m. 26'nın sunduğu bakış açısıyla değerlendirildiğinde yerel otoritenin eylemi belirlenebilir kişilerle alakalı veri toplamakla eşdeğerdir ve bu sebeple de veri koruma hukuku kapsamında yasal bir dayanağı bulunmalıdır.

AK mevzuatı gereğince, belirlenebilirlik benzer bir şekilde anlaşılmaktadır. Ödeme ve Diğer İşlemler İçin Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı'nın 1. maddesinin 2. fıkrası kimliğin belirlenmesi çok uzun zaman, masraf veya insan gücü gerektirecekse, kişinin belirlenebilir sayılmayacağını belirtmektedir.[59]

Kimlik doğrulama

Bu prosedür bir kişinin belirli bir kimliğe sahip olduğunu ve/veya güvenlikli bir bölgeye girme veya bankadaki bir hesaptan para çekme gibi belirli şeyleri yapmaya yetkili olduğunu

[58] Veri Koruma Direktifi, Madde 2(a).

[59] Avrupa Konseyi, Bakanlar Komitesi (1990), *Ödeme ve diğer ilgili operasyon için kullanılan kişisel verilerin korunması hakkında Öneri (90) 19*, 13 Eylül 1990.

kanıtlayabileceği bir süreçtir. Kimlik doğrulama, bir pasaporta kayıtlı fotoğraf veya parmak izi gibi biyometrik verilerin örneğin göç idaresine gelen bir kişinin verileriyle karşılaştırılması yoluyla; veya kimlik numarası veya şifre gibi yalnızca belirli bir kimliğe veya yetkiye sahip bir kişi tarafından bilinebilecek bilgilerin sorulması yoluyla; veya özel bir çipli kart veya bir banka kasasının anahtarı gibi yalnızca belirli bir kimliğe veya yetkiye sahip bir kişide bulunabilecek bir nesnenin ibrazını şart koşma yoluyla yapılabilir. Şifreler veya çipli kartlar dışında, bazen pin kodlarıyla birlikte kullanılan elektronik imzalar da elektronik işlemlerle alakalı olarak bir kişinin kimliğini belirleme ve doğrulama noktasında elverişli araçlardan birisidir.

Verilerin tabiatı

Her türlü bilgi, bir kişiye ilişkin olması şartı ile kişisel veri olabilir.

Örnek: Bir işçinin işte gösterdiği performansa dair amiri tarafından yapılan ve işçinin özlük dosyasında saklanan değerlendirme, "işçi kendini işine vermiyor" ve "işçi geçtiğimiz altı ay içerisinde beş hafta boyunca işe gelmedi" gibi kısmen veya bir bütün olarak amirin kişisel yorumunu yansıtan bilgilerden oluşsa bile işçiye dair kişisel veridir.

Kişisel veriler kişinin özel hayatının yanı sıra mesleki ve sosyal hayatına dair bilgileri de kapsamaktadır.

'Amann' davasında,[60] AİHM kişisel veri kavramını yorumlarken, bu kavramın kişinin özel alanına dair konularla sınırlı olmadığını söylemiştir. (Bkz. Bölüm 2.1.1.) Burada verilmiş olan tanım aynı zamanda Veri Koruma Direktifi açısından da önem taşımaktadır.

Örnek: **'Volker ve Markus Schecke ve Harmut Eifert v. Land Hessen'**[61] davasında ABAD söz konusu verilerin iş hayatına yönelik olmasının bir anlam ifade etmediğini vurgulamıştır. Bu noktada AİHM, AİHS madde 8'in yorumuna da atıfta bulunarak, 'özel hayat' teriminin sınırlayıcı bir biçimde yorumlanmaması gerektiğini ve mesleki faaliyetlerin özel hayat kavramının dışında tutulmasını haklı gösterecek herhangi bir sebep olmadığını belirtmiştir.

Bilgilerin içeriği bir kişiye dair verileri dolaylı olarak açığa vurduğunda bile veriler kişilere ilişkindir. Bir nesne veya bir olay -örn. bir cep telefonu, bir araba, bir kaza- ile bir kişi –örn. telefonun sahibi, arabayı kullanan, kazanın kurbanı- arasında yakın bir bağlantı bulunduğu bazı durumlarda bir nesne veya bir olay hakkındaki bilginin bile kişisel veri sayılması gerekebilir.

Örnek: **'Uzun v. Almanya'**[62] davasında başvuru sahibi ve diğer bir adam bombalı saldırılara dahil oldukları şüphesiyle gözetim altına alınmış ve bu diğer adamın arabasına yerleştirilen cihaz yoluyla küresel bir takip sistemi (GPS) üzerinden takip edilmiştir. AİHM, başvuranın GPS yoluyla takibinin başvuranın AİHS madde 8 ile korunan özel hayatına müdahale teşkil ettiğini belirtmiştir. Ancak AİHM, GPS gözetlemesinin kanuna uygun olarak yapıldığını ve çok sayıda cinayet teşebbüsüne dair soruşturma yürütme şeklindeki yasal amaçla orantılı olduğunu ve bu sebeple de demokratik bir toplumda gerekli olduğunu ifade etmiş ve AİHS madde 8'in ihlal edilmediğine karar vermiştir.

Verilerin görünüş şekli

[60] Bakınız AİHM, *Amann v. Switzerland,* No. 27798/95, 16 Şubat 2000, par. 65.

[61] Birlikte Görülen C-92/09 ve C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Kasım 2010, par. 59.

[62] AİHM, *Uzun v. Germany*, No. 35623/05, 2 Eylül 2010.

Verilerin hangi şekilde saklandığı veya kullanıldığının veri koruma hukukunun uygulanabilirliği ile bir alakası bulunmamaktadır. Yazılı veya sözlü iletişimin yanı sıra fotoğraflar,[63] kapalı devre televizyon sistemine ait görüntü [64]veya ses[65] de kişisel veri içerebilir. Elektronik olarak kaydedilmiş bilgiler veya kâğıda dökülmüş bilgiler de kişisel veri içerebilir; hatta insan dokusuna ait hücre örnekleri de bir kişinin DNA'sını içermeleri sebebiyle kişisel veri olarak sayılabilirler.

2.1.2. Özel nitelikli kişisel veriler

AB ve AK mevzuatında, nitelikleri gereği işlenmeleri halinde veri öznelerine yönelik risk oluşturabilecek ve bu sebeple de daha güçlü bir korumaya ihtiyaç duyan özel kişisel veri kategorileri bulunmaktadır. Özel nitelikli bu kişisel verilerin (hassas verilerin) işlenmesine ancak belirli güvencelerin sağlanması durumunda izin verilmelidir.

Hassas verilerin tanımına ilişkin olarak, gerek 108 Sayılı Sözleşme (madde 6) gerekse Veri Koruma Direktifi (madde 8) aşağıdaki kategorileri saymaktadır:

- Irk veya etnik kökene dair kişisel veriler;
- Siyasi düşünce, inanç veya diğer inançlara dair kişisel veriler;
- Sağlık ve cinsel hayata dair kişisel veriler.

Örnek: **'Bodil Lindqvist'[66]** davasında ABAD, kişinin ayağını incittiğine ve tıbbi gerekçelerle yarı zamanlı çalıştığı gerçeğine atıfta bulunulmasının VK Direktifi madde 8(1) uyarınca sağlığa dair kişisel veri teşkil edeceğini belirtmiştir.

Veri Koruma Direktifi ayrıca siyasi görüş veya bağlantıya dair kuvvetli bir emare olabileceği gerekçesiyle sendika üyeliğine dair bilgiyi de hassas veri olarak değerlendirmektedir.

108 Sayılı Sözleşme cezai mahkumiyetlere dair kişisel verileri de hassas veri olarak saymaktadır.

Veri koruma Direktifi madde 8(7) üye devletlerin "bir ulusak kimlik numarasının veya uygulamada kullanılacak herhangi başka bir tanımlayıcının hangi koşullar altında işlenebileceğine dair şartları belirlemesini şart koşmaktadır.

2.1.3. Anonim hale getirilmiş veya takma isim ile değiştirilmiş veriler

108 Sayılı Sözleşme'de ve VK Direktifi'nde yer alan verilerin sınırlı şekilde saklanması ilkesi uyarınca verilerin, veri öznelerinin verinin toplanma veya işlenme amacı için gerekli olan süreden daha uzun süreler boyunca belirlenmesine imkân vermeyecek bir biçimde saklanması gerekmektedir.[67] Bir veri sorumlusunun bu verileri tarihleri geçmiş olduğu ve ilk olarak belirlenen amaçlarına artık hizmet etmedikleri halde saklamak istemesi durumunda verilerin anonim hale getirilmeleri gerekmektedir.

Anonim hale getirilmiş veriler

[63] AİHM, *Von Hannover v. Germany*, No. 59320/00, 24 Haziran 2004; AİHM, *Sciacca v. Italy*, No. 50774/99, 11 Ocak 2005.
[64] AİHM, *Peck v. the United Kingdom*, No. 44647/98, 28 Ocak 2003; AİHM, *Köpke v. Germany*, No. 420/07, 5 Ekim 2010.
[65] Veri Koruma Direktifi, Gerekçesi 16 ve 17; AİHM, *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 Eylül 2001, par. 59 ve 60; AİHM, *Wisse v. France*, No. 71611/01, 20 Aralık 2005.
[66] ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003, par. 51.
[67] Veri Koruma Direktifi, Madde6 (1) (e); ve 108 Sayılı Sözleşme, Madde 5 (e).

Kişisel verilerin kimlik tespitine yarayabilecek bütün unsurlarından arındırılması halinde veri anonim hale getirilmiş sayılır. Bilgi içerisinde, makul bir çaba gösterilmesi suretiyle veri öznelerin yeniden tespitini sağlayabilecek hiçbir unsur kalamaz.[68] Başarılı bir şekilde anonim hale getirilmiş olan veriler artık kişisel veri değildirler.

Kişisel verilerin işlenmesini gerektiren sebepler ortadan kalkması, ancak tarihsel, bilimsel veya istatiksel sebeplerden dolayı verilerin saklanacak olması durumunda, VK Direktifi ile 108 Sayılı Sözleşme verilerin bu kapsamda saklanmasına ancak kötüye kullanımı önlemeye dair uygun güvencelerin alınması halinde izin vermiştir.[69]

Takma isim ile değiştirilmiş veriler

Kişisel veriler, isim, doğum tarihi, cinsiyet ve adres gibi tanımlayıcı unsurlar içermektedir. Kişisel bilgilerin takma isimle değiştirildiği durumlarda, bu tanımlayıcı unsurlar bir takma isimle değiştirilmektedir. Takma isimle değiştirme, örneğin, kişisel verilerdeki tanımlayıcı unsurların şifrelenmesi yoluyla yapılabilir.

Takma isimle değiştirilmiş veriler 108 Sayılı Sözleşme'nin veya VK Direktifi'nin yasal tanımlar kısmında açıkça yer almamıştır. Ancak, 108 Sayılı Sözleşmeye dair Açıklayıcı Rapor'un 42. Maddesi şu şekilde bir düzenleme içermektedir: "Verilerin isimlerle bağlantılı biçimlerde saklanmasına dair süre sınırlarına ilişkin gereklilik, verilerin belirli bir zamandan sonra bağlantılı oldukları kişinin isminden geri dönülemez biçimde ayrılmaları gerektiği anlamına gelmez; yalnızca verilerin ve tanımlayıcı unsurların kolayca bağlantılandırılmasının mümkün olmaması anlamı taşır. Bunu da verilerin takma isimle değiştirilmesi sayesinde başarmak mümkündür. Şifreyi çözecek anahtara sahip olmayan herkes bakımından, takma isimle değiştirilmiş veri ancak zor bir şekilde kimlik tanımlayıcı hale getirilebilir. Bu durumda bir kimliğe bağlantı halen vardır ancak bu bağlantı artık takma isim ve şifreleme anahtarının birleşiminden oluşmaktadır. Şifreleme anahtarını kullanma yetkisine sahip olanlar açısından kimlik belirlemesinin yeniden yapılması kolaylıkla mümkündür. Şifreleme anahtarlarının yetkisiz kişiler tarafından kullanımına karşı özel önlemler alınmalıdır.

Kişisel verileri kullanmaktan tamamen kaçınmanın mümkün olmadığı günümüzde, geniş ölçekte bir veri korumasına ulaşmanın en önemli yollarından birisi takma isim ile değiştirilmiş veriler olduğundan, bu şekildeki bir değiştirme eyleminin mantığı ve etkisi daha detaylı bir biçimde açıklanmalıdır.

Örnek: 'Charles Spencer, 3 Nisan 1967 doğumlu, 2 erkek ve 2 kız olmak üzere 4 çocuk sahibi' bilgisi aşağıdaki şekilde takma isimler ile değiştirilebilir:

'C.S. 1967, 2 erkek ve 2 kız olmak üzere 4 çocuk sahibi'
'324, 2 erkek ve 2 kız olmak üzere 4 çocuk sahibi'
'YESz3201, 2 erkek ve 2 kız olmak üzere 4 çocuk sahibi'

Takma isimlerle değiştirilmiş bu verilere erişen kullanıcıların birçoğu 324 veya YESz3201 ibarelerinden yola çıkarak "Charles Spencer, 3 Nisan 1967 doğumlu" şeklinde bir kimlik belirlemesi yapamayacaktır. Bu sebeple de takma isimle değiştirilmiş veriler kötüye kullanıma karşı korunma anlamında daha elverişlidir.

[68] *A.e.*, Gerekçe 26.
[69] *A.e.*, Madde6 (1) (e); ve 108 Sayılı Sözleşme, Madde 5 (e).

Ancak ilk verilen örnek daha az koruma sağlamaktadır. "C.S. 1967, 2 erkek ve 2 kız olmak üzere 4 çocuk sahibi" cümlesinin Charles Spencer'ın yaşadığı küçük kasabada kullanılması durumunda, Spencer Bey kolaylıkla tanınabilir. Verilerin takma isimle değiştirilmesinde kullanılan yöntem, verilerin korunmasının etkinliğini etkileyebilir.

Şifrelenmiş tanımlayıcılar içeren kişisel veriler kişilerin kimliğini gizli tutmanın bir yolu olarak çok çeşitli bağlamlarda kullanılmaktadır. Bu yöntem, veri sorumlularının veri öznelerinin gerçek kimliklerini bilmelerinin gerekmediği ancak aynı veri özneleriyle uğraştıklarından emin olmalarının gerektiği durumlar için özellikle kullanışlıdır. Bir araştırmacının bir hastalığın seyrini, kimlikleri yalnızca onları tedavi eden hastaneler tarafından bilinen ve araştırmacının yalnızca takma isimlerle değiştirilmiş vaka geçmişlerine erişebildiği hastalar üzerinden incelemesi hali bu kullanışlılığa bir örnek olarak verilebilir. Bu yüzden takma isimle değiştirme gizliliği pekiştiren teknolojiler arasında önemli bir halkadır. Tasarım yoluyla gizlilik ilkesinin uygulanması aşamasında da önemli bir unsur olarak işlev görebilir. Bu da gelişmiş veri işleme sistemlerinin çekirdeğine yerleştirilmiş bir veri korumaya sahip olmak demektir.

2.2. Veri işleme

Ana başlıklar

- 'İşleme' terimi esas olarak otomatik işlemeyi ifade etmektedir.
- AB mevzuatına göre 'işleme' ek olarak yapılandırılmış dosyalama sistemlerinde yapılan manuel işlemeyi de ifade eder.
- AK mevzuatına göre, 'işleme'nin anlamı manuel işlemeyi de içerek biçimde ulusal hukuk tarafından genişletilebilir.

108 Sayılı Sözleşme ile VK Direktifi kapsamında verilerin korunması birincil olarak otomatik veri işlemesine yöneliktir.

AK mevzuatına göre, otomatik işleme tanımı, otomatik halde gerçekleştirilen işlemlerin bazı aşamalarında kişisel verilerin manuel olarak kullanımının gerekli olabileceğini kabul eder. Benzer şekilde AB mevzuatı da otomatik veri işlemeyi 'kişisel veriler üzerinde tamamen veya kısmen otomatik olarak gerçekleştirilen işlemeler" olarak tanımlamaktadır.[70]

Örnek: **'Bodil Lindqvist'**[71] davasında ABAD:

"Bir internet sitesinde çeşitli kişilere atıfta bulunma ve bu kişilerin kimliklerini ismen veya diğer yollarla, örneğin telefon numaralarını veya çalışma şartlarına veya hobilerine dair bilgiler vererek açık etmek 95/46 sayılı Direktif'in 3. maddesinin 1. fıkrası kapsamında 'kişisel verilerin tamamen veya kısmen otomatik olarak işlenmesi"ne vücut verecektir.

Verilerin manuel olarak işlenmesi de veri korumasını gerektirir.

AB mevzuatı uyarınca verilerin korunması sadece otomatik veri işlemeleri ile sınırlı değildir. AB mevzuatı gereği verilerin korunması manuel dosyalama sistemleri, yani özel olarak yapılandırılmış kağıt dosyalar içerisinde yapılan kişisel veri işlemelerinde de uygulama alanı bulur.[72] Korumanın bu şekilde genişletilmiş olmasının sebepleri şöyledir:

[70] 108 Sayılı Sözleşme, Madde2 (c); ve Veri Koruma Direktifi Madde2 (b) ve Madde3 (1).
[71] ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003, par. 27.
[72] Veri Koruma Direktifi, Madde3 (1).

- Kâğıt dosyalar bilgilerin kolaylıkla ve hızlı bir şekilde bulunmasını sağlayacak bir şekilde yapılandırılabilir ve

- kişisel verilerin yapılandırılmış kağıt dosyalar içerisinde saklanması otomatik veri işlemelerine yönelik olarak mevzuat tarafından getirilen sınırlamaların aşılmasını kolaylaştırır.[73]

AK mevzuatı kapsamında, 108 sayılı Sözleşme esas olarak otomatik veri dosyalarına yönelik veri işlemelerini düzenler.[74] Bunun yanında korumanın manuel işlemeleri de kapsayacak bir biçimde genişletilmesi imkanını ulusal hukuka bırakır. 108 Sayılı Sözleşme'ye taraf birçok ülke bu imkânı kullanmış ve bu şekilde bir genişletme yaptıklarına dair Avrupa Konseyi Genel Sekreteri'ne beyanda bulunmuşlardır.[75] Veri korumasının böyle bir beyan kapsamında genişletilmesi durumunda bunun bütün manuel veri işlemelerine yönelik olması ve manuel dosyalama sistemlerindeki işlemlerle sınırlı olmaması gerekmektedir.[76]

Mevzuat kapsamına dahil olan işlemelerin niteliğine gelindiğinde, gerek AB gerekse AK mevzuatı uyarınca işleme kavramının oldukça kapsamlı olduğu görülür: " 'Verilerin işlenmesi' kişisel veriler üzerinde gerçekleştirilecek her türlü […] toplama, kaydetme, organize etme, saklama, uyarlama, veya değiştirme, kurtarma, danışma, kullanma, aktarım yoluyla ifşa etme, yayma veya başka bir şekilde kullanılabilir kılma, sıralama veya birleştirme, engelleme, silme veya imha etme işlemini içermektedir.[77] Verilerin bir veri sorumlusunun sorumluluk alanından çıkarak başka bir veri sorumlusunun sorumluluk alanına girmesi için gerçekleştirilen eylemler de 'işleme' kavramının kapsamına girmektedir.

Örnek: İş verenler işçileri ile alakalı maaşları ile alakalı olanlar dahil bazı veriler toplar ve bu verileri işlerler. İşverenin bu işlemeleri yasal olarak yapabilmesi iş sözleşmesi sayesindedir.

İş verenler işçilerin maaşlarına ait verileri vergi idarelerine iletmek durumundadır. Verilerin bu şekilde iletimesi 108 Sayılı Sözleşme ve VK Direktifi kapsamında bir 'işleme' teşkil edecektir. Ancak buradaki işlemenin yasal dayanağı iş sözleşmesi değildir. İşverenin vergi makamlarına maaş verilerini iletmesi sonucunu doğuran işleme faaliyetleri için ayrı bir yasal dayanak olması gerekir. Çoğu zaman bu yasal dayanak ulusal vergi yasalarında bulunur. Bu hükümler olmadığı takdirde verilerin aktarımı yasa dışı bir işleme olacaktır.

2.3. Kişisel verilerin kullanıcıları

[73] *A.e.*, Gerekçe 27.
[74] 108 Sayılı Sözleşme, Madde2 (b).
[75] Bakınız 108 Sayılı Sözleşme, Madde3 (2) (c).
[76] Bakınız 108 Sayılı Sözleşme, Madde3 (2).
[77] Veri Koruma Direktifi, Madde2 (b). Bakınız; 108 Sayılı Sözleşme, Madde2 (c).

Ana başlıklar

- Başkalarına ait kişisel verileri işlemeye karar veren kimseler verilerin korunması mevzuatı uyarınca veri sorumlusu sayılırlar; bu kararı birden çok kişi vermişse bu durumda 'ortak sorumlu' olabilirler.
- 'Veri işleyen' bir veri sorumlusu adına kişisel verileri işleyen yasal olarak ayrı bir konuma sahip kurumdur.
- Veri işleyen veri sorumlusunun talimatlarını dinlemeyip verileri kendi amaçları için kullanıyorsa, veri sorumlusu haline gelir.
- Veri sorumlusu tarafından iletilen verileri alan kişiye veri alıcısı denir.
- Veri sorumlusundan talimatları altında hareket etmeyen (ve veri öznesi olmayan) gerçek veya tüzel kişiye 'üçüncü kişi' denir.
- 'Üçüncü kişi veri alıcısı' veri sorumlusundan hukuken ayrı bir konumda bulunan ancak veri sorumlusundan kişisel veri alan kişi veya kurumdur.

2.3.1. Veri sorumluları ve veri işleyenler

Veri sorumlusu veya veri işleyen olmanın en önemli sonucu veri koruma hukukunun getirmiş olduğu yükümlülüklere uyma konusundaki yasal sorumluluktur. Dolayısıyla yalnızca yürürlükteki kanunlar bakımından sorumlu tutulabilecek olanların üstlenebileceği konumlardır. Özel sektörde, genelde bu görevliler gerçek veya tüzel kişilerdir; kamu sektöründe ise çoğu zaman bu bir kamu yetkilisidir. Tüzel kişiliği olmayan kuruluşlar veya kurumlar gibi diğer merciler ise yalnızca özel hükümlerin izin verdiği durumlarda veri sorumlusu veya veri işleyen olabilirler.

Örnek: Sunshine şirketinin pazarlama bölümü bir pazar araştırması için veri işlemeyi planlıyorsa, bu durumda veri sorumlusu pazarlama bölümü değil, Sunshine şirketinin kendisi olacaktır. Pazarlama bölümü kendine ait tüzel kişiliği bulunmadığından veri sorumlusu olamaz.

Şirketler topluluklarında, ana şirket ve bağlı şirketlerden her biri ayrı birer tüzel kişiliğe sahip olduklarından ayrı ayrı veri sorumluları veya veri işleyenler olarak sayılırlar. Bu hukuki bölünmenin bir sonucu olarak bir topluluğun üye şirketleri arasında verilerin aktarılabilmesi için ortada hukuki bir dayanak bulunması gerekecektir. Şirket topluluğunu oluşturan ayrı tüzel kişiler arasında kişisel verilerin aktarımını mümkün kılan bir ayrıcalık bulunmamaktadır.

Bu bağlamda gerçek kişilerin rolünden de bahsedilmesi gerekmektedir. AB mevzuatı kapsamında, gerçek kişiler, yalnızca kişisel veya hanehalkına yönelik faaliyetler kapsamında veri işlemeleri durumunda VK Direktifi kapsamına girmezler; veri sorumlusu sayılmazlar.[78]

Ancak, içtihatlarda bir gerçek kişinin internet kullanımı sırasında başka bireylere ait verileri yayınlaması durumunda verilerin korunması mevzuatının uygulama alanı bulacağına hükmedilmiştir.

Örnek: **'Bodil Lindqvist'**[79] davasında ABAD:

[78] Veri Koruma Direktifi, Gerekçe 12 ve Madde3 (2) son kısım.
[79] ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003.

'Bir internet sayfasında çeşitli kişilere atıfta bulunma ve bu kişilerin kimliklerini ismen veya diğer yollarla açık etmek […] 95/46 sayılı Direktif'in 3. maddesinin 1. fıkrası kapsamında 'kişisel verilerin tamamen veya kısmen otomatik olarak işlenmesi"ne vücut verir.[80]

Kişisel verilerin bu şekilde işlenmesi VK Direktifi'nin kapsamı dışında kalan yalnızca kişisel veya hanehalkına yönelik faaliyetler kapsamında değerlendirilemez; bu istisna "[…] bireylerin yalnızca özel veya aile hayatları kapsamında gerçekleştirdiği faaliyetlere ilişkin" olarak yorumlanmalıdır. Kişisel verilerin internette yayınlanması ve bu verilerin sayısız insanın erişimine açık hale getirilmesiyle bağlantılı işlemeleri bu kapsamda değerlendirmek mümkün değildir.[81]

Veri sorumlusu

AB mevzuatı uyarınca veri sorumlusu "tek başına veya başkalarıyla beraber kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen kişi"dir.[82] Veri sorumlusunun alacağı karar verilerin ne sebeple ve hangi şekilde işleneceğini belirler. AK mevzuatı, veri sorumlusunun tanımı kapsamında ek olarak veri sorumlusunun hangi kişisel veri kategorilerinin saklanması gerektiğine dair kararları veren merci olduğundan bahsetmektedir.[83]

108 Sayılı Sözleşme veri sorumlusunun tanımında bu aşamada değinilmesi gereken başka bir önemli unsurdan daha bahsetmektedir. Bu tanımda belirli bir amaçla belirli bazı verileri yasal olarak kimin işleyebileceği meselesi ele alınmaktadır. Hukuka aykırı işleme faaliyetleri gerçekleştirildiğinin iddia edildiği ve veri sorumlusunun tespit edilmesi gerektiği durumlarda, yasal olarak böyle bir işleme yapmaya yetkili olup olmadığına bakılmaksızın, verilerin işlenmesi gerektiğine karar veren kişi veya kurumun -örneğin bir şirket veya kamu otoritesi- veri sorumlusu sayılacağı düzenlenmektedir.[84] Bu sebeple verilerin silinmesine dair talep her daim 'fiili' anlamdaki veri sorumlusuna yapılmalıdır.

Birlikte veri sorumluluğu

VK Direktifi'nde yer alan tanım gereği, veri sorumlusu olarak birlikte veya ortak olarak hareket eden farklı yasal kuruluşların bulunması mümkündür.[85] Bu bağlamda ilgili kuruluşların verilerin ortak bir amaç için işlenmesine beraberce karar verdikleri söylenebilir. Bunun yasal olarak mümkün olabilmesi için verilerin ortak bir amaç uğruna beraberce işlenmesine imkân veren özel bir yasal dayanağa ihtiyaç bulunmaktadır.

Örnek: Borcunu ödemede temerrüde düşen müşterilere dair birden çok kredi kuruluşu tarafından kullanılan bir veri tabanı birlikte veri sorumluluğu halinin yaygın örneklerinden birisidir. Söz konusu veri tabanının ortak veri sorumlularından birisi olan bir bankaya kredi başvurusu yapıldığında, ilgili banka veri tabanını kontrol eder ve başvuranın kredi başvurusuna dair sağlıklı kararlar verebilir.

[80] *A.e.*, par. 27.
[81] *A.e.*, par. 47.
[82] Veri Koruma Direktifi, Madde2 (d).
[83] 108 Sayılı Sözleşme, Madde2 (d).
[84] Bakınız, Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 15.
[85] Veri Koruma Direktifi, Madde2 (d).

Birlikte veri sorumluluğuna dair düzenlemelerde, veri sorumlularından her birisi için veri işleme amacının aynı olmasının gerekip gerekmediği veya amaçların kısmen örtüşmesinin yeterli olup olmadığı hususunda bir hüküm yoktur. Konuyla alakalı AB düzeyinde bir içtihat ve sorumluluğa dair sonuçlarla alakalı bir netlik bulunmamaktadır. Madde 29 Çalışma Kurultayıbirlikte veri sorumluluğu kavramının mevcut veri işleme durumlarının karmaşıklığı göz önüne alınarak mevzuata bir nebze esneklik tanınması amacıyla daha geniş bir biçimde yorumlanması gerektiğini savunmaktadır.[86] Dünya Bankalararası Finansal İletişim Topluluğu'nun (SWIFT) tarafı olduğu bir dava Çalışma Grubu'nun görüşlerini ortaya koymaktadır.

Örnek: 'SWIFT' davası olarak bilinen davada, Avrupa bankacılık kuruluşları, bankacılık işlemleri sırasında gerçekleştirilen veri aktarımlarını gerçekleştirmesi için, ilk aşamada bir veri işleyen olarak SWIFT'i görevlendirmişlerdir. SWIFT, kendisini görevlendirmiş olan Avrupa bankacılık kuruluşlarından bu yönde bir talimat almaksızın, Birleşik Devletler'deki (A.B.D.) bir sunucu merkezinde tuttuğu bu bankacılık işlemi verilerini A.B.D. Hazine Bakanlığı'yla paylaşmıştır. Madde 29 Çalışma Kurultayıbu durumun yasallığına dair değerlendirmelerde bulunurken SWIFT'in ve SWIFT'i görevlendiren Avrupa bankacılık kurumlarının, Avrupalı müşterilerin verilerinin A.B.D. yetkililerine aktarılmasından dolayı bu müşterilere karşı birlikte veri sorumluları olarak değerlendirilmeleri gerektiği sonucuna varmıştır.[87] SWIFT, verilerin ifşasına karar vererek -hukuka aykırı bir biçimde- veri sorumlusu rolünü üstlenmiştir; bankacılık kuruluşları ise veri işleyeni denetleme yükümlülüklerini yerine getirme konusunda üzerlerine düşeni yapmamışlar ve bu sebeple de veri sorumlusu olarak yükümlülüklerinden sıyrılmış sayılamazlar. Bu durum da birlikte veri sorumluluğunu gerektirmektedir.

Veri İşleyen

AB hukuku kapsamında, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen kişi veri işleyen olarak tanımlanır.[88] Veri işleyenin yetkilendirildiği faaliyetler yalnızca belirli bir görevle sınırlandırılmış olabileceği gibi oldukça geniş ve kapsamlı da olabilir.

AK mevzuatı gereğince, veri işleyenin anlamı AB mevzuatı ile aynıdır.

Veri işleyenler, başkaları için veri işledikleri durumlar haricinde, örneğin kendi işçilerinin yönetimi, satışları veya hesapları vb. kişisel amaçları uğruna gerçekleştirdikleri işleme faaliyetleri bakımından veri sorumlusu sayılacaklardır.

Örnek: Everready şirketi başka şirketlerin insan kaynakları verilerinin yönetimi amacıyla veri işleme konusunda uzmanlaşmıştır. Bu faaliyeti kapsamında Everready bir veri işleyendir.

Everready kendi çalışanlarına ait verileri işlemesi durumunda ise işveren olarak yükümlülüklerini yerine getirme amacıyla gerçekleştirdiği bu veri işleme faaliyetleri bakımından veri sorumlusu olacaktır.

Veri sorumlusu ile veri işleyen arasındaki ilişki

[86] Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 19.
[87] Madde 29 Çalışma Kurultayı (2006), *10/2006 Sayılı, SWIFT aracılığı ile işlenen kişisel verilere ilişkin Öneri,* WP 128, Brüksel, 22 Kasım 2006.
[88] Veri Koruma Direktifi, Madde2 (e).

Daha önce gördüğümüz üzere veri sorumlusu kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen olarak tanımlanmaktadır.

Örnek: Sunshine şirketinin yöneticisi, pazar analizinde uzman bir şirket olan Moonlight şirketinin Sunshine'ın müşteri verilerine ilişkin olarak bir pazar araştırması yapmasına karar verir. Verilerin işlenmesine dair vasıtalara karar verme görevi Moonlight şirketine devredilmesine rağmen Sunshine şirketi veri sorumlusu olarak kalmaya devam eder ve Moonlight şirketi ise, Sunshine'ın müşterilerine ilişkin verileri aradaki sözleşme gereği yalnızca Sunshine şirketinin belirleyeceği amaçlarla sınırlı olarak kullanabilecek olan bir veri işleyen olur.

Verilerin işlenme vasıtalarına karar verme yetkisi bir veri işleyene devredilmiş olsa bile, veri sorumlusu veri işleyenin işleme vasıtaları konusunda aldığı kararlara müdahale edebilecek konumda olmalıdır. Genel sorumluluk halen, veri işleyenlerin kararlarının verilerin korunması hukukuna uygunluğunu denetlemesi gereken veri sorumlusundadır. Veri sorumlusunun veri işleyenin kararlarına müdahale etmesini yasaklayıcı hükümler içeren bir sözleşme büyük ihtimalle her iki tarafın da veri sorumlusuna dair yasal yükümlülükleri paylaştığı bir birlikte veri sorumluluğu olarak yorumlanacaktır.

Ayrıca veri işleyen veri sorumlusu tarafından konulan veri kullanımına dair sınırlandırmalara uymazsa veri sorumlusunun talimatlarını ihlal ettiği ölçüde veri sorumlusu haline gelecektir. Bu da veri işleyeni yüksek ihtimalle, hukuka aykırı bir biçimde hareket eden bir veri sorumlusu haline getirecektir. Buna karşılık olarak, ilk baştaki veri sorumlusunun, veri işleyenin yetki sınırını aşmasının nasıl mümkün olduğunu açıklaması gerekecektir. Madde 29 Çalışma Kurultayıda bu tür durumlarda, veri öznelerinin çıkarlarının en iyi şekilde korunmasını sağladığı için birlikte veri sorumluluğunun söz konusu olduğunu varsaymaktadır.[89] Birlikte veri sorumluluğun getirdiği önemli bir sonuç da veri öznelerine hukuk yolları anlamında daha geniş seçenekler sunan müşterek ve müteselsil tazminat sorumluluğu halleridir.

Veri sorumlusunun küçük çaplı bir şirket, veri işleyenin ise bu küçük şirkete hizmet şartlarını dayatabilecek güçte büyük ölçekli bir şirket olduğu durumlarda sorumluluğun bölünmesine dair sorunlar da söz konusu olabilir. Bu tür durumlarda, Madde 29 Çalışma Kurultayısorumluluk standardının ekonomik dengesizlik gerekçesiyle aşağı çekilmemesinin gerektiğini ve veri sorumlusu kavramına dair yorumlamaya sadık kalınması gerektiğini ifade etmektedir.[90]

Veri sorumlusu ile veri işleyen arasındaki ilişkinin detayları, açıklık ve şeffaflık adına, yazılı bir sözleşme ile belirlenmelidir.[91] Böyle bir sözleşmenin yapılmamış olması, veri sorumlusunun ortak sorumluluklara dair yazılı belge sunma yükümlülüğünün ihlalidir ve yaptırımlara yol açabilir.[92]

Veri işleyenler görevlerinin bir kısmını alt veri işleyenlere devretmek isteyebilirler. Bu şekilde bir devir yasal olarak mümkündür ve veri sorumlusunun her işleme öncesi izninin gerekip

[89] Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 25; ve *10/2006 Sayılı, SWIFT aracılığı ile işlenen kişisel verilere ilişkin Öneri,* WP 128, Brüksel, 22 Kasım 2006.

[90] Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 26.

[91] Veri Koruma Direktifi, Madde17 (3) ve (4).

[92] Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 27.

gerekmeyeceği veya işleme öncesi bilgilendirmenin yeterli olup olmayacağı gibi detaylar veri sorumlusu ve veri işleyen arasında yapılan sözleşmedeki şartlara bağlı olarak belirlenecektir.

AK mevzuatına göre, veri sorumlusu ve veri işleyen kavramlarına yönelik yukarıdaki yorumlar 108 Sayılı Sözleşme'ye uygun olarak alınan tavsiye kararlarından da görülebileceği üzere aynı şekilde geçerlidir.[93]

2.3.2. Veri alıcıları ve üçüncü kişiler

Veri alıcıları ile üçüncü kişiler arasındaki ayrım ilk olarak VK Direktifi kapsamında yapılmıştır ve buradaki fark temelde bu kişi/kurumların veri sorumlusu ile ilişkileri ve veri sorumlusu tarafından saklanan kişisel verilere erişme yetkilerinden kaynaklanmaktadır.

Üçüncü kişi, veri sorumlusundan hukuken farklı bir statüye sahip kişidir. Bu yüzden de verilerin üçüncü kişiye aktarılması her daim yasal bir dayanak gerektirecektir. VK Direktifi'nin 2(f) maddesi uyarınca, üçüncü kişi, "hukuken veri sorumlusundan bağımsız olan ve doğrudan veri sorumlusu veya veri işleyenin yetkisi altında veri işlemeye yetkilendirilmiş herhangi bir gerçek veya tüzel kişiyi, kamu makamı, ajansı veya veri öznesinden başka herhangi bir kişiyi ifade eder". Bu bağlamda, veri sorumlusundan hukuki bakımdan farklı bir şirket için çalışan kişiler -bu şirket aynı şirketler grubuna veya holdinge ait olsalar da- üçüncü kişi olurlar veya üçüncü bir kişiye ait sayılırlar. Buna karşın, banka müşterilerinin hesaplarını genel merkezin doğrudan yetkisi altında işleyen banka şubeleri 'üçüncü kişi' sayılmazlar. [94]

'Veri alıcısı', 'üçüncü kişi'ye kıyasla daha geniş bir terimdir. VK Direktifi madde 2(g) uyarınca veri alıcısı, "üçüncü kişi olsun veya olmasın, kendisine verilerin ifşa edildiği gerçek veya tüzel kişi, kamu makamı, ajans veya başka herhangi bir kişiyi" ifade eder. Veri alıcısı, veri sorumlusu veya veri işleyenin dışında bir kişi -bu durumda bir üçüncü kişi- olabileceği gibi veri sorumlusu veya veri işleyenin bünyesinde bulunan birisi de olabilir. Örneğin veri sorumlusu veya veri işleyenin bir çalışanı veya aynı şirket veya kamu makamının başka bir bölümü olabilir.

Veri alıcısı ve üçüncü kişiler arasındaki ayrımın önemi verilerin hukuka uygun olarak ifşasına dair şartlar bakımından ortaya çıkmaktadır. Veri sorumlusunun veya veri işleyenin çalışanları, veri sorumlusu veya veri işleyenin işleme faaliyetlerinde yer almaları durumunda başka bir yasal şart aranmaksızın kişisel veri alıcısı olabilirler. Buna karşın, veri sorumlusundan veya veri işleyenden hukuken ayrı konumda bulunan bir üçüncü kişi, belirli bir duruma yönelik belirli yasal gerekçeler bulunmadıkça veri sorumlusu tarafından işlenen kişisel verileri kullanmaya yetkili değildir. Bu sebeple 'üçüncü kişi veri alıcıları'nın kişisel verileri hukuka uygun bir biçimde alabilmesi için her zaman hukuki bir dayanağa ihtiyaçları olacaktır.

Örnek: İşvereni tarafından kendisine verilen görevler kapsamında kişisel verileri kullanan bir veri işleyen çalışanı bir veri alıcısıdır; verileri, veri işleyenin talimatları uyarınca ve veri işleyen adına kullandığından üçüncü kişi sayılamaz.

Veri işleyenin bir çalışanı olarak bu verilere erişim imkânı olan bu çalışan verileri kendi amaçları için kullanmak ister ve bunları başka bir şirkete satarsa, bu durumda çalışanın üçüncü kişi olarak hareket ettiği söylenebilecektir. Bu çalışan artık veri işleyenin (işverenin) talimatlarını yerine getirmemektedir. Üçüncü kişi olarak da bu verilerin toplanması ve satışına

[93] Örneğin, Profilleme Tüzüğü, Madde 1.

[94] Madde 29 Çalışma Kurultayı (2010), *1/2010 Sayılı, 'Veri Sorumlusu' ve 'Veri İşleyen' kavramlarına ilişkin Öneri*, WP 169, Brüksel, 16 Şubat 2010, s. 31.

dair bir yasal bir dayanağı olması gerekmektedir. Bu örnekte kesinlikle böyle bir yasal dayanak bulunmamaktadır ve çalışanın faaliyetleri yasal değildir.

2.4. Rıza

Ana başlıklar

- Kişisel verilerin işlenmesine dair hukuki bir dayanak olarak rızanın, özgür iradeyle açıklanmış, bilgilendirilmeye dayalı ve belirli bir konuya ilişkin olması gerekir.
- Rıza açık bir şekilde verilmiş olmalı. Rıza sarih bir şekilde veya veri öznesinin kişisel verilerinin işlenmesine rıza gösterdiğine şüphe bırakmayacak bir biçimde davranması yoluyla zımni olarak verilebilir.
- Özel nitelikli kişisel verilerin işlenmesi ilgilinin açık rızası olmaksızın işlenemez.
- Rıza her zaman geri çekilebilir.

Rıza, "veri öznesi tarafından belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı" ifade etmektedir.[95] Birçok durumda, verilerin işlenmesi için gerekli yasal bir dayanaktır (Bölüm 4.1 bakınız).

2.4.1. Geçerli rızanın unsurları

AB mevzuatı rızanın geçerli olabilmesi için 3 unsurun varlığını aramaktadır. Bu sayede veri öznelerinin, verilerinin kullanımını gerçekten kabul ettikleri hususu güvence altına alınmış olacaktır.

- Veri öznesi rızasını hiçbir baskı altında kalmadan vermiş olmalıdır;
- Veri öznesi rıza vereceği konunun içeriği ve sonuçları hakkında gereğince bilgilendirilmiş olmalıdır;
- Rızanın kapsamı makul derecede belirli olmalıdır.

Bu üç şartın her biri sağlanmış ise, verilerin korunması hukuku kapsamında rıza geçerli sayılmaktadır.

108 Sayılı Sözleşme rızanın tanımlamamasını yapmamakta, bu tanımlamayı ulusal hukuka bırakmaktadır. Ancak, AK mevzuatında, 108 sayılı Sözleşme'ye uygun olarak verilmiş tavsiye kararlarında da ifade edildiği üzere geçerli rızaya dair şartlar yukarıda sunulmuş olan şartlarla aynıdır.[96] Geçerli rıza için aranan şartlar, Avrupa medeni hukukunda geçerli bir irade beyanı için aranan şartlarla aynıdır.

Hukuki ehliyet gibi medeni hukukta geçerli rıza için ek olarak aranan şartlar yasal bağlamda temel ön koşullar olduklarından verilerin korunması alanında da doğal olarak uygulanmaktadır.

[95] Veri Koruma Direktifi, Madde 2 (h).
[96] Örneğin, 108 Sayılı Sözleşme, İstatiksel Veri Tüzüğü, 6. Nokta.

Hukuki ehliyeti bulunmayan kişiler tarafından verilmiş geçersiz bir rıza, bu kişilere ait verilerin işlenmesi bakımından hukuki bir dayanağın bulunmaması sonucunu doğuracaktır.

Rıza sarih veya zımni bir şekilde verilmiş olabilir.[97] Sarih rıza veri öznesinin niyeti konusunda şüpheye yer bırakmaz ve sözlü veya yazılı olarak verilebilir; zımni rızanın varlığı ise durumdan çıkarılır. Rıza kesin bir şekilde verilmelidir.[98] Veri öznesinin, verilerinin işlenmesine izin verdiğine dair kabulünü ortaya koymak istediğine dair makul bir şüphe bulunmamalıdır. Örneğin, tek başına hareketsizlikten yola çıkarak var olduğu kabul edilen bir rıza, kesin şekilde verilmiş bir rıza sayılamayacaktır. İşlenecek verilerin hassas olduğu durumlarda rızanın sarih olması kanunen zorunludur ve rıza kesin olmalıdır.

Özgür iradeyle açıklanmış rıza

Özgür iradeyle açıklanmış rıza, "veri öznesinin hile, tehdit, zorlama veya rıza göstermemesi durumunda belirgin olumsuz sonuçlar doğurma riski altında olmadan gerçek bir seçim yapabilecek durumda olması" halinde geçerli sayılır.[99]

Örnek: Birçok havaalanında, yolcuların biniş alanlarına girebilmeleri için vücut taramasından geçmeleri gerekmektedir.[100] Bu tarama sırasında yolcuların verileri işlendiği için, işlemelerin VK Direktifi madde 7'de sayılan hukuki dayanaklardan birisine uygun olmaları gerekmektedir (Bkz. Bölüm 4.1.1). Bazı durumlarda, rızalarının işlemeyi haklı kılacağı ima edilerek vücut taraması yolculara bir seçenek olarak sunulmaktadır. Ancak, yolcuların büyük bir çoğunluğu vücut taramasından geçmeyi reddetmelerinin kendilerine şüphe ile bakılmasına veya üst araması gibi ek kontrollere sebep olacağından korkabilirler. Çoğu yolcu olası sorunların ve gecikmelerin önüne geçmek için vücut taramasına rıza göstermektedir.

Bu sebeple, tarama işlemine yönelik sağlam bir hukuki temel ancak yasa koyucunun bir düzenlemesi olan VK Direktifi madde 7(e)'de bulunabilecek ve bu üstün kamu yararı sebebiyle yolcuların işbirliği yapmasına yönelik bir yükümlülük meydana getirecektir. Söz konusu düzenleme kapsamında, vücut taraması ve üst araması arasında bir seçim sunmaya devam edilebilir ancak bu belirli koşullar altında gereken ek sınır kontrol önlemlerinin yalnızca bir parçası olabilir. Bu tür yasal düzenlemeler kişinin üzerini el ile arama ve tarama cihazı yardımı ile arama seçeneğini kapsayabilir. Avrupa Komisyonu'nun güvenlik tarayıcılarına yönelik olarak 2011 yılında çıkartılan iki tüzükte getirdiği düzenlemeler bunlardır.[101]

Özgür iradeyle açıklanan rıza, rızayı alan veri sorumlusu ile rızayı veren veri öznesi arasında ekonomik veya başka bir açıdan belirgin bir dengesizlik olması halinde ortaya çıkan bağımlılık/itaat durumlarında tehdit altına girebilir.[102]

---

[97] Veri Koruma Direktifi, Madde 8 (2).

[98] *A.e.,* Madde 7 (a) ve Madde 26 (1).

[99] Bakınız Madde 29 Çalışma Kurultayı (2011), *15/2011 Sayılı Rıza Kavramına ilişkin Öneri*, WP 187, Brüksel, 13 Temmuz 2011, s. 12.

[100] Bu örnek s.15'ten alınmıştır.

[101] 272/2009 Sayılı, *Sivil havacılık güvenliği konusunda AB havalimanlarında güvenlik tarayıcıların kullanılmasına ve ortak temel standartları'nın tamamlanmasına* ilişkin Tüzüğün değiştirilmesi üzerine, 10 Kasım 2011, OJ 2011 L 293, ve 1141/2011 Sayılı, 185/2010 Sayılı, *Sivil havacılık güvenliği konusunda AB havalimanlarında güvenlik tarayıcıların kullanılmasına dair uygulamaya* ilişkin Komisyon Tüzüğün değiştirilmesi üzerine, 11 Kasım 2011, OJ 2011 L 294.

[102] Bakınız Madde 29 Çalışma Kurultayı (2001), *8/2001 Sayılı, İstihdam alanında kişisel verilerin işlenmesine ilişkin Öneri,* WP 48, Brüksel, 13 Eylül 2001; ve Madde 29 Çalışma Kurultayı (2005), 95*/46/AB Sayılı Direktifin 26(1). maddesi'nin ortak anlayışına ilişkin Çalışma Metni, 24 Ekim 1995*, WP 114, Brüksel, 25 Kasım 2005.

Örnek: Büyük ölçekli bir şirket sırf kurum içi iletişimi geliştirmek adına bütün çalışanlarının isimlerini, şirketteki görevlerini ve iş adreslerini içeren bir rehber oluşturmayı planlamaktadır. Personel daire başkanı, örneğin toplantılarda çalışanların birbirlerini tanımalarını kolaylaştırmak için bu rehbere her bir çalışanın fotoğrafının da eklenmesini önerir. Çalışan temsilcileri bu eklemenin ancak ilgili çalışanın rızası olması durumunda yapılabilmesini talep ederler.

Böyle bir durumda, bir işçinin rızasının rehberdeki fotoğrafların işlenmesi için yasal dayanak oluşturacağı ifade edilebilir. Zira rehberde bir fotoğrafın yayınlanmasının kendi içerisinde olumsuz sonuçlarının olmadığı bellidir. Üstelik, çalışanın fotoğrafının rehberde yayınlanmasına rıza göstermemesi durumunda işveren tarafından kendisine yöneltilecek olumsuz etkilere maruz kalmayacağını düşünmek de akla yatkındır.

Bu açıklamalar, rıza gösterilmemesinin olumsuz sonuçlar doğurabileceği durumlarda verilen rızanın asla geçerli olamayacağı şeklinde anlaşılmamalıdır. Örneğin, bir süpermarketin müşteri kartını almaya rıza gösterilmemesi durumunda karşılaşılabilecek sonuç belirli bazı mallardaki indirimlerden yararlanamamak olacaksa, kartı almış olan müşterilerin gösterdikleri rıza bu müşterilerin kişisel verilerinin işlenmesi için geçerli bir yasal dayanak oluşturmaya devam edecektir. Süpermarket ve müşterisi arasında bir bağımlılık/itaat ilişkisi yoktur ve rıza göstermemenin sonuçları veri öznesinin rızasını özgür iradeyle açıklamasına engel olacak kadar ciddi değildir.

Diğer taraftan, yeterli derecede önemli mal ve hizmetlerin münhasıran bazı kişisel verilerin üçüncü kişilere ifşası yoluyla elde edilebildiği durumlarda, veri öznesinin verilerin ifşasına dair rızası özgür iradeyle açıklanmış rıza olarak değerlendirilemez ve bu sebeple verilerin korunması hukuku kapsamında geçerli değildir.

Örnek: Uçak yolcularının, yolcu isim kaydı (PNR) olarak da adlandırılan ve kimlikleri, yeme alışkanlıkları veya sağlık sorunları vb. verileri içeren kayıtlarının belirli bir yabancı ülkenin göç idaresine aktarılabileceğine dair havayolu şirketlerine verdikleri bir onay, yolcuların o ülkeyi ziyaret etmek istemeleri durumunda başka bir seçenekleri olmadığı için verilerin korunması hukuku bağlamında geçerli bir rıza sayılamaz. Bu tür verilerin aktarımının yasal bir şekilde yapılabilmesi için rızadan başka bir hukuki dayanağa, büyük ihtimalle özel bir kanuna, ihtiyaç olacaktır.

Bilgilendirilmeye dayalı rıza

Veri öznesi kararını vermeden önce yeterli bilgiye sahip olmalıdır. Yeterli bilginin verilip verilmediği hususu her olay bakımından ayrı ayrı değerlendirilmelidir. Yapılacak bilgilendirilme, genel olarak, rıza gerektiren konuya dair kesin ve kolayca anlaşılabilir bir tanım ve buna ek olarak rıza gösterilmesi veya gösterilmemesinin sonuçlarını genel hatlarıyla aktaran bir özetten oluşur. Bilgilendirmede kullanılacak dil bilgilendirmenin olası muhatapları göz önüne alarak oluşturulmalıdır.

Bilgilendirme aynı zamanda veri öznesinin kolayca ulaşabileceği şekilde olmalıdır. Bilgilendirmenin erişilebilirliği ve görünürlüğü önemli unsurlardır. Çevrimiçi ortamlardaki bilgilendirmelerin katmanlı bir şekilde yapılması, yani veri öznesi tarafından erişilebilir olan kapsamlı bilgilendirme metni dışında özet olarak hazırlanmış bir bilgilendirmenin de veri öznesine sunulması iyi bir çözüm olabilir.

Belirli bir konuya ilişkin rıza

Geçerli olabilmesi için rızanın belirli bir konuya ilişkin olması gerekir. Bu gereklilik, rızanın amacıyla alakalı olarak yapılan bilgilendirmenin kalitesiyle de yakından bağlantılıdır. Bu bağlamda, ortalama bir veri öznesinin makul beklentileri göz önünde bulundurulmalıdır. Yürütülen işleme faaliyetlerine yapılan ekleme ve değişikliklerin, bu faaliyetleri rızanın ilk alındığı zamanda öngörülemeyecek bir biçimde değiştirmiş olması durumunda veri öznesinin rızasının tekrar alınması gerekmektedir.

Örnek: **'Deutsche Telekom AG'**[103] davasında ABAD, Özel Hayatın Gizliliği ve Elektronik İletişim Direktifi'nin[104] 12. maddesi uyarınca abonelerine ait kişisel verileri aktarma yükümlülüğü altında bulunan bir telekomünikasyon hizmet sağlayıcısının, abonelerin rızalarını verdikleri tarihte veri alıcılarının belirli olmaması sebebiyle, veri öznelerinden alacağı yenilenmiş rızalara ihtiyacı olup olmadığı konusunu tartışmıştır.

ABAD söz konusu hüküm gereği verilerin aktarılmasından önce rızaların yenilenmesinin gerekmediğini, çünkü veri öznelerinin anılan düzenleme gereği yalnızca işlemenin amacına, yani verilerinin yayınlanmasına yönelik rıza göstermelerinin mümkün olduğunu, bu verilerin yayınlanacağı farklı dizinler arasından seçim yapma imkanlarının bulunmadığını belirtmiştir.

Mahkemenin de altını çizdiği üzere, " Özel Hayatın Gizliliği ve Elektronik İletişim Direktifi'nin 12. maddesinin bağlamsal ve sistematik bir yorumundan da anlaşılacağı gibi, 12(2) maddesi kapsamında rıza, herhangi bir dizin sağlayıcının kimliğine yönelik değil, kişisel verilerin kamuya açık bir dizinde yayınlanması amacına ilişkindir."[105] Bunun da ötesinde, "bir aboneye zarar verebilecek olan asıl şeyin, yayını yapanın kim olduğundan çok, o aboneye ait kişisel verilerin kamuya açık bir dizinde yayınlanması eyleminin kendisi olduğu ortaya çıkabilir".[106]

2.4.2. Rızayı her daim geri çekme hakkı

VK Direktifi genel bir her daim rızayı geri çekme hakkından bahsetmemektedir. Buna karşın böyle bir hakkın var olduğu ve veri öznesinin de bu haktan istediği zaman yararlanabileceği yaygın şekilde kabul edilmektedir. Rızanın geri çekilmesi için gerekçe gösterme zorunluluğu ve rızanın geri çekilmesi sebebiyle artık yararlanılamayacak olan avantajların kaybedilmesi dışında ve üzerinde herhangi bir olumsuz etki doğma riski bulunmamalıdır.

Örnek: Bir müşteri veri sorumlusuna verdiği mail adresine kampanya mailleri yollanmasını kabul eder. Müşteri mailleri almak istemediğini belirttiği anda, veri sorumlusu derhal mail gönderimlerine son vermelidir. Bunu yaparken de cezalandırıcı nitelikte, örneğin işlem bedeli vb. yaptırımlar uygulanmamalıdır.

Eğer müşteri kişisel verilerinin kampanya maili gönderimleri için kullanılmasına rıza gösterdiği için konaklama ücretlerinde 5% indirimden faydalanmaktaysa, kaydını sildirmeye karar verdiğinde daha önce faydalanmış olduğu indirimlerin geri ödenmesi talep edilemez.

3. Avrupa veri koruma hukukunun temel ilkeleri

[103] ABAD, C-543/09, *Deutsche Telekom AG v. Germany*, 5 Mayıs 2011; özellikle bakınız par. 53 ve 54.
[104] Avrupa Birliği Parlamentosu ve Konseyi, 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi, 12 Temmuz 2002, OJ 2002 L 201.
[105] ABAD, C-543/09, *Deutsche Telekom AG v. Germany*, 5 Mayıs 2011; par. 61.
[106] *A.e.*, par. 62

AB	İşlenen konular	AK
VK Direktifi, Madde 6 (1) (a) ve (b) ABAD, C-524/06, *Huber v. Germany*, 16 Aralık 2008 ABAD, Birlikte Görülen C-92/09 ve C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Kasım 2010	**Hukuka uygun işlenme ilkesi**	108 Sayılı Sözleşme, Madde 5 (a) ve (b) AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 AİHM, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 Ekim 2002 AİHM, *Peck v. the United Kingdom*, No. 44647/98, 28 Ocak 2003 AİHM, *Khelili v. Switzerland*, No. 16188/07, 18 Ekim 2011 AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987
VK Direktifi, Madde 6 (1) (b)	**İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi**	108 Sayılı Sözleşme, Madde 5 (b)
	Veri kalitesi ilkesi	
VK Direktifi, Madde 6 (1) (c)	**Verilerde gereklilik ilkesi**	108 Sayılı Sözleşme, Madde 5 (c)
VK Direktifi, Madde 6 (1) (d)	**Verilerde doğrululuk ilkesi**	108 Sayılı Sözleşme, Madde 5 (d)
VK Direktifi, Madde 6 (1) (e)	**Verilerin sınırlı muhafazası ilkesi**	108 Sayılı Sözleşme, Madde 5 (e)
VK Direktifi, Madde 6 (1) (e)	**Bilimsel ve istatiksel araştırmalar için istisnalar**	108 Sayılı Sözleşme, Madde 9 (3)
VK Direktifi, Madde 6 (1) (a)	**Adil işleme ilkesi**	108 Sayılı Sözleşme, Madde 5 (a) AİHM, *Haralambie v. Romania*, No. 21737/03, 27 Ekim 2009 AİHM, *K.H. and Others v.*

		Slovakia, No. 32881/04, 28 Nisan 2009
VK Direktifi, Madde 6 (2)	**Hesap verilebilirlik ilkesi**	

108 Sayılı Sözleşme madde 5'te yer verilen ilkeler Avrupa veri koruma mevzuatının özünü oluştururlar. VK Direktifi'nin 6. maddesinde de konuya ilişkin daha detaylı düzenlemeler öncesinde bir başlangıç noktası olarak yer alırlar. AK ve AB düzeyinde yapılacak bundan sonraki bütün veri koruma mevzuatının bu ilkelerle uyumlu olması ve bu yeni düzenlemeler yorumlanırken temel ilkelerin akıldan çıkarılmaması gerekmektedir. Bu ilkelere ulusal yasalar kapsamında istisnalar veya sınırlandırmalar getirilebilir;[107] ancak bu istisna ve sınırlandırmaların kanunlarda açıkça öngörülmeleri, meşru bir amaç için olmaları ve demokratik bir toplumda gerekli olmaları zorunludur. Bu üç şartın da yerine getirilmesi gerekmektedir.

3.1. Hukuka uygun işlenme ilkesi

Ana başlıklar

- Hukuka uygun işlenme ilkesini anlamak için verilerin korunması hakkına yönelik hukuka uygun sınırlamaların koşullarını ortaya koyan Şart madde 52(1)'ye ve haklı müdahalenin şartlarını düzenleyen AİHS madde 8(2)'ye bakmak gerekir.

- Kişisel verilerin işlenmesinin hukuka olabilmesi için aşağıdaki şartların gerçekleşmesi gerekmektedir:
  1. Kanuna uygun olmalı; ve
  2. Meşru bir amaç için yapılıyor olmalı; ve
  3. Meşru bir amaca ulaşmak için demokratik bir toplumda gerekli olmalıdır

AB ve AK mevzuatı uyarınca, hukuka uygun işlenme ilkesi sayılan ilk ilkedir; 108 Sayılı Sözleşmenin 5. maddesi ile VK Direktifi'nin 6. maddesinde neredeyse aynı ifadeler kullanılarak düzenlenmektedir.

Bu hükümlerin hiçbiri 'hukuka uygun işlenme'nin ne anlama geldiğine dair bir tanım içermemektedir. Bu yasal terimin anlaşılabilmesi için AİHM'nin AİHS'de yer alan haklı müdahale kavramına dair kararlarında yer verdiği yorumlara ve Şart'ın 52. maddesi kapsamında hukuka uygun sınırlandırmalara dair şartlara bakmak gerekmektedir.

3.1.1. AİHS kapsamında haklı müdahalenin şartları

Kişisel verilerin işlenmesi, veri öznesinin özel hayatın gizliliğine saygı gösterilmesi hakkına bir müdahale teşkil edebilir. Özel hayatın gizliliği hakkı mutlak bir hak değildir ve başka özel kişilerin (kişisel çıkarlar) veya bir bütün olarak toplumun menfaatleri (kamu yararı) gibi yasal menfaatlerle dengelenmelidir.

Devlet tarafından yapılacak müdahalenin haklı olabilmesi için aranan şartlar şu şekildedir:

[107] 108 Sayılı Sözleşme, Madde 9 (2); VK Direktifi, Madde13 (2).

Kanuna uygun olma

AİHM kararlarına göre, müdahale, belirli niteliklere sahip bir ulusal yasa hükmüne dayanması durumunda kanuna uygun sayılır. Bu kanunun "ilgili kişiler tarafından erişilebilir ve sonuçları bakımından öngörülebilir" olması gerekmektedir.[108] Bir hüküm, "herhangi bir bireyin davranışlarını -icabında uygun bir tavsiye ile- düzenlemesine yetecek kesinlikte oluşturulmuş olması durumunda" öngörülebilir olarak değerlendirilir.[109] Bu bağlamda 'kanundan' beklenen kesinlik derecesi somut olaya göre değişecektir.[110]

Örnek: **'Rotaru v. Romania'**[111] davasında AİHM, ulusal güvenliğe ilişkin bilgilerin toplanmasına, kaydedilmesine ve gizli dosyalarda arşivlenmesine imkân tanıyan Romanya mevzuatını, bu yetkilerin kullanım sınırlarına dair herhangi bir düzenleme içermemesi ve konuyu yetkililerin takdirine bırakması sebebiyle, AİHS'nin 8. maddesine aykırı bulmuştur. Örneğin, işlenebilecek verilerin hangileri olduğuna, gözetleme tedbirlerinin hangi kategorideki kişilere yönelik olarak yapılabileceğine, bu tedbirlerin veya prosedürlerin hangi durumlarda işletebileceğine dair ilgili ulusal mevzuatta herhangi bir hüküm yer almamaktadır. Mahkeme, bu eksiklikler sebebiyle ulusal düzenlemelerin AİHS'nin 8. maddesi kapsamında aranan öngörülebilirlik şartını yerine getirmediğine ve ilgili maddenin ihlal edildiğine karar vermiştir.

Örnek: **'Taylor-Sabori v. Birleşik Krallık'**[112] davasında başvuran polis tarafından takibe alınmıştır. Polis, başvurana ait çağrı cihazının bir 'kopyasını' kullanarak, başvurana gönderilen mesajları dinlemiştir. Sonrasında polis kontrole tabi bir ilacı tedarik amaçlı tertip suçlamasıyla başvuranı tutuklamıştır. Savcılığın iddialarının bir kısmı başvurana ait çağrı cihazına gelen mesajların polis tarafından eş zamanlı olarak alınan dökümlerine dayandırılmıştır. Ancak başvuranın davasının görüldüğü dönemde, özel bir telekomünikasyon sistemi üzerinden yapılan iletişimlerin dinlenmesine yönelik olarak İngiliz hukukunda bir düzenleme bulunmamaktadır. Bu sebeple de başvuranın haklarına yapılan müdahale "kanuna uygun olarak" yapılmamıştır. Mahkeme, AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

Meşru bir amaç için yapılma

Meşru amaç, kamu menfaatlerinden birisi veya diğer kişilerin hak ve özgürlükleri şeklinde tezahür edebilir.

Örnek: **'Peck v. Birleşik Krallık'**,[113] davasında başvuran, KDT kamerasının kendisini çektiğinden haberi olmaksızın bileklerini keserek intihar girişiminde bulunmuştur. KDT görüntülerini takip eden polisler başvuranı kurtardıktan sonra, emniyet teşkilatı KDT görüntülerini medyaya servis etmiş ve bu görüntüler de medya tarafından başvuranın yüzü gizlenmeden yayınlanmıştır. AİHM, görüntülerin ilgili kişinin yüzünün gizlenmeksizin veya ilgilinin rızası alınmaksızın kamu otoriteleri tarafından kamuya ifşa edilmesini haklı

[108] AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, par. 50; Bakınız AİHM, *Kopp v. Switzerland*, No. 23224/94, 25 Mart 1998, par. 55 ve AİHM, *Iordachi and Others v. Moldova*, No. 25198/02, 10 Şubat 2009, par. 50.

[109] AİHM, *Amann v. Switzerland* [GC], No. 27798/95, 16 Şubat 2000, par. 56; Bakınız AİHM, *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984, par. 66; AİHM, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983, par. 88.

[110] AİHM, *The Sunday Times v. the United Kingdom*, No. 6538/74, 26 Nisan 1979, par. 49; Bakınız AİHM, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Mart 1983, par. 88.

[111] AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 Mayıs 2000, par. 57; Bakınız AİHM, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, 28 Haziran 2007; AİHM, *Shimovolos v. Russia*, No. 30194/09, 21 Haziran 2011; ve AİHM, *Vetter v. France*, No. 59842/00, 31 Mayıs 2005.

[112] AİHM, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 Ekim 2002.

[113] AİHM, *Peck v. the United Kingdom*, No. 44647/98, 28 Ocak 2003, özellikle par. 85.

gösterebilecek bağlantılı veya yeterli bir gerekçe bulunmadığına karar vermiştir. Mahkeme AİHS'nin 8. maddesinin ihlal edildiği kanısına varmıştır.

Demokratik bir toplumda gerekli olma

AİHM, "gereklilik kavramı, müdahalenin toplumsal bir ihtiyacın oluşturduğu baskı sebebiyle yapıldığını ve bu bakımdan da meşru amaçla orantılı olduğunu ifade eder" demektedir.[114]

Örnek: **'Khelili v. Switzerland'**[115] davasında, polis tarafından gerçekleştirilen bir kontrol sırasında başvuranın üzerinden "Hoş, güzel kadın, 30'lu yaşlarda, beraber bir içki içmek veya ara sıra takılmak isteyen bir beyle tanışmak istiyor. Tel. no […]" şeklinde bir yazı içeren kartvizitler çıkmıştır. Başvuranın iddiasına göre, bu kartvizitlerin bulunmasını takiben polis başvuranın ismini kendi kayıtlarına, başvuran bu mesleği yaptığını ısrarla inkâr etmesine karşın, hayat kadını olarak girmiştir. Başvuran "hayat kadını" kelimesinin polisin bilgisayar kayıtlarından silinmesini talep etmiştir. AİHM bir bireyin kişisel verilerinin gelecekte yeniden suça karışabileceği gerekçesiyle saklanmasının bazı koşullar altında ölçülü olabileceğini ilkesel olarak kabul etmiştir. Ancak başvuranın durumunda, yasadışı hayat kadınlığı iddiası oldukça belirsiz ve genel olarak görünmektedir ve yasadışı hayat kadınlığından hiçbir zaman hüküm giymemiş olması sebebiyle de bu iddianın sağlam gerçeklere dayandığı söylenemez. Bu yüzden de söz konusu müdahalenin AİHS'nin 8. maddesi bağlamında 'baskı yapan toplumsal bir ihtiyaç' sebebiyle gerçekleştirildiği düşünülemez. Konuyu yetkililerin başvurana dair tutulan verilerin doğruluğunu ve başvuranın haklarına yönelik müdahalenin ciddiyetini kanıtlamaları açılarından ele alan Mahkeme, 'hayat kadını" ibaresinin uzun yıllar boyunca emniyet kayıtlarında saklanmasının demokratik bir toplumda gerekli olmadığına karar vermiştir. Mahkeme AİHS'nin 8. maddesinin ihlal edildiği kanısına varmıştır.

Örnek: **'Leander v. İsveç'**,[116] Mahkeme, ulusal güvenlik açısından önem taşıyan pozisyonlarda çalışmak üzere başvuruda bulunan kişiler hakkında gizli bir araştırma yürütülmesinin kendi başına demokratik bir toplumda gerekli olma şartına aykırı olmadığına karar vermiştir. Veri öznesinin çıkarlarının korunması için ulusal mevzuat kapsamında öngörülen özel güvencelerin -örneğin parlamento ve Adalet Bakanı tarafından yapılan denetimler- varlığı sebebiyle AİHM, İsveç personel kontrol sisteminin AİHS madde 8(2)'de öngörülen koşulları karşıladığına karar vermiştir. Aleyhine başvuruda bulunulan devletin kontrolü altında bulunan geniş değerlendirme imkanlarıyla alakalı olarak, devletin, başvuranla alakalı somut olay kapsamında ulusal güvenlik çıkarlarının başvuranın bireysel çıkarlarına üstün geldiği yönünde bir değerlendirmede bulunmaya yetkisi olduğu kabul edilmiştir. Bu durumda AİHM İsveç'te uygulanan gizli araştırmaların AİHS madde 8(2) uyarınca geçerli olduklarını belirtmiştir. Mahkeme, AİHS madde 8'in ihlal edilmediği kararına varmıştır.

3.1.2. AB Temel Haklar Şartı kapsamında hukuka uygun sınırlamaların şartları

Şart'ın yapısı ve lafzı AİHS'den farklıdır. Şart, güvence altına alınmış haklara yapılan müdahalelerden bahsetmemekte ama bu hakların kullanımına yönelik yapılabilecek sınırlandırılmalara dair bir hüküm içermektedir.

[114] AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987, par. 58.
[115] AİHM, *Khelili v. Switzerland*, No. 16188/07, 18 Ekim 2011.
[116] AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987, par. 59 ve 67.

Madde 52(1) gereğince, Şart kapsamında tanınan haklara ve özgürlüklere getirilen sınırlandırmalar ve buna uygun olarak verilerin korunması hakkına, örneğin kişisel verilerin işlenmesine getirilen sınırlandırmalar sadece aşağıdaki şartların varlığı halinde geçerli sayılırlar:

- kanunlarda açıkça öngörülmüşse; ve
- verilerin koruması hakkının özüne dokunmamaktaysa; ve
- gerekli ve orantılılık ilkesi ile uyumlu ise; ve
- AB tarafından tanınan kamu menfaati amaçlarına veya başkalarının hak ve özgürlüklerini koruma ihtiyacına yönelikse.

Örnek: **'Volker ve Markus Schecke'**[117] davasında AİHM, Avrupa Konseyi'nin ve Avrupa Komisyonu'nun orantılılık ilkesinin getirdiği sınırlamalar ile uyumlu davranmadığı kanaatına varmıştır. İlgili AB kurumları, tarımsal fonlardan yardım alan tüm gerçek kişilerin kişisel bilgilerini kişilerin yardımdan yararlandığı döneme, yararlanma sıklıklarına veya yararlanmanın doğasına ve miktarına dair herhangi bir elemeye gitmeksizin yayınlamaları sebebiyle orantılılık ilkesine aykırı hareket etmişlerdir.

Bu sebeple, ABAD 1290/2005 sayılı Konsey Tüzüğü'nün bazı hükümlerinin ve 259/2008 sayılı Tüzüğün tamamının hükümsüz olduğuna karar vermiştir.[118]

Şart 52(1)'de sunulmuş olan hukuka uygun işlenmenin şartları, farklı bir şekilde ifade edilmiş olsalar da AİHS 8(2)'yi anımsatmaktadır. Şart'ın 52(3) maddesinde belirtildiği üzere, Şart'ın 52(1) maddesinde sayılan koşulların AİHS'nin 8(2) maddesi ile uyumlu olması gerekmektedir: "Bu Şart'ın, İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi ile teminat altına alınmış olan haklara tekabül eden hakları içermesi durumunda söz konusu hakların anlamı ve kapsamı, söz konusu Sözleşme'de belirtilenlerle aynı olacaktır."

Ancak 52(3) maddesinin son cümlesi uyarınca, "bu hüküm, Birlik hukukunun daha kapsamlı koruma sağlamasını engellemez." AİHS madde 8(2) ve Şart madde 52(3)'ün ilk cümlesinin karşılaştırılması bağlamında ele alındığında bu cümleden, AİHS madde 8(2) uyarınca haklı müdahaleye dair öngörülen koşulların, Şart kapsamında verilerin korunması hakkına yönelik hukuka uygun sınırlamalar bakımından da asgari koşullar olduğu sonucunu çıkarabiliriz. Bunun bir sonucu olarak da AB hukuku kapsamında verilerin hukuka uygun şekilde işlenmeleri için AİHS madde 8(2) kapsamındaki asgari şartların yerine getirilmiş olması lazımdır. AB hukuku, belirli özel durumlarda ek şartlar öngörebilir.

AB hukuku kapsamındaki hukuka uygun olarak işlenme ilkesinin AİHS'nin ilgili hükümleri ile uyumlu olarak ele alınması hususu Avrupa Birliği Antlaşması'nın 6(3) maddesiyle de desteklenmektedir: 'AİHS tarafından güvence altına alınan temel hak ve özgürlükler Birlik hukukunun genel ilkelerini temsil etmektedir'.

[117] ABAD, Birlikte Görülen C-92/09 ve C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Kasım 2010, par. 89 ve 86.

[118] Ortak Tarım Politikası'nın Finansmanı Hakkında, 1290/2005 (AB) Sayılı Konsey Tüzüğü, 21 Haziran 2005, OJ 2005 L 209; ve Avrupa Birliği Tarımsal Garanti Fonu (EAGF) ve Avrupa Birliği Kırsal Kalkınma Tarım Fonundan (EAFRD) kaynaklanan fonlarından faydalanan kişilerin bilgileri'nin yayınlanmasına ilişkin 259/2008 (AB) Sayılı Konsey Tüzüğü, 18 Mart 2008, OJ 2008 L 76.

3.2. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi

Ana başlıklar

- Verilerin işlenmesinin amacı işleme başlamadan önce görünür bir şekilde tanımlanmalıdır.
- AB hukukunca, işlemenin amacı açıkça tanımlanmalıdır; AK mevzuatına göre bu mevzu ulusal hukuka bırakılmıştır.
- Verilerin belirsiz amaçlar için işlenmesi verilerin korunması mevzuatına aykırıdır.
- Yeni amaç ve eski (ilk) amacın birbiriyle uyumsuz olması durumunda, verilerin başka bir amaçla tekrar kullanılması için ek bir hukuki dayanak gereklidir.
- Verilerin üçüncü kişilere aktarılması ek bir hukuki dayanak gerektiren yeni bir amaçtır.

Amaç ile bağlantılı, sınırlı ve ölçülü olma ilkesi esas itibariyle kişisel verilerin işlenmesinin meşruiyetinin işlemenin amacına bağlı olacağı anlamına gelir.[119] İşlemenin amacı veri sorumlusu tarafından verilerin işlenmesine başlamadan önce belirlenmeli ve açıkça ilan edilmelidir.[120] AB mevzuatına göre bu bir beyan, başka bir deyişle ilgili denetim makamına yapılacak bir bildirim veya bu denetim makamının teftişine ve veri öznesinin erişimine açık olarak veri sorumlusu tarafından iç tarafta düzenlenecek bir belge yoluyla yapılmalıdır.

Kişisel verilerin belirsiz ve/veya sınırsız amaçlar için işlenmesi hukuka aykırıdır.

Verilerin işlenmesine yönelik her yeni amacın kendisine ait bir hukuki dayanağı bulunmalıdır; verilerin başka bir yasal amaç kapsamında daha önceden toplanmış veya işlenmiş olmasına dayanılamaz. Yani hukuka uygun işleme, başlangıçta belirlenmiş amaç ile sınırlıdır, verilerin yeni bir amaçla işlenmesi için yeni bir hukuki dayanak gerekmektedir. Verilerin üçüncü kişilere ifşasının da daha dikkatli bir değerlendirmeye tabi tutulması gerekecektir çünkü verilerin ifşası genellikle yeni bir amaca yönelik olacak ve verilerin toplanmasında kullanılan yasal dayanaktan ayrı bir hukuki dayanak gerektirecektir.

Örnek: Bir havayolu şirketi uçuşun düzgün bir şekilde gerçekleştirilebilmesi amacıyla gerekli rezervasyonları yapmak için müşterilerinin verilerini toplamaktadır. Havayolu şirketinin yolcuların koltuk numaraları; tekerlekli sandalye ihtiyacı gibi özel fiziksel sınırlamaları ve Yahudi veya Müslüman inancına uygun yemek vs. gibi özel yemek tercihleri hakkında verilere ihtiyacı olacaktır. PNR içerisinde yer alan bu verilerin varış ülkesinin göç idaresi tarafından havayolundan talep edilmesi durumunda bu veriler sonraki aşamada göç kontrolü amacıyla, yani verilerin toplanması aşamasındaki ilk amaçtan farklı bir amaç için kullanılacaktır. Dolayısıyla da bu verilerin bir göç idaresine aktarılması için yeni ve ayrı bir hukuki dayanak gerekecektir.

Belirli amacın kapsamını ve sınırlarını tanımlarken 108 Sayılı Sözleşme ve VK Direktifi uygunluk kavramına başvurmaktadır: verilerin uygun amaçlar için kullanılmaları başlangıçtaki yasal dayanak temelinde mümkündür. 'Uygun'dan kastın tam olarak ne olduğu ise belirlenmemiş olup, her somut olay bakımından yoruma açık bırakılmıştır.

[119] 108 Sayılı Sözleşme, Madde5 (b); VK Direktifi, Madde6 (1) (b).

[120] Bakınız Madde29 Çalışma Kurultayı (2013), *03/2013 Sayılı, Amaç Kısıtlandırmalarına ilişkin Öneri*, WP 203, Brüksel, 2 Nisan 2013.

Örnek: Sunshine şirketinin müşterilerine ilişkin olarak CRM sürecinde toplamış olduğu verilerin, bu verileri üçüncü şirketlerin pazarlama kampanyalarında kullanmak isteyen bir doğrudan pazarlama şirketi olan Moonlight'a satılması Sunshine şirketinin başlangıçtaki CRM amaçlarıyla uygun olmayan yeni bir amaç teşkil eder. Bu sebeple verilerin Moonlight şirketine satılması için yeni bir hukuki dayanağa ihtiyaç bulunmaktadır.

Buna karşın, Sunshine şirketinin CRM verilerini kendi pazarlama faaliyetlerinde kullanması, yani kendi ürünleri için kendi müşterilerine pazarlama mesajları göndermesi genellikle uygun bir amaç olarak kabul edilir.

VK Direktifi açıkça "verilerin tarihsel, istatiksel veya bilimsel amaçlar için yeniden kullanılması, üye devletlerin uygun güvenceleri öngörmüş olmaları halinde uygun olmayan bir amaç olarak değerlendirilemez" demektedir.[121]

Örnek: Sunshine şirketi müşterileri hakkındaki CRM (Müşteri İlişkileri Yönetimi) verilerini toplamış ve saklamıştır. Bu verilerin Sunshine şirketi tarafından müşterilerinin alışveriş alışkanlıklarına dair istatiksel bir analiz için kullanılması, istatistiksel amaçlar uygun amaçlar olarak değerlendirildiklerinden mümkündür. Veri öznesinin rızası gibi ek hukuki dayanaklara ihtiyaç yoktur.

Aynı verilerin münhasıran istatiksel amaçlar için üçüncü bir kişi konumundaki Starlight şirketine aktarılacak olması durumunda ise, istatistiksel amaçlar kapsamında kimlik bilgilerine genellikle ihtiyaç olmadığından veri öznelerinin kimliklerinin gizlenmesi vb. uygun görülen önlemlerin alınmış olması koşuluyla herhangi ek bir hukuki dayanak olmaksızın bu aktarım mümkün olabilecektir.

3.3. Veri kalitesi ilkeleri

Ana başlıklar

- Veri kalitesi ilkeleri veri sorumlusu tarafından işleme faaliyetlerinin her aşamasında uygulanmalıdır.
- Verilerin sınırlı olarak muhafaza edilmesi ilkesi gereği, verilere toplandıkları amaç kapsamında ihtiyaç kalmaması durumunda silinmeleri gerekmektedir.
- Verilerin sınırlı olarak muhafaza edilmesi ilkesine getirilecek istisnalar kanunla düzenlenmeli ve veri öznelerinin korunmasına yönelik özel tedbirler içermelidir.

3.3.1 Verilerde gereklilik ilkesi

Sadece "amaç için uygun ve gerekli olan ve toplanma ve/veya işlenmelerine sebep olan amaca göre ölçüsüz olmayan veriler" işlenmelidir. İşlenmesi için seçilen verilerin kategorileri işleme faaliyetlerinin ilan edilen genel amacına erişmek için gerekli olmalıdır ve bir veri sorumlusu, verilerin toplanması aşamasında toplanan bilgileri işleme için belirlenen özel amaç için doğrudan gerekli olacak biçimde sınırlamalıdır.[122]

[121] Örnek olarak Avusturya Veri Koruma Kanununa (*Datenschutzgesetz*) bakınız, Federal Law Gazette No. 165/1999, par. 46, İngilizce olarak mevcut: www.dsk.gv.at/DocView. axd?CobId=41936.

[122] 108 Sayılı Sözleşme, Madde5 (c); ve VK Direktifi, Madde6 (1) (c).

Modern toplumlarda, verilerde gereklilik ilkesinin bir yönü daha bulunmaktadır: özel hayatın gizliliğini korumak amacı ile geliştirilmiş yeni teknolojiler sayesinde bazı durumlarda kişisel verilerin tamamen kullanım dışı bırakılması veya yine gizliliğe yarayacak bir çözüm olarak takma isimle değiştirilebilmesi mümkündür. Bu özellikle de geniş çaplı işleme sistemleri için yerinde bir çözümdür.

Örnek: Bir belediye meclisi şehrin toplu ulaşım sistemini düzenli olarak kullanan vatandaşlarına yönelik olarak çipli bir kart sunmaktadır. Kart sahibinin ismi yazılı olarak kartın üzerinde ve elektronik olarak da çipin içerisinde bulunmaktadır. Otobüs ve tramvay kullanımında bu kartın okuyucu cihazların önünden geçirilmesi gerekmektedir. Cihaz tarafından okunan veri, seyahat kartını satan alan kişilerin isimlerinin kayıtlı olduğu bir veritabanında elektronik olarak kontrol edilmektedir.

Bu sistem verilerde gereklilik ilkesine tam anlamıyla uymamaktadır: Bir bireyin ulaşım sistemini kullanmaya yetkili olup olmadığı çipteki kişisel veriler bir veri tabanı ile karşılaştırılmadan da tespit edilebilir. Örneğin çipe yerleştirilecek barkod gibi özel bir elektronik görüntü sayesinde de okuyucu cihazın kartın geçerliliğini doğrulaması mümkün olabilir. Böyle bir sistem hangi kişinin hangi toplu taşıma aracını hangi zamanda kullandığına dair bir kayıt da tutmayacaktır. Bu sayede hiçbir kişisel veri toplanmamış ve veri toplanmasının asgari seviyeye indirilmesi yükümlülüğü getiren gereklilik ilkesi açısından en uygun çözüm elde edilmiş olacaktır.

3.3.2. Tamlık ve Doğruluk ilkesi

Kişisel verileri saklayan bir veri sorumlusu, elindeki verilerin tam ve doğru olduğundan makul bir kesinlikle emin olmasını sağlayacak adımları atmaksızın o verileri kullanamayacaktır.

Verilerin doğruluğunun sağlanması yükümlülüğü verilerin işlenmesinin amacı bağlamında değerlendirilmelidir.

Örnek: Mobilya satan bir şirket müşterilerinin kimliklerini ve adreslerini daha sonra ilgili kişilere fatura kesmek amacı ile toplamıştır. 6 ay sonra aynı şirket bir pazarlama kampanyası başlatmayı ve eski müşterileri ile irtibata geçmeyi ister. Bu müşterilere ulaşabilmek için de şirket, ulusal adres siciline erişmek ister. Bu sicil yüksek ihtimalle müşterilerin güncel adres bilgilerini içerecektir çünkü ülkede ikamet eden kişilerin mevcut adreslerini yasa uyarınca bu sicile bildirme zorunluluğu bulunmaktadır. Bu sicilde yer alan verilere erişim ise bu erişim için haklı bir sebep gösterebilecek kişi ve kurumlarla sınırlıdır.

Bu durumda şirket, elindeki verilerin doğru ve güncel olması gerektiğinden yola çıkarak nüfus sicilinden eski müşterilerinin yeni adres verilerini toplamaya yetkili olduğunu iddia edemez. İlgili veriler faturalandırma sırasında toplanmıştır ve bu amaç kapsamında, yalnızca satış sırasındaki verilerin gerekli olduğundan bahsedilebilir. Pazarlama menfaatleri kişisel verilerin korunması hakkına üstün gelen menfaatler olmadığından ve sicildeki verilere erişimi haklı kılmayacağından, yeni adres bilgilerini toplamak için yasal bir dayanak bulunmamaktadır.

Bazen saklanan verilerin güncellenmesi de hukuken yasaklanmış olabilir çünkü verilerin saklanmasındaki esas amaç olayların belgelendirilmesidir.

Örnek: Bir ameliyat tutanağının, tutanaktaki bulguların hatalı olduğu sonradan anlaşılmış olsa bile değiştirilmesi, yani 'güncellenmesi' yasaktır. Yani bu demektir ki, bu tutanak yanlış tutulmuş olsa dahi veriler değiştirilemez. Böyle durumlarda yalnızca tutanaktaki görüşlere dair ek yorumların eklenmesi söz konusu olabilir. Bu eklemelerin de daha sonraki bir aşamada yapılan katkılar oldukları açıkça belirtilmelidir.

Diğer yandan, verilerin güncellenmesi de dahil olmak üzere doğruluğunun düzenli olarak kontrol edilmesinin, verilerin doğru tutulmaması halinde veri öznesine verebileceği olası zarar sebebiyle mutlak bir gereklilik olduğu durumlar da oluşabilir.

Örnek: Bir kişinin bir bankacılık kurumuyla sözleşme imzalamak istemesi durumunda ilgili banka genellikle müstakbel müşterisinin kredi notunu/geçmişini kontrol eder. Bu amaçla kurulmuş ve gerçek kişilerin kredi geçmişlerini içeren özel veri tabanları bulunmaktadır. Böyle bir veri tabanının birey hakkında yanlış veya tarihi geçmiş bilgiler içermesi durumunda veri öznesi ciddi sorunlarla karşı karşıya kalabilir. Dolayısıyla bu veri tabanlarının sorumlularının verilerin tamlık ve doğruluğu ilkesini yerine getirmek için özel bir çaba sarf etmesi gerekmektedir.

Gerçeklerden ziyade şüphelere, örneğin ceza soruşturmalarına dayanan veriler de veri sorumlusu bu bilgileri toplamak için bir yasal dayanağa sahip olduğu ve veri sorumlusunun böyle bir şüpheye sahip olmasını yeterli ölçüde haklı gösterdiği müddetçe toplanabilir ve saklanabilirler.

3.3.3. Verilerin sınırlı muhafazası ilkesi

VK Direktifi madde 6(1)(e) ve 108 Sayılı Sözleşme madde 5(e), kişisel verilerin "toplanma ve işlenme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde veri öznelerin kimliklerini belirlemeye imkân veren bir biçimde" saklanmaları gerektiğini belirtir. Bu sebeple veriler amaç gerçekleştirildikten sonra silinmelidir.

'S. ve Marper' davasında AİHM, AK'nin ilgili düzenlemelerinde yer alan temel ilkeler ve Sözleşmeye Taraf Devletlerin mevzuat ve uygulaması gereği, verilerin toplanması amacıyla ve süreyle sınırlı muhafaza edilmesiyle alakalı olarak verilerin saklanmasının, özellikle de kolluk faaliyetleri bakımından ölçülü olması gerektiğini ifade etmiştir.[123]

Kişisel verilerin sınırlı süreyle muhafazası ancak kişilerin kimliklerini belirlemeye imkân veren biçimlerde saklanan veriler bakımından uygulanır. Artık ihtiyaç kalmayan verilerin hukuka uygun bir şekilde saklanması da verilerin anonimleştirilmesi veya takma isim ile değiştirilmesi yoluyla mümkün olabilir.

Verilerin bilimsel, tarihsel veya istatiksel amaçlar için saklanması VK Direktifi kapsamında açıkça verilerin sınırlı muhafaza ilkesinin uygulama alanı dışında bırakılmıştır.[124] Ancak bu amaçlar için verilerin saklandığı durumlarda ulusal hukuk çerçevesinde özel güvenceler sağlanmalıdır.

3.4. Adil işleme ilkesi

[123] AİHM, *S. and Marper v. the United Kingdom*, Nos. 30562/04 ve 30566/04, 4 Aralık 2008; ayrıca bakınız: AİHM, *M.M. v. the United Kingdom*, No. 24029/07, 13 Kasım 2012.
[124] VK Direktifi, Madde6 (1) (e).

Ana başlıklar

- Adil işleme ilkesi, işleme sürecinin özellikle de veri öznelerine yönelik olarak şeffaf olması anlamına gelmektedir.
- Veri sorumluları, veri öznelerini işleme öncesinde bilgilendirmeli ve en azından işlemenin amacı ve veri sorumlusunun kimliği ve adresi hakkında bilgi vermelidir.
- Kanunlar tarafından özel olarak izin verilmedikçe kişisel verilerin gizli veya üstü örtülü bir biçimde işlenmesi mümkün değildir.
- Veri özneleri verilerine, her nerede işleniyor olurlarsa olsunlar erişim hakkına sahiptirler.

Adil işleme ilkesi öncelikle veri sorumlusu ve veri öznesi arasındaki ilişkiyi düzenlemektedir.

3.4.1. Şeffaflık

Bu ilke gereğince veri sorumlusu veri öznelerini verilerinin ne şekilde kullanıldığına dair sürekli olarak bilgilendirmek ile mükelleftir.

Örnek: **'Haralambie v. Romanya'**[125] davasında, başvuran, istihbarat teşkilatının kendisi hakkında oluşturduğu dosyaya erişim talep etmiştir. Bu bilgiler ancak 5 yıl sonra kendisine verilmiştir. AİHM, devlet yetkilileri tarafında haklarında dosyalar tutulan kişilerin bu dosyalara erişim imkanına sahip olmalarında hayati bir çıkarları olduğunu vurgulamıştır. Devlet yetkilileri bu bilgilere erişimi sağlamak adına etkili bir prosedür sağlamakla yükümlüdürler. AİHM, aktarılan dosyaların miktarı veya arşiv sistemindeki yetersizlikler de dahil hiçbir sebebin başvuranın dosyasına erişiminin beş yıl geciktirilmesini haklı gösteremeyeceğine hükmetmiştir. Yetkililer başvuranın kişisel dosyalarına makul bir süre içerisinde erişimini sağlayacak olan etkili ve erişilebilir bir prosedürü sağlama konusunda başarısız olmuşlardır. AİHM, AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

İşleme prosedürleri, veri öznelerine, kolayca ulaşılabilecekleri ve verilerine ne olacağını anlamalarını sağlayacak bir şekilde açıklanmalıdır. Ayrıca veri öznelerinin verilerinin işlenip işlenmediğine, işleniyorsa bu verilerin hangileri olduğuna dair veri sorumlusundan bilgi alma hakları bulunmaktadır.

3.4.2. Güven oluşturulması

Veri sorumluları, verileri hukuka uygun ve şeffaf olarak işleyeceklerini veri öznelerine ve kamuoyuna kanıtlamalıdırlar. İşleme faaliyetleri gizli bir şekilde yürütülmemeli ve öngörülemeyen olumsuz etkileri bulunmamalıdır. Veri sorumluları, müşterilerin, iş sahiplerinin veya vatandaşların verilerinin kullanımına dair bilgilendirildiklerinden emin olmalıdır. Ayrıca veri sorumluları, veri öznelerinin taleplerini, özellikle de veri işlemesinin yasal dayanağını veri öznesinin rızasının oluşturduğu durumlarda, mümkün olduğunca gecikmeksizin karşılamalıdırlar.

Örnek: **'K.H. ve ötekiler v. Slovakya'**[126] davasında başvuranlar hamileliklerinden doğumlarına kadar olan süreçte doğu Slovakya'daki iki hastanede bakılan Roman kökenli 8 kadından oluşmaktadır. Sonrasında başvuranlardan hiçbirisi, defalarca denemelerine rağmen bir daha hamile kalamamışlardır. Ulusal mahkemeler ilgili hastanelerin, tıbbi kayıtlara bakıp

[125] AİHM, *Haralambie v. Romania*, No. 21737/03, 27 Ekim 2009.
[126] AİHM, *K.H. and Others v. Slovakia*, No. 32881/04, 28 Nisan 2009.

yazılı notlar almaları için başvuranlara ve temsilcilerine izin vermelerini emretmiş ancak söz konusu kayıtların fotokopilerinin çekilmesine izin verilmesi yönündeki talepleri, kötüye kullanımları önleyeceği iddiasıyla reddetmişlerdir. Veri öznelerinin kişisel verilerinin bir kopyalarının veri öznesinin erişebileceği bir halde bulundurulması, Devletlerin AİHS'nin 8. maddesi kapsamındaki pozitif yükümlülüklerinden birisidir. Kişisel verilerin kopyalanması için gerekli ayarlamaların belirlenmesi veya kopyalama talebinin reddinin gerekli görüldüğü durumlarda bu karara ilişkin ikna edici gerekçelerin sunulması Devletin görevidir. Başvuranların davasında, ulusal mahkemeler tıbbi kayıtların kopyalanması yönündeki taleplerin reddedilmesinin temel gerekçesi olarak söz konusu bilgilerin kötüye kullanımlarının önlenmesini ileri sürmüşlerdir. Ancak AİHM, tıbbi kayıtların tamamına erişim tanınması durumunda başvuranların nasıl olup da kendilerine ilişkin bu bilgileri kötüye kullanabileceklerini anlayamamıştır. Bunun da ötesinde, böylesi bir kötüye kullanım riski, verilerin kopyasını alma taleplerinin reddedilmesi dışındaki bazı yollarla, örneğin dosyalara erişim yetkisine sahip kişilerin sınırlandırılması gibi yöntemlerle de önlenebilirdi. Devlet, başvuranların sağlık durumlarına ilişkin bilgilere erişim taleplerinin reddedilmesini haklı gösterecek ikna edici gerekçelerin varlığını ortaya koyamamıştır. AİHM, AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

İnternet hizmetleriyle alakalı olarak, veri işleme sistemlerinin özellikleri, veri öznelerinin verilerine neler olduğunu gerçek bir biçimde anlamalarını mümkün kılmalıdır.

Adil işleme, aynı zamanda, veri öznelerinin meşru çıkarlarının gerektirmesi durumunda, veri sorumlularının öngörülen asgari yasal zorunlulukların da ötesine geçmeye hazır oldukları anlamına gelir.

3.5. Hesap verilebilirlik ilkesi

Ana başlıklar

- Hesap verilebilirlik ilkesi, işleme faaliyetleri sırasında verilerin korunması için veri sorumluları tarafından aktif olarak uygulanacak önlemleri gerektirir.
- Veri sorumluları yürüttükleri işleme faaliyetlerinin veri koruma hukukuna uygunluğunu gözetmekle yükümlüdürler.
- Veri sorumluları, herhangi bir zamanda, veri öznelerine, kamuoyuna ve denetim makamlarına, veri koruma yasalarına uygun hareket ettiklerini kanıtlayabilmelidir.

İktisadi Kalkınma ve İşbirliği Örgütü (OECD) 2013 tarihinde benimsemiş olduğu gizlilik ilkelerinde, verilerin korunmasının uygulamada işe yarayabilmesi açısından veri sorumlularının önemli bir role sahip olduğunu vurgulamıştır. İlgili ilkeler kapsamında bir hesap verilebilirlik ilkesi geliştirilmekte ve şöyle denmektedir: "Bir veri sorumlusu yukarıda belirtilen ilkelerin gerçekleşmesini sağlayan tedbirlere uyum bakımından hesap verebilir olmalıdır."[127]

108 Sayılı Sözleşme veri sorumlularının hesap verebilirliğine değinmez ve konuyu ulusal hukuka bırakırken, VK Direktifi madde 6(2) verilerin kalitesine dair 1. paragrafta belirtilmiş olan ilkelere uyumun veri sorumlusu tarafından sağlanması gerektiğini öngörmüştür.

[127] Ekonomik İş Birliği ve Kalkınma Örgütü (2013), *Kişisel verilerin korunması ve sınır ötesi akışlarının yönetilmesine ilişkin esaslar*, Madde14.

Örnek: Hesap verilebilirlik ilkesini vurgulayan önemli bir yasama örneği 2002/58 sayılı Özel Hayatın Korunması ve Elektronik İletişim Direktifi'ne 2009 yılında yapılan değişikliklerdir.[128] Değiştirilmiş 4. madde uyarınca, Direktif bir güvenlik politikasının uygulanması yükümlülüğü getirmektedir; maddede geçtiği haliyle "kişisel verilerin işlenmesiyle alakalı bir güvenlik politikasının uygulanmasının sağlanması". Yani, direktifin içinde bulunan güvenlik hükümleri kapsamında kanun koyucu, bir güvenlik politikasına sahip olunması ve bunun uygulanması gerektiği yönünde açık bir şarta yer vermenin gerekli olduğuna karar vermiştir.

Madde 29 Çalışma Kurultayın'ıngörüşüne göre,[129] hesap verilebilirliğin özü veri sorumlusunun aşağıdaki yükümlülüklerinden oluşmaktadır:

- işleme faaliyetleriyle alakalı olarak verilerin korunmasına dair kurallara uygun davranılmasını -normal koşullar altında- temin edecek tedbirleri almak; ve

- verilerin korunmasına dair kurallara uyum adına hangi tedbirlerin alındığını veri öznelerine ve denetim makamlarına kanıtlayacak belgeleri hazır bulundurmak.

Bu bağlamda hesap verilebilirlik ilkesi veri öznelerinin veya denetim makamlarının eksiklikleri göstermesi için beklemekten ziyade veri sorumlularının mevzuata uyduklarını aktif olarak göstermelerini gerektirmektedir.

4. Avrupa veri koruma hukukunun kuralları

AB	İşlenen konular	AK
Hassas olmayan verilerin hukuka uygun olarak işlenmesine dair kurallar		
Veri Koruma Direktifi, Madde 7 (a)	**Rıza**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (b) ve 3.6

[128] 2002/22/AB Sayılı, Elektronik haberleşme şebekeleri ve hizmetleri ile ilgili evrensel hizmet ve kullanıcı hakları Direktifi'nin değiştirilmesine ilişkin, Avrupa Birliği Parlamentosu ve Konseyi, 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ve 2006/2004 Sayılı Tüketici koruma kanunlarının uygulanmasından sorumlu ulusal makamlar arasındaki işbirliği Tüzüğü, 2009/136/AB Sayılı Avrupa Birliği Parlamentosu ve Konseyi Direktifi, 25 Kasım 2009, OJ 2009 L 337, s. 11.

[129] Madde 29 Çalışma Kurultayı, *3/2010 Sayılı, Hesap Verilebilirlik İlkesine ilişkin Öneri,* WP 173, Brüksel, 13 Temmuz 2010.

Veri Koruma Direktifi, Madde 7 (b)	**Sözleşmeye dayalı ve sözleşme öncesi ilişki**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (b)
Veri Koruma Direktifi, Madde 7 (c)	**Veri sorumlusunun hukuki yükümlülükleri**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (a)
Veri Koruma Direktifi, Madde 7 (d)	**Veri öznesinin hayati çıkarları**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (b)
Veri Koruma Direktifi, Madde 7 (e) ABAD, C-524/06, *Huber v. Germany*, 16 Aralık 2008	**Kamu menfaati ve resmi yetkinin kullanılması**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (b)
Veri Koruma Direktifi, Madde 7 Madde 8 (2) ve 8 (3) ABAD, Birleştirilmiş davalar C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011	**Başkalarının meşru menfaatleri**	Profil Oluşturma Tavsiye Kararı, Madde 3.4 (b)
Özel nitelikli (hassas) kişisel verilerin hukuka uygun olarak işlenmesine dair kurallar		
Veri Koruma Direktifi, Madde 8 (1)	**Genel işleme yasağı**	108 Sayılı Sözleşme , Madde 6
Veri Koruma Direktifi, Madde 8 (2)–(4)	**Genel işleme yasağına getirilen istisnalar**	108 Sayılı Sözleşme , Madde 6
Veri Koruma Direktifi, Madde 8 (5)	**(Cezai) Mahkumiyetler ile ilgili verilerin işlenmesi**	108 Sayılı Sözleşme , Madde 6
Veri Koruma Direktifi, Madde 8 (7)	**Kimlik numaralarının işlenmesi**	
Güvenli işlemeye dair kurallar		
Veri Koruma Direktifi, Madde 17	**Güvenli işleme sağlama yükümlülüğü**	108 Sayılı Sözleşme , Madde 7 AİHM, *I. v. Finland*, No. 20511/03, 17 Temmuz 2008
Özel Hayatın Korunması ve Elektronik İletişim Direktifi,	**Veri ihlali bildirimleri**	

Madde 4 (2)		
Veri Koruma Direktifi, Madde 16	**Gizlilik yükümlülüğü**	
Verilerin işlenmesinde şeffaflığa dair kurallar		
	Şeffaflık	108 Sayılı Sözleşme , Madde 8 (a)
Veri Koruma Direktifi, Madde 10 ve 11	**Bilgilendirme**	108 Sayılı Sözleşme , Madde 8 (a)
Veri Koruma Direktifi, Madde 10 ve 11	**Bilgilendirme yükümlülüğüne getirilen istisnalar**	108 Sayılı Sözleşme , Madde 9
Veri Koruma Direktifi, Madde 18 ve 19	**Bildirim**	Profil Oluşturma Tavsiye Kararı, Madde 9.2 (a)
Uyuma teşvik kuralları		
Veri Koruma Direktifi, Madde 20	**Ön kontrol**	
Veri Koruma Direktifi, Madde 18 (2)	**Kişisel veriler koruma yetkilileri**	Profil Oluşturma Tavsiye Kararı, Madde 8.3
Veri Koruma Direktifi, Madde 27	**Davranış kuralları**	

İlkeler ister istemez genel niteliklidirler. Somut olaylara uygulanmaları sırasında belirli bir yorum payı ve mevcut yollar arasından seçim imkânı bulunur. AK mevzuatına göre, bu yorum payını ulusal mevzuatları düzeyinde açıklığa kavuşturmak 108 Sayılı Sözleşme'nin Taraflarına bırakılmıştır. AB hukukunda ise durum farklıdır: Verilerin korunması hususunda gereken düzenin iç pazarda kurulması için ulusal mevzuatlardaki veri koruması seviyelerini uyumlu hale getirecek detaylı kuralların AB düzeyinde oluşturulması gerekli görülmüştür. VK Direktifi, 6. maddesinde yer verilen ilkeler kapsamında, ulusal hukuk düzenlerinde tam olarak uygulanması gereken bir detaylı kurallar bütünü öngörmüştür. Bu sebeple, Avrupa düzeyinde veri korumasıyla alakalı detaylı kurallara dair aşağıdaki yorumlar ağırlıklı olarak AB mevzuatına yöneliktir.

4.1. Hukuka uygun işlemeye dair kurallar

Ana başlıklar

*Kişisel verilerin hukuka uygun olarak işlenmesi bu şartlar altında mümkündür:

*İşleme veri öznesinin rızasına dayanıyorsa; veya

*Veri öznelerinin hayati menfaatleri verilerinin işlenmesini gerektiriyorsa; veya

*İşleme, veri öznelerinin temel haklarının korunmasına dair menfaatler izin verdiği ölçüde, başkalarının meşru çıkarlarından kaynaklanıyorsa.

*Özel nitelikli kişisel verilerin hukuka uygun olarak işlenmesi daha özel ve katı bir rejime tabidir.

VK Direktifi verilerin hukuka uygun olarak işlenmesine dair iki farklı kural dizisinden bahsetmektedir: Biri hassas olmayan verileri kapsayan işlemelere dair madde 7, diğeri hassas verileri kapsayan işlemlere dair madde 8.

4.1.1. Hassas olmayan verilerin hukuka uygun olarak işlenmesi

VK Direktifi'nin 'Kişisel verilerin işlenmesinin hukuka uygunluğuna dair genel kurallar' başlıklı ikinci bölümü, 13. madde kapsamında sayılan istisnalar saklı kalmak kaydıyla, kişisel veriler üzerinde yapılacak her türlü işlemenin öncelikle verilerin kalitesine dair Direktif'in 6. maddesinde sayılan ilkelere ve ikincil olarak verilerin işlenmesini meşru hale getirecek 7. maddedeki kriterlerden birisine uygun olması gerektiğini öngörmektedir.[130] Bu hassas olmayan verilerin işlenmesini hukuka uygun hale getiren durumları açıklamaktadır.

Rıza

AK mevzuatı uyarınca, rıza unsuru 108 Sayılı Sözleşme'de veya VK Direktifi'nde yer almamaktadır. Ancak, AİHM içtihatlarında ve çeşitli AK tavsiye kararlarında bu unsura değinilmiştir. AB mevzuatı kapsamında, verilerin hukuka uygun olarak işlenmesine dair bir dayanak olarak rıza, VK Direktifi madde 7(a)'da somut bir şekilde düzenlenmekte ve Şart'ın 8. maddesinde rıza unsuruna açıkça değinilmektedir.

Sözleşmeye dayalı ilişki

AB mevzuatı kapsamında verilerin hukuka uygun olarak işlenmesine dair başka bir dayanak VK Direktifi'nin 7(b) maddesinde yer alan "veri öznesinin taraf olduğu bir sözleşmenin ifası için gerekli olma" halidir. Bu madde ayrıca sözleşme öncesi ilişkileri de kapsamaktadır. Örneğin, taraflardan biri bir sözleşme akdetmek istemektedir ancak kontrol etmesi gereken bazı şeyler olduğundan henüz akdetmemiştir. Eğer taraflardan birisinin bu amaçla verileri işlemesi

[130] ABAD, Birlikte Görülen C-465/00, C-138/01 ve C-139/01. *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*, 20 Mayıs 2003, par. 65; ABAD, C-524/06, *Huber v. Germany,* 16 Aralık 2008, par. 48; ABAD, Birlikte Görülen C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011, par. 26.

gerekiyorsa, "sözleşme akdedilmeden önce gerekli adımların atılabilmesi için veri öznesinin talebi üzerine" yapıldığı sürece bu şekilde bir işleme meşru olacaktır.

AK mevzuatı gereğince, "başkalarının hak ve özgürlüklerinin korunması" AİHS madde 8(2)'de verilerin korunması hakkına yapılacak hukuka uygun bir müdahale gerekçesi olarak sayılmaktadır.

Veri sorumlusunun hukuki yükümlülükleri

AB mevzuatı, verilerin işlenmesini hukuka uygun hale getirecek, "veri öznesinin hukuki bir yükümlülüğüne uygun davranmak için gerekliyse" şeklinde düzenlenmiş başka bir kriterden de bahsetmektedir. Bu madde özel sektörde faaliyet gösteren veri sorumlularına yöneliktir; kamuda faaliyet gösteren veri sorumlularının hukuki yükümlülükleri VK Direktifi madde 7(e)'de düzenlenmektedir. Özel sektör veri sorumlularının başkalarına ait verileri işlemek yükümlülüğü altında bulundukları birçok durumdan bahsetmek mümkündür; örneğin hekimler ve hastaneler hastaların tedavi sürecine ait verileri uzun yıllar boyunca saklama yükümlülüğü altındadır; işverenler sosyal güvenlik ve vergilendirme gerekçeleriyle işçilerine ait verileri, işletmeler ise vergilendirme gerekçesiyle müşterilerine ait verileri işlemekle yükümlüdürler.

Hava yolu şirketlerinin yolcu verilerini yabancı göç idarelerine zorunlu olarak aktarmaları bağlamında yabancı bir hukuk düzeninden kaynaklanan yasal yükümlülüklerin AB hukuku kapsamında veri işlemeleri için hukuki bir dayanak oluşturup oluşturmadığı sorusu da gündeme gelmiştir. (Bu konu Bölüm 6.2.'de detaylı olarak ele alınmaktadır.).

Veri sorumlusunun yükümlülükleri AK mevzuatı kapsamında da verilerin işlenmesine yönelik hukuki bir dayanak oluşturmaktadır. Daha önce de belirtildiği üzere, özel sektörde faaliyet gösteren bir veri sorumlusunun yasal yükümlülükleri, AİHS m. 8(2)'de bahsedildiği üzere başkalarının meşru çıkarlarına dair yalnızca tek bir örneği teşkil etmektedir. Bu sebeple yukarıdaki örnek AK mevzuatı bakımından da uygulama alanı bulacaktır.

Veri öznesinin hayati çıkarları

AB mevzuatı kapsamında VK Direktifi madde 7(d), kişisel verilerin "veri öznesinin hayati çıkarlarının korunması gerekçesiyle" işlenmesi durumunda hukuka uygun sayılacağını belirtmektedir. Veri öznesinin hayatta kalmasıyla yakından ilişkili bu çıkarlar örneğin tıbbi verilerin veya kayıp kişilere ilişkin verilerin hukuka uygun olarak kullanılmasına yönelik bir dayanak oluşturabilirler.

AK mevzuatı kapsamında, veri öznesinin hayati çıkarları, verilerin korunması hakkına yönelik hukuka uygun bir müdahale gerekçesi olarak AİHS m.8'de yer almamaktadır. 108 Sayılı Sözleşme'yi belirli alanlar bakımından tamamlayıcı nitelikteki bazı AK tavsiye kararlarında, veri öznesinin hayati çıkarları, verilerin hukuka uygun olarak işlenmeleri için geçerli bir dayanak olarak ifade edilmektedir.[131] Veri öznelerinin hayati çıkarları açıkça veri işlemeyi haklı kılan sebepler arasında görülmektedir: veri öznesinin temel haklarının korunması hiçbir zaman veri öznesinin hayati çıkarlarını tehlikeye atmamalıdır.

Kamu menfaati ve resmi yetkinin kullanılması

[131] Profilleme Tüzüğü, Madde3.4 (b).

Kamuyu ilgilendiren işlerin düzenlenmesine yönelik çok sayıda yol olduğundan, VK Direktifi'nin 7(e) maddesi "kamu yararına yürütülen bir görevin ifası veya verileri elinde bulunduran veri sorumlusu veya üçüncü bir kişiye ait resmi bir yetkinin kullanılması için gerekliyse" kişisel verilerin hukuka uygun olarak işlenebileceğini düzenler.[132]

Örnek: **'Huber v. Almanya'**,[133] davasında, Almanya'da yaşayan bir Avusturya vatandaşı olan Bay Huber, Federal Göçmen ve Mülteci Dairesi'nden Yabancı Uyruklular Merkezi Sicili'nde ('AZR') yer alan kendine ait verilerin silinmesini talep etmiştir. Almanya'da üç aydan fazla bir süreyle oturacak olan yabancı uyruklu kişilere dair kişisel verileri içeren bu sicil istatiksel amaçlarla ve kolluk kuvvetleri ve yargı makamları tarafından suçların veya kamu güvenliğini tehdit eden faaliyetlerin soruşturulması ve kovuşturulması aşamalarında kullanılmaktadır. Davayı ABAD'a taşıyan mahkeme, diğer devlet kurumlarının da erişime sahip olduğu Yabancı Uyruklular Merkezi Sicili gibi bir sicilde tutulan kişisel verilerin işlenmesinin, Alman vatandaşları için böyle bir sicilin bulunmadığı göz önüne alındığında, AB hukuka uygun olup olmadığını sormuştur.

Birincil olarak ABAD, VK Direktifi madde 7(e) uyarınca, kişisel verilerin işlenmesinin ancak kamu menfaati veya resmi bir yetkinin kullanılması için gerekli olması durumunda hukuka uygun olacağını belirtmiştir.

ABAD'a göre, "bütün Üye Devletlerde eşdeğer seviyede bir korumanın sağlanması amacı göz önünde tutulduğunda VK Direktifi madde 7(e)'de yer verilen gereklilik kavramının […] Üye Devletler arasında farklılık gösterecek bir anlamı olamaz. Dolayısıyla da elimizde Topluluk hukuku kapsamında kendi bağımsız anlamına sahip ve direktifin 1(1) maddesinde belirtilen amaçları tam olarak yansıtması gereken bir kavram bulunmaktadır."[134]

Mahkeme ayrıca, bir Üye Devletin topraklarındaki -o üye devletin vatandaşı olmayan- bir Birlik vatandaşının seyahat özgürlüğünün mutlak olmadığını, Avrupa Birliği Antlaşması ve bağlantılı tedbirler uyarınca sınırlamalara ve şartlara tabi olabileceğini hatırlatmaktadır. Buradan hareketle, oturma hakkıyla alakalı yasaları uygulamakla görevli makamlara destek olması adına AZR gibi bir sicilin kullanılması bir Üye Devlet için prensip olarak meşru ise, bu sicilin o belirli amaç için gerekli olmayan hiçbir bilgiyi içermemesi gerekmektedir. Mahkeme, kişisel verilerin işlenmesi için kurulmuş bu şekildeki bir sistemin yalnızca ilgili mevzuatı uygulamak için gerekli olan verileri içermesi ve sistemin merkezi niteliğinin ilgili mevzuatın uygulamasını daha etkili hale getirmesi durumunda AB hukuka uygun olacağını değerlendirmiştir. Ulusal mahkeme somut olayda bu şartların oluşup oluşmadığını belirlemek durumundadır. Şartlar yerine getirilmediyse, kişisel verilerin AZR gibi bir sicilde istatiksel amaçlar için saklanması ve işlenmesi hiçbir şekilde VK Direktifi madde 7(e) uyarınca gerekli olarak görülemez.[135]

Son olarak, sicilde yer alan verilerin verilerin suçla savaş amacıyla kullanılmalarıyla alakalı olarak Mahkeme, bu amacın "faillerin tabiiyetinden bağımsız olarak suçların ve ihlallerin kovuşturulması"na ilişkin olacağını ifade etmiştir. Söz konusu sicil ilgili Üye Devletin kendi vatandaşlarına dair verileri kapsamamaktadır ve uygulamadaki bu farklılık Avrupa Birliğinin İşleyişi Hakkında Antlaşma'nın 18. maddesi kapsamında yasaklanan bir ayrımcılık teşkil etmektedir. Mahkeme'nin yorumuna göre bu madde, "bir Üye Devletin, kendi vatandaşı

[132] Bakınız, VK Direktifi, Gerekçe 32.
[133] ABAD, C-524/06, *Huber v. Germany*, 16 Aralık 2008.
[134] *A.e.*, par. 52.
[135] *A.e.*, par. 54, 58, 59, 66-68.

olmayan Birlik vatandaşlarına ait kişisel verileri suçla mücadele amacıyla işleyecek bir sistem kurmasını yasaklar".[136]

Kişisel verilerin kamusal alanda faaliyet gösteren yetkililer tarafından kullanımı da AİHS madde 8'in kapsamına girmektedir.

Veri sorumlusu veya üçüncü kişinin meşru çıkarları

Meşru çıkarlara sahip olan tek kişi veri öznesi değildir. VK Direktifi madde 7(f) "veri öznesinin temel hak ve özgürlüklerinin korunmasını gerektiren durumlar saklı kalmak kaydıyla, veri sorumlusunun veya verilerin ifşa olunduğu üçüncü kişi veya kişilerin meşru çıkarları için gerekli olması durumunda" kişisel verilerin işlenmesinin hukuka uygun olacağını düzenlemektedir.

ABAD aşağıdaki kararda açıkça Direktif madde 7(f)'ye dayanmıştır:

Örnek: **'ASNEF ve FECEMD'**[137] davasında ABAD, ulusal hukukun, verilerin hukuka uygun işlenmelerine dair VK Direktifi madde 7(f) ile belirlenen şartlara bir ekleme yapamayacağını açıklığa kavuşturmuştur. Bu açıklama, İspanyol veri koruma mevzuatında yer alan ve veri öznesinin dışındaki gerçek kişilerin, yalnızca ilgili bilgilerin daha önce kamuya açık kaynaklarda yer almış olması durumunda verilerin işlenmesinde meşru bir çıkarları olduğunu ileri sürebileceklerine dair bir düzenlemeye atfen yapılmıştır.

ABAD ilk önce, VK Direktifi'nin, kişisel verilerin işlenmesiyle alakalı bireylerin hak ve özgürlüklerine yönelik korumanın düzeyinin bütün Üye Devletlerde aynı seviyede olması amacını taşıdığını belirtmiştir. Bu alandaki ulusal mevzuatın direktif ile uyumlulaştırılmasının sağlanan korumanın düzeyinde herhangi bir azalmaya sebep olmaması gerektiği de vurgulanmıştır. Aksine AB içinde yüksek düzeyde bir koruma sağlamayı hedeflemelidir.[138] Dolayısıyla, ABAD, VK Direktifi'nin 7. maddesinde kişisel verilerin işlenmesinin hukuka uygun olarak değerlendirileceği durumlara dair kapsamlı ve sınırlayıcı bir liste yapılmasının bütün Üye Devletlerde aynı koruma düzeyinin sağlanması amacından ileri geldiğini belirtmiştir. Ek olarak, "Üye Devletler bu listeye hukuka uygun işlemeye dair yeni ilkeler ekleyemezler veya 7. maddede sayılan altı ilkeden birinin kapsamını değiştirecek ek koşullar getiremezler.[139] Mahkeme, VK Direktifi madde 7(f) uyarınca gerekli olan dengelemeyle bağlantılı olarak, "veri öznesinin temel haklarına yönelik olarak işlemeden kaynaklanabilecek ihlalin ciddiyetinin söz konusu verilerin daha önceden kamuya açık kaynaklarda yer almış olup olmadığına göre değişebileceğinin göz önüne alınmasının mümkün olduğunu" kabul etmiştir.

Ancak, "VK Direktifi madde 7(f), bazı kişisel veri kategorilerinin Üye Devletler tarafından kategorik ve genelleştirilmiş bir şekilde ve her bir somut olay bakımından çatışan haklar ve çıkarlar bakımından bir dengeleme yapılmaksızın işleme kapsamı dışında tutulmalarının yasak olduğunu düzenlemektedir."

[136] *A.e.,* par. 78 ve 81.
[137] ABAD, Birlikte Görülen C-468/10 ve C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011.
[138] *A.e.*, par. 28. Bakınız VK Direktifi, Gerekçe 8 ve 10.
[139] AİHM, *Rotaru v. Romania* [GC], No. 28341/95, 4 Mayıs 2000, par. 57; Bakınız AİHM, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, 28 Haziran 2007; AİHM, *Shimovolos v. Russia*, No. 30194/09, 21 Haziran 2011; ve AİHM, *Vetter v. France,* No. 59842/00, 31 Mayıs 2005.

Bu değerlendirmeler çerçevesinde Mahkeme, "VK Direktifi madde 7(f)'nin, veri öznesinin rızasının bulunmadığı ve veri öznesinin kişisel verilerinin işlenmesinin veri sorumlusunun veya verilerin ifşa olunduğu üçüncü kişi veya kişilerin meşru çıkarları için gerektiği durumlarda, veri öznesinin temel hak ve özgürlüklerine saygı gösterilmesi yanında verilerin daha önceden kamuya açık kaynaklarda yer almış olmasını da şart koşan, dolayısıyla da böyle kaynaklarda yer almayan verilerin işlenmesini kategorik ve genelleştirilmiş bir biçimde engelleyen ulusal düzenlemelerin getirilmesini yasaklayan bir hüküm olarak yorumlanması gerektiğini" belirtmiştir. [140]

AK'nin tavsiye kararlarında da benzer yorumlamalara rastlamak mümkündür. AK'nin Profil Oluşturma Tavsiye Kararı, başkalarının meşru çıkarları için gerekmesi durumunda ve "veri öznesinin temel hak ve özgürlüklerinin korunması hali saklı kalmak kaydıyla", kişisel verilerin profil oluşturma amacıyla işlenmesini meşru olarak değerlendirmektedir.[141]

4.1.2. Özel nitelikli (hassas) kişisel verilerin hukuka uygun olarak işlenmesi

AK mevzuatı, hassas verilerin kullanımına dair uygun bir korumanın düzenlenmesini ulusal yasalara bırakırken, AB mevzuatı, VK Direktifi madde 8 uyarınca, ırk veya etnik kökene, siyasi görüşe, dini veya felsefi inanca, sendika üyeliğine, sağlık veya cinsel hayata ilişkin bilgiler içeren veri kategorilerinin işlenmesine yönelik detaylı düzenlemer içermektedir. Kural olarak hassas verilerin işlenmesi yasaktır.[142] Ancak, bu yasağın istisnalarını sınırlı sayı ilkesi uyarınca sayan düzenlemeler Direktif madde 8(2) ve 8(3)'de yer almaktadır. Bu istisnalar arasında veri öznesinin açık rızası, veri öznesinin hayati menfaatleri, başkalarının meşru çıkarları ve kamu yararı bulunmaktadır.

Hassas olmayan verilerin işlenmesinden farklı olarak, veri öznesiyle kurulmuş bir sözleşme ilişkisi, hassas verilerin işlenmesinin meşruluğu için genel bir dayanak olarak görülemez. Bu sebeple, hassas verilerin veri öznesiyle yapılan bir sözleşme bağlamında işlenecek olması halinde, bu verilerin kullanımı için veri öznesinin, sözleşmenin akdedilmesine yönelik rızası dışında, ayrı bir açık rızası gerekmektedir. Veri öznesinin hassas verileri ister istemez ortaya çıkaran mal ve hizmetlere yönelik açık bir talebi açık rıza hükmünde değerlendirilmelidir.

Örnek: Bir uçak yolcusu, bilet rezervasyonu kapsamında, havayolu şirketinin bir tekerlekli sandalye ve Yahudi inancına uygun yemek sağlamasını talep ederse, yolcu sağlık durumu ve dini inancına dair bilgilerin açıklanmasına rıza gösterdiğine dair ek bir rıza maddesini imzalamamış olsa bile havayolu şirketi bu verileri kullanabilir.

Veri öznesinin açık rızası

Verilerin hukuka uygun olarak işlenmesinin ilk koşulu, bilgilerin hassas olup olmadığına bakılmaksızın, veri öznesinin rızasıdır. Hassas bilgi söz konusu ise bu rıza açıkça verilmelidir. Ancak ulusal mevzuat kapsamında hassas verilerin kullanılması bakımından rızanın tek başına yeterli bir yasal dayanak olmadığı[143], örneğin işlemenin veri öznesine yönelik olağandışı riskler

[140] *A.e.*, par. 40, 44, 48 ve 49.
[141] Profilleme Tüzüğü, Madde3.4 (b).
[142] VK Direktifi, Madde8 (1).
[143] *A.e., Madde8 (2) (a).*

oluşturabileceği istisnai durumlarda rızanın tek başına yeterli yasal dayanak oluşturmayacağı düzenlenebilir.

Konuyla alakalı özel bir durum kapsamında, zımni rıza bile hassas verilerin işlenmesi için yasal bir dayanak olarak kabul edilmektedir: VK Direktifi madde 8(2)(e) uyarınca veri öznesi tarafından aleni bir şekilde kamuya duyurulmuş verilere ilişkin işlemeler yasak değildir. Bu hüküm veri öznesinin verilerini kamuya açıklama şeklindeki eyleminin bu verilerin kullanılmasına yönelik zımni rızası olarak yorumlanması gerektiğini kabul etmektedir.

Veri öznesinin hayati menfaatleri

Hassas olmayan verilerin işlenmesinde olduğu gibi, hassas veriler veri öznesinin hayati menfaatleri söz konusu olduğunda işlenebilir.[144]

Hassas verilerin işlenmesinin bu temelde hukuka uygun olabilmesi için verilerin işlenmesine dair kararın, örneğin bilinç kaybı veya kendisine ulaşılamaması vb. sebeplerle veri öznesinin takdirine sunulamayacak olması gerekir.

Başkalarının meşru menfaatleri

Hassas olmayan verilerin işlenmesinde olduğu gibi, hassas veriler başkalarının meşru menfaatleri söz konusu olduğunda işlenebilir. Ancak hassas veriler bakımından ve VK Direktifi madde 8(2) uyarınca bu işleme ancak aşağıdaki durumlarda mümkündür:

- veri öznesinin fiziksel veya hukuki bağlamda rıza göstermesine imkan bulunmadığı hallerde işlemenin başka bir kişinin meşru menfaatleri açısından gerekli olması;[145]

- hassas verilerin iş hukuku kapsamında önem taşıdığı hallerde, örneğin tehlikeli sınıfta yer alan iş yerleri bakımından tıbbi veriler, veya resmi tatiller bakımından dini inançlarda olduğu gibi.[146]

- siyasi, felsefi, dini veya sendikasal amaçla kurulmuş vakıfların, derneklerin veya kar amacı gütmeyen diğer kuruluşların üyeleri, sponsorları veya ilgili diğer taraflarla alakalı verileri işlemesi durumunda (bu tür veriler hassas verilerdir çünkü veri öznelerin dini veya siyasi inançlarını açığa vurmaları muhtemeldir);[147]

- hassas verilerin yasal bir talebin ortaya koyulması, uygulanması veya savunulması amacıyla bir mahkeme veya idari mercii önünde kullanılması.[148]

- Bunlara ek olarak, VK Direktifi madde 8(3) kapsamında tıbbi verilerin muayene ve tedavi amacıyla sağlık kuruluşları tarafından kullanıldığı durumlarda bu hizmetlerin yönetimi de bu istisna kapsamındadır. Özel bir koruma önlemi olarak, 'sağlık kuruluşu" tanımı kapsamına giren kuruluşlar mesleki gizlilik (sır saklama) yükümlülüğü altında bulunanlarla sınırlandırılmıştır.

[144] *A.e., Madde8 (2) (c).*
[145] *A.e., Madde8 (2) (c).*
[146] *A.e., Madde8 (2) (b).*
[147] *A.e., Madde8 (2) (b).*
[148] *A.e., Madde8 (2) (b).*

Kamu menfaati

Ek olarak, Veri Koruma Direktifi madde 8(4) uyarınca, Üye Devletler, aşağıdaki koşullara uyulduğu sürece hassas verilerin işlenebileceği yeni amaçlar öngörmekte serbesttir:

- verilerin işlenmesi somut bir kamu menfaatinin gerçekleştirilmesine yönelik sebeplerden kaynaklanıyorsa; ve
- verilerin bu amaçla işlenebileceği ulusal mevzuatta veya bir denetim makamının kararında yer alıyorsa; ve
- bu ulusal hükümler veya denetim makamı tarafından alınan karar veri öznesinin menfaatlerini etkili şekilde koruyacak gerekli güvencelere sahipse.[149]

Öne çıkan bir örnek, birçok Üye Devlette kurulmak üzere olan elektronik tıbbi kayıt sistemleridir. Bu sistemler, sağlık kuruluşları tarafından bir hastanın tedavi sürecinde topladıkları tıbbi verilerin bu hastaya sağlık hizmeti sunan ulusal çaptaki diğer sağlık kuruluşlarının erişimine sunulmasına izin vermektedir.

Madde 29 Çalışma Kurultayı, bu şekildeki sistemlerin kurulmasının hastalara ait verilerin işlenmesine dair VK Direktifi'nin 8(3) maddesi kapsamında mümkün olmadığını değerlendirmiştir. Söz konusu elektronik tıbbi kayıt sistemlerinin varlığının somut bir kamu yararı teşkil ettiği varsayılsa bile, madde 8(4) kapsamında, kurulmaları için açık bir yasal dayanağın bulunması ve sistemin güvenli bir şekilde işlemesi için gerekli tedbirlerin alınmış olması gerekecektir.[150]

4.2. İşleme sürecinin güvenliğine dair kurallar

Ana başlıklar

- İşleme sürecinin güvenliğine dair kurallar, veri sorumlusunun ve veri işleyenin, veri işleme faaliyetlerine yetkisiz müdaheleleri önlemek için gerekli teknik ve örgütsel tedbirleri almasına yönelik bir yükümlülüğe işaret eder.
- Gereken veri güvenliği seviyesi aşağıdaki kriterlere göre belirlenir:

1) herhangi belirli bir işleme tipi için piyasada bulunabilecek güvenlik önlemleri; ve
2) maliyetler;
3) işlenen veririnin hassaslığı.

- Verilerin güvenli olarak işlenmesi görevi genel bir sorumluluk bağlamında işleme sürecinde yer alan bütün kişilere, veri sorumlularına veya işleyenlere düşmekte ve verilerin gizli kaldığından emin olunması gerekmektedir.

Veri sorumlularının ve veri işleyenlerin veri güvenliğini sağlamaya yönelik gerekli önlemleri alma yükümlülüğü AK veri koruma mevzuatında ve AB veri koruma mevzuatında yer almaktadır.

4.2.1. Veri güvenliğinin unsurları

[149] *A.e., Madde8 (2) (b).*

[150] Madde 29 Çalışma Kurultayı (2007), *Sağlıkla ilgili kişisel verilerin elektronik sağlık kayıtlarında işlenmesine ilişkin Çalışma Belgesi,* WP 131, Brüksel, 15 Şubat 2007.

AB mevzuatında yer alan ilgili hükümler gereğince:

> *'Üye Devletler, kişisel verilerin, özellikle de işleme sürecinde verilerin bir ağ üzerinde aktarımının söz konusu olduğu hallerde, kazara veya hukuka aykırı olarak imhası veya kaza eseri kaybolması, değişmesi, yetkisiz kişilerin eline geçmesi veya erişimine açılması durumlarına yönelik olarak gerekli teknik ve örgütsel tedbirlerin veri sorumlusu tarafından alınmasını sağlamalıdırlar.*[151]

AK mevzuatında da benzer bir hüküm yer almaktadır:

> *"Otomatik veri dosyalarında saklanan kişisel verilerin kazara veya yetkisiz bir müdahale sonucu imhaya veya kaza eseri kaybolmaya, yetkisiz erişim, değişiklik veya yayılmaya karşı korunmaları için gerekli güvenlik tedbirleri alınmalıdır".*[152]

Verilerin güvenli olarak işlenmesine yönelik endüstriyel, ulusal ve uluslararası standartların da getirildiği sıklıkla görülmektedir. Örneğin Avrupa Gizlilik Mührü (EuroPriSe), AB'nin ürünleri, özellikle de yazılımları Avrupa veri koruma hukukuna uygunluk anlamında sertifikalandırma olanaklarını araştırdığı eTEN (Trans-Avrupa Telekomünikasyon Ağları) projelerinden birisidir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) ise AB'nin, Üye Devletlerin ve iş dünyasının ağ ve bilgi güvenliği alanlarındaki sorunları önleme, tespit etme ve çözümler bulma konusundaki kabiliyetlerini geliştirmek üzere kurulmuştur.[153] ENISA düzenli olarak güncel güvenlik tehditleri hakkında analizler yayınlar ve bu tehditlerin nasıl üstesinden gelinebileceğine dair tavsiyelerde bulunur.

Veri güvenliği tek başına doğru teçhizata -donanım ve yazılıma- sahip olmakla sağlanamaz. Aynı zamanda, uygun iç organizasyon kuralları gerektirir. Bu kurallar tercihen aşağıdaki hususları kapsamalıdır:

- çalışanların veri güvenliği kuralları ve veri koruma hukuku kapsamındaki yükümlülükleri, özellikle de gizlilik/sır saklama yükümlülükleri hakkında düzenli olarak bilgilendirilmesi;

- sorumlulukların açık bir şekilde dağıtılması ve veri işleme süreçleriyle, özellikle de kişisel verilerin işlenmesine yönelik kararlar ve verilerin üçüncü kişilere aktarılmasıyla alakalı yetkinliklere dair açık bir çerçevenin çizilmesi;

- kişisel verilerin yalnızca yetkili kişinin talimatları veya genel olarak belirlenen kurallar uyarınca kullanılması;

- veri sorumlusunun veya veri işleyenin bulundukları bölgeye ve donanım ve yazılımlarına erişimin, erişim yetkisine yönelik kontrollerle korunması;

- kişisel verilere erişim yetkilerinin bunu vermeye yetkili kişiler tarafından verildiğinden ve düzgün şekilde belgelendirildiğinden emin olunması;

---

[151] VK Direktifi, Madde17 (1).
[152] 108 Sayılı Sözleşme, Madde7.
[153] Avrupa Birliği Parlamentosu ve Konseyi, *460/2004 Sayılı, Avrupa Ağ ve Bilgi Güvenliğ Ajansı'nın kurulmasına ilişkin Tüzük,* 10 Mart 2004, OJ 2004 L 77.

- kişisel verilere elektronik yollardan erişimin otomatik protokoller aracılığıyla yapılması ve bu protokollerin iç denetim birimi tarafından düzenli olarak kontrol edilmesi;

- Yasa dışı veri aktarımlarının gerçekleşmediğini gösterebilmek adına, otomatik erişim dışındaki biçimlerde ifşa edilen veriler bakımından belgelendirmenin dikkatli şekilde yapılması.

Personele veri güvenliği hakkında yeterli eğitimin verilmesi de alınacak etkili güvenlik önlemlerinin unsurlarından birisidir. Gerekli tedbirlerin yalnızca kâğıt üzerinde kalmaması, uygulamada da kullanılması ve işe yarayabilmesi için doğrulama prosedürlerinin de öngörülmesi gerekmektedir (örneğin iç veya dış denetimler gibi).

Veri sorumlusu veya veri işleyenin güvenlik düzeyini arttıracak önlemler kişisel veri koruma memurları, çalışanlara verilecek güvenlik eğitimleri, düzenli denetimlerin yapılması, sızma testleri ve kalite mühürleri gibi tedbirleri içermektedir.

Örnek: **'I v. Finlanda'**[154] davasında başvuran, çalıştığı hastanedeki diğer çalışanlar tarafından tıbbi kayıtlarına hukuka aykırı olarak erişildiğini ispatlayamamıştır. Başvuranın verilerin korunması hakkının ihlal edildiği yönündeki iddiası, bu sebeple ulusal mahkemeler tarafından reddedilmiştir. AİHM, hastanenin tıbbi dosyalar için kullandığı kayıt sisteminin "yalnızca uygulanan son beş tedaviyi göstermesi ve dosya arşive kaldırılır kaldırılmaz bu bilgilerin de siliniyor olması sebebiyle hasta kayıtlarının geçmişe yönelik olarak açıklığa kavuşturulmasına imkân vermediği" gerekçesiyle AİHS'nin 8. maddesinin ihlal edildiği sonucuna varmıştır. Mahkeme, ulusal mahkemelerin bu gerçek üzerinde yeterince durmadığını ancak söz konusu kayıt sisteminin ulusal mevzuatta yer alan yasal koşullara açıkça aykırı olmasının bu kararda belirleyici olduğunu ifade etmiştir.

Veri ihlali bildirimleri

Veri güvenliği ihlalleriyle başa çıkmak için birçok Avrupa ülkesinin veri koruma mevzuatlarına dahil ettiği yeni bir yol bulunmaktadır: elektronik haberleşme hizmetleri sağlayıcılarının veri ihlallerini muhtemel mağdurlara ve denetim makamlarına bildirme zorunluluğu. Telekomünikasyon sağlayıcıları bakımından, bu bildirim AB hukuku kapsamında zorunludur.[155] Veri ihlalleri bildirimlerinin veri öznelerine yapılmasının amacı zararların önlenmesidir: veri ihlallerinin ve olası sonuçlarının bildirilmesi veri öznelerine yönelik olumsuz etkilerin oluşması riskini en aza indirgemektedir. Ciddi ihmaller söz konusu olduğunda, hizmet sağlayıcılar para cezasına da çarptırılabilir.

Veri öznelerine ve/veya denetim makamlarına bu ihlallerin bildirilmesi amacıyla ulusal mevzuatlar tarafından tanınan süreler genellikle kısa olduğundan, veri ihlallerinin etkili şekilde

[154] AİHM, *I. v. Finland*, No. 20511/03, 17 Temmuz 2008.

[155] Bakınız, Avrupa Birliği Parlamentosu ve Konseyi, 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi, 12 Temmuz 2002, OJ 2002 L 201, madde 4 (3), 2009/136/AB Sayılı Direktif tarafından değiştirilen Avrupa Birliği ve Konseyi Direktifi, 2002/22/AB Sayılı Elektronik iletişim ağları ve hizmetleri ile ilgili evrensel hizmet ve kullanıcı haklarına ilişkin Direktif, 25 Kasım 2009, Ayrıca bakınız; 2002/58 Sayılı Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi ve 2006/2004 Sayılı, Tüketici koruma kanunlarının uygulanmasından sorumlu ulusal makamlar arasındaki işbirliği Tüzüğü, 2009/136/AB Sayılı Avrupa Birliği Parlamentosu ve Konseyi Direktifi, 25 Kasım 2009, OJ 2009 L 337.

yönetilmesi ve bildirimlerin yapılabilmesi için iç taraftaki prosedürlerin önceden belirlenmiş olması gerekmektedir.

4.2.2. Gizlilik

AB mevzuatı uyarınca, verilerin güvenli şekilde işlenmesi, bu sürece dahil olan bütün kişilere, veri sorumlularına veya veri işleyenlere yönelik genel bir ödev olarak ifade edilmekte ve verilerin gizli kalması bu şekilde güvence altına alınmaktadır.

Örnek: Bir sigorta şirketi çalışanı iş yerinde bulunduğu sırada, şirket müşterisi olduğunu söyleyen birisi tarafından telefonla aranır ve sigorta sözleşmesine dair bilgiler talep edilir.

Müşterilerin verilerinin gizli tutulması görevi, çalışanın bu kişisel verileri ifşa etmeden önce asgari güvenlik tedbirlerini uygulamasını gerektirmektedir. Bu da, örneğin, müşterinin dosyasında kayıtlı bulunan telefon numarasına konuyla alakalı dönüş yapılacağına dair bir cevap verilmesi yoluyla sağlanabilir.

VK Direktifi'nin 16. maddesi gizliliği yalnızca veri sorumlusu-veri işleyen ilişkisi bağlamında ele almaktadır. Veri sorumlularının verileri, üçüncü kişilere ifşa bakımından gizli tutmak zorunda olup olmadıkları direktifin 7. ve 8. maddesinde düzenlenmektedir.

Verilerin, bir kişinin bilgisi dahiline veri sorumlusu veya veri işleyenin bir çalışanı olarak değil de tamamen kendi kişisel konumları gereği geçtiği durumlarda gizlilik yükümlülüğü geçerli olmayacaktır. Bu durumda VK Direktifi'nin 16. maddesi uygulama alanı bulmayacaktır çünkü kişisel verilerin bireyler tarafından kullanılması, hanehalkı istisnası kapsamına girdiği sürece direktifin düzenleme alanının tamamen dışında kalmaktadır.[156] Hanehalkı istisnası kişisel verilerin "gerçek bir kişi tarafından ve tamamen kişisel veya hanehalkı faaliyetleri sırasında" kullanılmasını ifade eder.[157] ABAD'ın 'Bodil Linqvist'[158] davasında verdiği karardan beri bu istisnanın özellikle de verilerin ifşası bakımından dar olarak yorumlanması gerekmektedir. Özellikle bu istisna kişisel verilerin internet ortamındaki belirsiz sayıda kişiye yayınlanması durumunu kapsamayacaktır (Daha fazla bilgi için bkz. Bölüm 2.1.2, 2.2., 2.3.1., ve 6.1).

AK mevzuatı uyarınca, gizlilik yükümlülüğü, 108 Sayılı Sözleşme'nin veri güvenliğine dair 7. maddesinde yer alan veri güvenliği kavramı içerisinde bulunmaktadır.

Veri işleyenler için gizlilik yükümlülüğü, veri sorumlusu tarafından kendilerine emanet edilen kişisel verilerin yalnızca veri sorumlusunun talimatlarına uygun olarak kullanılabileceği anlamına gelmektedir. Bir veri sorumlusunun veya veri işleyenin çalışanları bakımından ise gizililik yükümlülüğü, bu çalışanların kişisel verileri yalnızca yetkili amirlerinin talimatları doğrultusunda kullanmaları anlamına gelir.

Gizlilik yükümlülüğü veri sorumluları ve veri işleyenler arasındaki her türlü sözleşmede yer alması gereken bir yükümlülüktür. Ayrıca veri sorumluları ve veri işleyenler, genellikle iş akdinde yer verecekleri bir gizlilik hükmü yoluyla, çalışanlarına yönelik bir gizlilik yükümlülüğü getirmek durumundadırlar.

[156] VK Direktifi, Madde3 (2) ikinci paragraf.
[157] *A.e.*
[158] ABAD, C-101/01, *Lindqvist,* 6 Kasım 2003.

Gizliliğe yönelik mesleki yükümlülüklerin ihlali, AK 108 Sayılı Sözleşme'ye taraf devletlerde ve birçok Üye Devlette ceza yasaları gereği cezalandırılabilir niteliktedir.

4.3. Verilerin işlenmesinde şeffaflığa dair kurallar

Ana başlıklar

- Kişisel verilerin işlenmesine başlamadan önce veri sorumlusu, veri öznesi bu bilgilere zaten sahip değilse, veri öznelerine kendi kimliği hakkında bilgi vermeli ve verileri hangi amaç ile işleyeceğini bildirmelidir.
- Verilerin üçüncü kişilerden toplandığı hallerde, bilgilendirme yükümlülüğü aşağıdaki koşulların gerçekleşmesi durumunda uygulanmaz:

1) verilerin işlenmesinin yasa ile öngörülmüş olması; veya
2) bilgilendirme yükümlülüğünün imkansız olduğunun anlaşılması veya aşırı bir gayret gerektirecek olması.

- Ayrıca, veri sorumlusu verileri işlemeye başlamadan önce:

1) denetim makamına planlanan işleme faaliyetleri ile alakalı bildirimde bulunmalı; veya
2) ulusal yasaların öngörmesi durumunda, işlemeye dair iç belgelendirmeyi bağımsız bir veri koruma memuruna yaptırmalı.

Verilerin adil olarak işlenmesi ilkesi, verilerin şeffaf bir şekilde işlenmesini gerektirmektedir. AK mevzuatı uyarınca her kişi veri işleme dosyalarının varlığını, amaçlarını ve ilgili veri sorumlusunu tespit edebilecek durumda olmalıdır.[159] Bunların nasıl sağlanacağı ise ulusal hukuk düzenlerine bırakılmıştır. AB mevzuatı ise veri öznesi yararına şeffaflığı sağlamak adına veri sorumlusuna yönelik olarak veri öznesini bilgilendirme ve kamuoyuna bildirim yükümlülükleri öngörmektedir.

Her iki yasal sistemde de sınırlamanın belirli kamu menfaatlerini ve veri öznesinin veya başkalarının hak ve özgürlüklerini korumak için demokratik bir toplumda gerekli olması durumunda veri sorumlusunun şeffaflık yükümlülüklerine yönelik istisnalar ve sınırlamalar getirilebilir.[160] Bu tür istisnalar, örneğin suçların soruşturulması bağlamında gerekli görülebilir veya başka koşullar altında haklı gerekçelere dayanabilir.

4.3.1. Bilgilendirme

AK ve AB mevzuatına göre, verilerin işlenmesine başlamadan önce veri sorumluları, veri öznelerine planlanan işlemeyle alakalı bilgilendirmede bulunmakla yükümlüdür.[161] Bu yükümlülük veri öznesinden gelecek bir talebe bağlı olarak değil, veri öznesinin söz konusu bilgilerle ilgilenip ilgilenmediğine bakılmaksızın, veri sorumluları tarafından proaktif bir şekilde yerine getirilmelidir.

Bilgilendirmenin içeriği

[159] 108 Sayılı Sözleşme, Madde8 (a).
[160] *A.e.*, Madde9 (2); ve VK Direktifi, Madde13 (1).
[161] 108 Sayılı Sözleşme, Madde8 (a); ve VK Direktifi Madde10 ve 11.

Bilgilendirme, işlemenin amacını, veri sorumlusunun kimlik ve iletişim bilgilerini içermelidir.[162] VK Direktifi, "verilerin toplandığı belirli durumlarla alakalı olarak, veri öznesi bakımından adil işlemenin güvence altına alınması için gerekli olması" durumunda bu bilgilendirme kapsamında başka ek bilgiler de verilmesi gerektiğini düzenlemektedir. VK Direktifi madde 10 ve 11 diğer konularla birlikte işlenen verilerin kategorilerini, bu verilerin alıcılarını ve verilere erişim hakkı ile verilerin düzeltilmesini talep hakkını da genel hatlarıyla belirlemektedir. Verilerin veri öznelerinden toplanması sırasında yapılacak bilgilendirmede, soruların cevaplanmasının zorunluluk veya gönüllülük esaslarından hangisine dayalı olduğuna ve bu sorulara cevap verilmemesi durumunda ortaya çıkabilecek olası sonuçlara dair bilgiler de yer almalıdır.[163]

AK mevzuatı uyarınca bu bilgilendirmenin yapılması verilerin adil işlenmesi ilkesi kapsamında iyi bir uygulama ve bu bağlamda da AK mevzuatının bir parçası olarak değerlendirilebilir.

Adil işleme ilkesi bilgilendirmenin veri özneleri tarafından kolaylıkla anlaşılabilir olmasını gerektirmektedir. Muhataplar açısından uygun olan bir dil kullanılmalıdır. Hedef alınan kitlenin yetişkinler veya çocuklar, kamuoyu veya akademik uzmanlar olmasına bağlı olarak kullanılan dilin seviyesi veya türü de farklılık göstermelidir.

Bazı veri özneleri verilerinin nasıl ve neden işlendiğiyle alakalı olarak yalnızca özet bir şekilde bilgilendirilmek isterlerken, bazıları da detaylı bir açıklamaya ihtiyaç duyacaklardır. Uygun şekilde bilgilendirmeye dair bu yönün ne şekilde dengeleneceğiyle alakalı olarak, Madde 29 Çalışma Kurultayın'ınbir görüşünde katmanlı bilgilendirme[164] olarak isimlendirilen ve veri öznesinin detay seviyesine karar verebileceği bir yapı öne çıkarılmaktadır.

Bilgilendirmenin yapılma zamanı

VK Direktifi bilgilendirmenin ne zaman yapılması gerektiğiyle alakalı, verilerin veri öznesinden (madde 10) veya üçüncü bir kişiden (madde 11) toplanmasına bağlı olarak kısmen değişen hükümler içermektedir. Verilerin veri öznesinden toplanmış olması durumunda bilgilendirmenin en geç toplama anında yapılması gerekmektedir. Verilerin üçünkü kişilerden toplanması durumunda ise bilgilendirmenin en geç veri sorumlusunun verileri kaydettiği anda veya verilerin ilk kez üçüncü bir kişiye ifşa edilmesinden önce yapılması gerekmektedir.

Bilgilendirme zorunluluğunun istisnaları

AB mevzuatı uyarınca, veri öznesinin bilgilendirilmesi zorunluluğuna getirilmiş genel bir istisna veri öznesinin zaten bu bilgilere sahip olduğu durumlarda söz konusudur.[165] Burada veri öznesinin, durumun koşulları gereği, verilerinin belirli bir amaç için belirli bir veri sorumlusu tarafından işleneceğinin farkında olması durumundan bahsedilmektedir.

VK Direktifi'nin verilerin veri öznesinden alınmadığı durumlara yönelik bilgilendirme yükümlülüğünü düzenleyen 11. maddesi, istatistiksel amaçlarla ve tarihi veya bilimsel

[162] 108 Sayılı Sözleşme, Madde8 (a); ve VK Direktifi, Madde10 (a) ve (b).
[163] VK Direktifi, Madde10 (c).
[164] Madde 29 Çalışma Kurultayı (2004), *10/2004 Sayılı, Uyumlaştırılmış Bilgi Hükümlerine ilişkin Öneri,* WP 100, Brüksel, 25 Kasım 2004.
[165] VK Direktifi, Madde10 ve 11 (1).

araştırma amacıyla yapılacak işlemelerde de böyle bir yükümlülüğün aşağıdaki hallerde bulunmayacağını belirtmektedir:

- bu bilgilendirmeyi yapmanın imkansız olduğu anlaşılırsa; veya
- bilgilendirmeyi yapmanın aşırı bir gayret gerektirecek olması durumunda; veya
- verilerin kaydedilmesi veya ifşasının yasa ile açıkça düzenlenmiş olması durumunda.[166]

Yalnızca VK Direktifi madde 11(2)'de işleme faaliyetlerinin kanunla düzenlenmiş olması durumunda veri öznelerinin bilgilendirilmesinin gerekli olmadığı düzenlenmektedir. Kanunların muhatapları tarafından bilindiği şeklindeki genel yasal varsayımdan yola çıkılarak, direktifin 10. maddesi kapsamında bir veri öznesinden verilerin toplanması durumunda veri öznesinin bu bilgilere sahip olduğu ileri sürülebilir. Ancak kanunlara dair bu bilgili olma hali yalnızca bir varsayımdan ibaret olduğundan, işleme kanunla düzenlmiş olsa bile veri öznesinin, özellikle de verilerin doğrudan veri öznesinden toplandığı durumlarda bu bilgilendirmeyi yapmak aşırı bir külfet getirmeyeceğinden, adil işleme ilkesi gereği madde 10 kapsamında bilgilendirilmesi gerekecektir.

AK mevzuatı kapsamında, 108 sayılı Sözleşme, 8. maddesine dair istisnaları açıkça düzenlemektedir. Aynı şekilde, VK Direktifi'nin 10. ve 11. maddelerinde belirtilen istisnalar 108 Sayılı Sözleşme'nin 9. maddesi kapsamındaki istisnalar açısından iyi uygulama örnekleri olarak görülebilirler.

Farklı bilgilendirme yolları

Bilgilendirmede kullanılacak ideal yol her bir veri öznesine sözlü veya yazılı olarak bilgilendirmede bulunulmasıdır. Verilerin veri öznesinden alındığı durumlarda bilgilendirme işlemi toplama işlemiyle eş zamanlı olarak yapılmalıdır. Özellikle verilerin üçünkü kişilerden toplandığı hallerde, veri öznelerine şahsen ulaşmanın yaratacağı zorluklar göz önüne alınırsa, bilgilendirmenin uygun bir şekilde yayınlanma yoluyla yapılması da mümkündür.

Bilgilendirme yapmanın en etkili yollarından birisi de veri sorumlusunun ana sayfasında bilgilendirme kayıtlarına uygun bir şekilde -örneğin internet sitesi gizlilik politikası şeklinde- yer vermesidir. Ancak nüfusun önemli bir kesimi halen internet kullanmamaktadır ve bir şirketin veya bir kamu makamının bilgilendirme politikası bu gerçeği hesaba katmalıdır.

4.3.2. Bildirim

Ulusal yasalar, faaliyetlere ilişkin kayıtların yayınlanabilmesi adına, veri sorumlularını işleme faaliyetlerine dair yetkili denetim makamlarına bildirimde bulunma yükümlülüğü altına sokabilirler. Alternatif olarak, ulusal mevzuat veri sorumlularının, veri sorumlusu tarafından gerçekleştirilen işleme faaliyetlerinin bir kaydını tutmakla görevli bir kişisel veri koruma memuru istihdam etmelerini şart koşabilir.[167] Tutulan bu iç kayıtlar, talep üzerine vatandaşlara açılmalıdır.

Örnek: Kurum içi bir kişisel veri koruma memuru tarafından yapılacak bu bildirim ve belgelendirmenin söz konusu veri işlemeye dair temel özellikleri betimlemesi gerekmektedir.

[166] *A.e.*, Gerekçe 40 ve Madde 11 (2).
[167] *A.e.*, Madde18 (2) ikinci paragraf.

Bu kapsamda, veri sorumlusuna, verinin ne amaç ile işlendiğine, işlemenin yasal dayanağına, işlenen verilerin kategorilerine, muhtemel üçüncü kişi alıcılara ve verilerin sınır ötesi aktarımının planlanıp planlanmadığına, planlanıyorsa bu verilerin hangileri olduğuna dair bilgilere yer verilmelidir.

Denetim makamı bu bildirimleri özel bir sicil formatında yayınlamalıdır. Bu durum aynı şekilde veri sorumlusu tarafından bağımsız bir kişiye verdiği belgelendirme kapsamındadır. Sicilin amacına ulaşması için de buna erişimin kolay ve ücretsiz olması gerekir. Aynı koşullar bir veri sorumlusunun kişisel veri koruma memuru tarafından tutulan kayıtlar bakımından da geçerlidir.

VK Direktifi'nin 18(2) maddesinde[168] listelenen veri öznelerine yönelik bir risk oluşturma ihtimali düşük işleme faaliyetleri bakımından, yetkili denetim makamlarına bildirimde bulunma veya iç tarafta bir veri koruma memuru istihdam etme yükümlülüğüne ulusal hukuk düzenleri tarafından istisnalar getirilebilir.

4.4. Uyuma teşvik kuralları

Ana başlıklar

- Hesap verilebilirlik ilkesini getiren VK Direktifi, uyuma teşvik konusunda birçok yöntemden bahsetmektedir:

1) planlanan işleme faaliyetlerinin ulusal denetim makamlarınca ön kontrolünün yapılması;
2) veri sorumlusuna verilerin korunması alanında danışmanlık yapacak kişisel veri koruma memurları;
3) Mevcut veri koruma kurallarının toplumun belirli bir alanına, özellikle de iş sektörüne uygulanmasına yönelik detayları belirten davranış kuralları.

- AK Mevzuatı, Profil Oluşturma Tavsiye Kararı'nda da uyuma teşvik için benzer yöntemleri önermektedir.

4.4.1. Ön denetim

VK Direktifi madde 20 gereğince, -işlemenin amacı veya mevcut koşulları gereği- veri öznelerinin hak ve özgürlüklerine yönelik belirli riskler oluşturabilecek işleme faaliyetlerinin, denetim makamları tarafından işleme başlamadan önce denetlenmesi gerekmektedir. Ulusal mevzuat hangi işleme faaliyetlerinin ön denetime tabi tutulacağını belirlemek durumundadır. Bu denetimler, işleme faaliyetlerinin yasaklanması veya işleme faaliyetinin tasarlanan halinde bazı özelliklerin değiştirilmesi yönünde bir emirle sonuçlanabilir. VK Direktifi madde 20 gereksiz derecede riskli işlemelerin daha başlamadan bu faaliyeti yasaklamaya yetkili olan denetim makamları tarafından engellenmesi amacıyla getirilmiş bir düzenlemedir. Bu sistemin doğru bir şekilde işleyebilmesi için ön koşul denetim makamına bildirimin yapılmış olmasıdır. Veri sorumlularının bu bildirimde bulunma yükümlülüklerini yerine getirdiklerinden emin olmak için de denetim makamlarının bazı zorlayıcı yetkilere, örneğin veri sorumlularını cezalandırma yetkisine sahip olması gerekecektir.

Örnek: Eğer bir şirket yasa gereği ön denetime tabi işleme faaliyetleri yürütmekteyse, ilgili şirket planlanan işleme faaliyetlerine dair belgeleri denetim makamına sunmak zorundadır.

[168] *A.e.*, Madde18 (2) birinci paragraf.

Şirket, denetim makamından olumlu bir cevap almadıkça işleme faaliyetlerine başlayamayacaktır.

Bazı Üye Devletlerde, denetim makamının belirli bir zaman dilimi -örneğin üç ay- içerisinde konuyla alakalı bir cevap vermemiş olması halinde işleme faaliyetlerinin başlatılabileceğine dair ulusal düzenlemeler bulunmaktadır.

4.4.2. Kişisel veri koruma memurları

VK Direktifi, veri sorumlularının, kişisel veri koruma memuru olarak çalışacak bir memur istihdam edebileceklerine dair ulusal mevzuatta bir düzenleme yapılmasının mümkün olduğunu belirtmektedir.[169] Böyle bir görevlinin bulundurulmasındaki amaç ise veri öznelerinin hak ve özgürlüklerinin işleme faaliyetleri sebebiyle olumsuz olarak etkilenmesini önlemektir.[170]

Örnek: Almanya'da, Alman Federal Veri Koruma Yasası'nın (Bundesdatenschutzgesetz) 4f Kısmı'nın 1. Alt kısmı gereğince, kişisel verilerin otomatik işleme tabi tutulması alanında 10 veya daha fazla kişi çalıştıran özel şirketlerin kurum içi bir kişisel veri koruma memuru istihdam etmeleri gerekmektedir.

Yukarıda belirtilen amaca ulaşılması, direktifte de belirtildiği üzere, memurun veri sorumlusunun organizasyonu içindeki pozisyonu itibariyle belirli bir seviyede bağımsız olmasına bağlıdır. Haksız yere işten çıkarma gibi ihtimallere karşı koruma sağlayacak güçte işçi hakları da bu görevin etkili bir şekilde yerine getirilebilmesi açısından gerekli olacaktır.

Kurum içi kişisel veri koruma memurları kavramı, ulusal veri koruma mevzuatıyla uyumun teşvik edilmesi amacıyla bazı AK Tavsiye Kararlarında da benimsenmiştir.[171]

4.4.3. Davranış kuralları

Uyuma teşvik kapsamında, iş dünyası ve diğer sektörler tipik işleme faaliyetlerine yönelik detaylı kuralları belirleyebilir, böylece de en iyi uygulama biçimleri bir sisteme bağlanabilir. Bu sektörlerde çalışanların uzmanlıkları sayesinde pratik ve bu pratiklikleri sebebiyle de büyük ihtimalle tercih edilecek çözüm yolları bulunabilecektir. Buna uygun olarak, Üye Devletler – ve Avrupa Komisyonu- Üye Devletler tarafından direktife uygun olarak yürürlüğe konan ulusal mevzuatın düzgün bir şekilde uygulanmasına katkıda bulunacak ve çeşitli sektörlerin belirli özelliklerini dikkate alan davranış kurallarının hazırlanması yönünde teşvik edilmektedir.[172]

Bu davranış kurallarının, direktife uygun olarak yürürlüğe konan ulusal mevzuatın düzenlemeriyle uyumlu olmasını sağlamak için Üye Devletler'in bu davranış kurallarının değerlendirilmesine yönelik bir prosedür belirlemeleri gerekmektedir. Bu prosedür de normal olarak ulusal makamların, ticaret derneklerinin ve veri sorumlusu kategorilerini temsil eden diğer kurumların sürece dahil olmalarını gerektirecektir.[173]

[169] *A.e.*, Madde18 (2) ikinci paragraf.
[170] *A.e.*
[171] Örneğin, Profilleme Tüzüğü, Madde8.3.
[172] Bakınız VK Direktifi, Madde 27 (1).
[173] *A.e.*, Madde27 (2).

Topluluk kodları taslakları ve var olan Topluluk kodlarına yapılacak ekleme ve değişikliklere dair öneriler değerlendirilmesi için Madde 29 Çalışma Kurultayı'na sunulabilirler. Bu Çalışma Grubu'nun onayı sonrasında, Avrupa Komisyonu bu kodların gerekli şekilde yayınlanması için gereken işlemleri gerçekleştirebilir.[174]

Örnek: Avrupa Doğrudan ve İnteraktif Pazarlama Federasyonu (FEDMA) kişisel verilerin doğrudan pazarlamada kullanımıyla alakalı olarak bir Avrupa Uygulama Kodu hazırlamıştır. Bu kod Madde 29 Çalışma Kurultayı'na sunulmuştur. Elektronik pazarlama iletişime dair bir ek ise 2010 yılında koda eklenmiştir.[175]

[174] *A.e.,* Madde27 (3).

[175] Madde 29 Çalışma Kurultayı (2010), 4/2010 Sayılı *FEDMA, doğrudan pazarlama'da kullanılan kişisel verilerin Avrupa Davranış Kurallarına ilişkin* Önerisi, WP 174, Brüksel, 13 Temmuz 2010.

5.Veri öznelerinin hakları ve bu hakların uygulanması

AB	İşlenen konular	AK
Erişim hakkı		
Veri Koruma Direktifi, Madde 12 ABAD, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, 7 May 2009	**Kendi verilerine erişim hakkı**	108 Sayılı Sözleşme, Madde 8 (b)
	Verilerin düzeltilmesini, silinmesini ve engellenmesini isteme hakkı	108 Sayılı Sözleşme, Madde 8 (c) AİHM, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 Kasım 2008 AİHM, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 Haziran 2006 AİHM, *Ciubotaru v. Moldova*, No. 27138/04, 27 Nisan 2010
İtiraz hakkı		
Veri Koruma Direktifi, Madde 14 (1) (a)	**Veri öznesinin özel durumu sebebiyle itiraz hakkı**	Profil Oluşturma Tavsiye Kararı, Madde 5.3
Veri Koruma Direktifi, Madde 14 (1) (b)	**Verilerin doğrudan pazarlama amaçları için kullanılmasına itiraz hakkı**	Doğrudan Pazarlama Tavsiye Kararı, Madde 4.1
Veri Koruma Direktifi, Article 15	**Otomatik kararlara itiraz hakkı**	Profil Oluşturma Tavsiye Kararı, Madde 5.5
Bağımsız denetim		
Şart, Madde 8 (3) Veri Koruma Direktifi, Madde 28 AB Kurumları Veri Koruma Tüzüğü, Bölüm V Veri Koruma Tüzüğü ABAD, C-518/07, *European Commission v. Federal Republic of Germany*, 9 Mart	**Ulusal denetim makamları**	108 Sayılı Sözleşme, Ek Protokol, Madde 1

2010 ABAD, C-614/10, *European Commission v. Republic of Austria*, 16 Ekim 2012 ABAD, C-288/12, *European Commission v. Hungary*, 8 Nisan 2014		
Kanun yolları ve yaptırımlar		
Veri Koruma Direktifi, Madde 12	**Veri sorumlusuna yapılan talep**	108 Sayılı Sözleşme, Madde 8 (b)
Veri Koruma Direktifi, Madde 28 (4) AB Kurumları Veri Koruma Tüzüğü, Madde 32 (2)	**Denetim makamlarına yapılmış olan şikayetler**	108 sayılı Sözleşme, Ek Protokol, Madde 1 (2) (b)
Şart, Madde 47	**Mahkemeler (genel olarak)**	AİHS, Madde 13
Veri Koruma Direktifi, Madde 28 (3)	**Ulusal mahkemeler**	108 Sayılı Sözleşme, Ek Protokol, Madde 1 (4)
TFEU, Madde 263 (4) AB Kurumları Veri Koruma Tüzüğü, Madde 32 (1) TFEU, Madde 267	**ABAD**	
	AİHM	AİHS, Madde 34
Kanun yolları ve yaptırımlar		
Şart, Madde 47 Veri Koruma Direktifi, Madde 22 ve 23 ABAD, C-14/83, *Sabine von Colson and Elisabeth Kamann v. Land Nordrhein- Westfalen*, 10 Nisan 1984	**Ulusal veri koruma hükümlerinin ihlali**	AİHS, Madde 13 (Yalnızca AK üye ülkeleri için) 108 Sayılı Sözleşme, Madde 10 AİHM, *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008 AİHM, *Biriuk v. Lithuania*, No.

ABAD, C-152/84, *M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority*, 26 Şubat 1986		23373/03, 25 Kasım 2008
AB Kurumları Veri Koruma Tüzüğü, Madde 34 ve 49 ABAD, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 29 Haziran 2010	**AB hukukunun AB kurum ve kuruluşları tarafından ihlali**	

Genel bağlamda hukuk kurallarının, özel bağlamda ise veri öznelerinin haklarının etkinliği bu kural ve hakların uygulanabilmelerini sağlayacak olan uygun mekanizmaların varlığına önemli bir ölçüde bağlıdır. Avrupa veri koruma mevzuatına göre, veri öznesinin verilerini koruyabilmesi için ulusal hukuk tarafından yetkilendirilmiş olması gerekmektedir. Bağımsız denetim makamları da ulusal hukuk düzenleri tarafından kurulmalı, veri öznelerine haklarını kullanmalarında yardımcı olmalı ve kişisel verilerin işlenme süreçlerini denetlemelidirler. Ek olarak, AİHS ve Şart kapsamında güvence altına alınmış olan etkili bir yola başvurma hakkı, yargı yollarının herkese açık olmasını gerektirmektedir.

5.1. Veri öznelerinin hakları

Ana başlıklar

- Ulusal yasalar gereği herkes, veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme hakkına sahiptir.
- Veri özneleri ulusal mevzuat kapsamında aşağıdaki haklara da sahip olacaktır:

1) kendileriyle alakalı verileri işleyen herhangi bir veri sorumlusu üzerinden bu verilere erişebilme;
2) veriler doğru değil ise bunları işleyen veri sorumlusundan verilerin düzeltilmesini (veya gerekiyorsa kullanımının engellenmesini) talep etme;
3) veriler veri sorumlusu tarafından hukuka aykırı bir şekilde işleniyorsa, verilerin silinmesini veya kullanımının engellenmesini isteme.

- Ayrıca, veri öznelerinin aşağıdaki durumlarda veri sorumlularına itiraz hakkı bulunacaktır:

1) otomatik kararlara yönelik itiraz hakkı (yalnızca otomatik yollarla işlenmiş veriler kullanılarak verilen kararlar);
2) verilerin işlenmesinin orantısız sonuçlara yol açması durumunda işlemeye itiraz hakkı;
3) veriler doğrudan pazarlama amaçları için kullanılmasına itiraz hakkı.

5.1.1. Erişim hakkı

AB mevzuatı kapsamında, VK Direktifi madde 12, veri öznelerinin erişim hakkı kapsamında veri sorumlusundan "kendilerine ait verilerin işlenip işlenmediği konusunda teyit ve en azından işlemenin amaçlarına, işlenen verilerin kategorilerine, ve verilerin ifşa olunduğu veri alıcılarına

veya veri alıcısı kategorilerine dair bilgi alma" ve "verilerin eksik veya yanlış olması sebebiyle Direktif'in düzenlemeleriyle uyuşmayan nitelikteki verilerin düzeltilmesi, silinmesi veya kullanımının engellenmesi" haklarını da içeren unsurları barındırmaktadır. Ayrıca, verilerin işlenmesi Direktifin hükümleri ile uyumlu değilse verilerin düzeltilmesini ve engellenmesini kapsamaktadır.

AK mevzuatında, bu hakların aynıları bulunur ancak ulusal mevzuatla öngörülmeleri gerekmektedir. (108 Sayılı Sözleşme madde 8). Birçok AK tavsiye kararında, 'erişim' terimi kullanılmakta, erişim hakkının çeşitli yönleri anlatılmakta ve yukarıdaki paragrafta belirtilenle aynı biçimde ulusal hukuk düzenlerinde hayata geçirilmesi önerilmektedir.

108 Sayılı Sözleşme'nin 9. maddesi ve VK Direktifi'nin 13. maddesi uyarınca, bir veri sorumlusunun bir veri öznesi tarafından yapılan erişim talebine uyma yükümlülüğü başkalarının üstün nitelikteki yasal menfaatleri neticesinde sınırlandırılabilir. Üstün nitelikteki yasal menfaatler ulusal güvenlik, kamu güvenliği ve suçların kovuşturulması gibi kamu menfaatlerinden veya verilerin korunmasındaki çıkardan daha ağır basan özel menfaatlerden oluşabilir. Getirilecek istisna veya sınırlamaların her biri demokratik bir toplumda gerekli olmalı ve amaçla orantılı olmalıdır. Çok istisnasi durumlarda, örneğin tıbbi aciliyetler sebebiyle, veri öznesinin korunması için şeffaflığın sınırlanması gerekebilir; bu özellikle de bütün veri öznelerinin erişim hakkının sınırlandırılması bakımından söz konusu olabilir.

Verilerin yalnızca bilimsel araştırma veya istatistiksel amaçlarla işlendiği durumlarda, VK Direktifi, erişim hakkının ulusal mevzuatla sınırlanmasına müsaade etmektedir; ancak yeterli yasal güvencelerin sağlanması gerekmektedir. Özelikle, bu veri işlemesi kapsamında herhangi bir bireye yönelik özel tedbirlerin veya kararların alınmadığı ve "veri öznesinin gizliliğini ihlal edebilecek hiçbir riskin kesinlikle bulunmadığı" güvencelerinin sağlanması gerekmektedir.[176] 108 Sayılı Sözleşme madde 9(3) kapsamında da benzer hükümler yer almaktadır.

Kendi verilerine erişim hakkı

AK mevzuatı kapsamında, kendi verilerine erişim hakkı 108 Sayılı Sözleşmenin 8. maddesinde açıkça yer almıştır. AİHM birçok kararında kişinin, başkaları tarafından saklanan veya kullanılan verilerine erişim hakkının bulunduğunu ve bu hakkın özel hayata saygı gösterilmesi ihtiyacından doğduğunu ifade etmiştir.[177] 'Leander'[178] davasında ise AİHM, kamu kurumları tarafından saklanan kişisel verilere erişim hakkının bazı durumlarda sınırlanabileceğini kararlaştırmıştır.

AB mevzuatı kapsamında, kendi verilerine erişim hakkı VK Direktifi'nin 12. maddesinde ve temel bir hak olarak da Şart'ın 8(2) maddesinde düzenlenmiştir.

VK Direktifi madde 12(a) gereğince Üye Devletler, kişisel verilere ve bilgilere erişim hakkını her bir veri öznesine tanımak durumundadır. Özellikle, her veri öznesinin veri sorumlusundan kendisine ait verilerin işlenip işlenmediğine dair teyit alma ve en azından aşağıdaki unsurları içeren bir bilgi alma hakkı bulunmaktadır:

[176] VK Direktifi, Madde13 (2).

[177] AİHM, *Gaskin v. the United Kingdom*, No. 10454/83, 7 Temmuz 1989; AİHM, *Odièvre v. France* [GC], No. 42326/98, 13 Şubat 2003; AİHM, *K.H. and Others v. Slovakia*, No. 32881/04, 28 Nisan 2009; AİHM, *Godelli v. Italy*, No. 33783/09, 25 Eylül 2012.

[178] AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987.

- verilerin işlenme amaçları;
- işlenen verilerin kategorileri;
- hangi verilerin işlenme aşamasında oldukları;
- verilerin ifşa olunduğu veri alıcıları veya veri alıcısı kategorileri;
- işlenme aşamasındaki verilerin kaynağına dair elde bulunan her türlü bilgi;
- otomatik olarak alınan kararlar söz konusu ise, verilerin herhangi bir otomatik işleme tabi tutulması sırasında geçerli olan mantık.

Ulusal hukuk kapsamında veri sorumlusu tarafından verilmesi gereken ek bilgiler düzenlenebilir, örneğin işlemenin yasal dayanağına atıfta bulunulması şart koşulabilir.

Örnek: Kişi kendi verilerine erişerek, bu verilerin tam ve doğru olup olmadığını belirleyebilir. Bu sebeple, veri öznesinin işlenen verilerin kategorileriyle ve verilerin içeriğiyle alakalı bilgilendirilmesi bir gerekliliktir. Bu yüzden de veri sorumlusu, veri öznesine ismini, adresini, doğum tarihini ve ilgi alanlarını işlediğini söylemekle yetinemez. Bu bağlamda veri sorumlusu işlediği verilerin "isim: N.N.; bir adres: 1040 Viyana, Schwarzenbergplatz 11, Avusturya; doğum tarihi: 10.10.1974; ilgi alanı:(veri öznesinin beyanı uyarınca) klasik müzik" olduğunu veri öznesine ifşa etmek zorundadır. Yukarıda sayılan son unsur, ek olarak, verinin kaynağına dair de bilgi içermektedir.

İşlenme sürecinde olan verilere ve bunların kaynağına ilişkin bütün bilgilere dair bilgilendirmenin veri öznesine iletimi anlaşılabilir bir biçimde yapılmalıdır. Bu da veri sorumlusunun veri öznesine neyi işlediğiyle alakalı daha detaylı açıklamalar yapmasının gerekebileceği anlamına gelir. Örneğin bir erişim talebine cevap olarak yalnızca teknik kısaltmalara atıfta bulunulması veya tıbbi terimler kullanılması, sırf bu kısaltmalar veya terimler saklanıyor olsa bile, genellikle yeterli olmayacaktır.

Veri sorumlusu tarafından işlenen verilerin kaynağına dair elde bulunan bütün bilgilerin yapılacak bir erişim talebine verilecek cevap kapsamında iletilmesi gerekmektedir. Bu düzenleme dürüstlük ve hesap verilebilirlik ilkeleri ışığında değerlendirilmelidir. Bir veri sorumlusu, ifşa sorumluluğundan kurtulmak adına verilerin kaynağına dair bilgileri imha edemez veya kendi faaliyet alanlarında normal olarak kabul edilen standartları ve belgelendirme ihtiyaçlarını görmezden gelemez. İşlenen verilerin kaynağına dair gerekli belgelendirmenin yapılmaması, veri sorumlusunun erişim hakkı kapsamındaki yükümlülüklerini yerine getirmediği anlamına gelecektir.

Otomatik değerlendirmelerin söz konusu olduğu durumlarda, veri öznesinin değerlendirilmesi sırasında dikkate alınan o belirli kriter de dahil olmak üzere, değerlendirmenin genel mantığının açıklanması gerekmektedir.

VK Direktifi bilgiye erişim hakkının geçmişi kapsayıp kapsamadığına ve kapsıyorsa da geçmişteki hangi dönemi kapsadığına dair bir açıklık getirmemektedir. Bu bağlamda, ABAD'ın içtihatlarında belirtildiği üzere, kişinin kendi verilerine erişim hakkı süre sınırları yoluyla aşırı bir biçimde sınırlanamaz. Veri öznelerine geçmişteki veri işleme faaliyetleriyle alakalı olarak bilgi edinebilmeleri için de makul bir fırsat tanınmalıdır.

Örnek: **'Rijkeboer'**[179] davasında ABAD'a, VK Direktifi madde 12 uyarınca, bir bireyin kişisel verilerin alıcılarına veya alıcı kategorilerine ve verilerin içeriğine dair bilgilere erişim hakkının

[179] ABAD, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 Mayıs 2009.

erişim talebinin yapıldığı tarihten bir yıl öncesine kadar olan süreyle sınırlanıp sınırlanamayacağı sorulmuştur. ABAD, madde 12(a)'nın bu tür bir zaman sınırlamasına izin verip vermediğini belirlemek için ilgili maddeyi direktifin amaçları ışığında yorumlamaya karar vermiştir. Mahkeme, ilk olarak, veri öznesinin verileri düzelttirme, sildirme veya engelletme hakkını (Madde 12(b)) veya verinin ifşa olunduğu üçüncü kişilere düzeltme, silme veya engellemeye dair bildirimde bulunma hakkını (Madde 12(c)) kullanabilmesi için erişim hakkının gerekli olduğunu belirtmiştir. Erişim hakkı aynı zamanda veri öznesinin kişisel verilerinin işlenmesine itiraz hakkını (Madde 14) veya işleme sebebiyle zarara uğradığı durumlarda dava hakkını (Madde 22 ve 23) kullanabilmesi için de gereklidir.

Mahkeme, yukarıda atıfta bulunulan maddelerin uygulamada etkili olabilmesi için "söz konusu hak doğası gereği geçmişe de yöneliktir. Eğer bu şekilde olmaz ise, veri öznesi, yasa dışı veya yanlış olarak addedilen verileri düzelttirme, sildirme veya engelletme veya uğradığı zararlar için yasal yollara başvurma ve tazminata hak kazanma haklarını etkili bir şekilde kullanamayacaktır."

Verilerin düzeltilmesini, silinmesini ve engellenmesini isteme hakkı

Herkes, verilerinin doğruluğunu ve verilerin hukuka uygun işlenmesini denetlemek açısından kendisi ile ilgili verilere erişim hakkına sahip olmalıdır.[180] Bu ilkelere uygun olarak, veri özneleri, eğer verilerin yanlış veya eksik olması sebebiyle işlemenin direktif hükümlerine aykırı olarak yapıldığını düşünüyorlarsa, kendileri hakkında tutulan verilerin düzeltilmesini, silinmesini ve engellenmesini ulusal mevzuat kapsamında isteme hakkına sahiptir.[181]

Örnek: **'Cemalettin Canlı v. Türkiye'**[182] davasında AİHM, ceza yargılaması kapsamında sunulan hatalı polis raporu sebebiyle AİHS madde 8'in ihlal edildiğine karar vermiştir.

Başvuran yasa dışı örgüt üyeliği suçlamasıyla iki defa yargılanmış ancak hiçbir zaman suçlu bulunmamıştır. Başvuranın başka bir suçtan tutuklanıp yargılandığı bir davada emniyet mahkemeye "ek suçlara dair bilgilendirme formu" başlıklı bir rapor sunmuş ve bu raporlarda başvuranı iki ayrı yasa dışı örgütün üyesi olarak göstermiştir. Başvuranın bu raporla ve emniyet kayıtlarıyla alaklı düzeltme talepleri yerine getirilmemiştir. AİHM polis raporunda yer alan bilgilerin, yetkililer tarafından sistemli bir şekilde toplanmaları ve saklanmaları durumunda kamuya açık bilgilerin de 'özel hayat' kapsamına girmeleri mümkün olduğundan, AİHS'nin 8. maddesi kapsamında olduğuna karar vermiştir. Ayrıca, polis raporu yanlış bilgiler içermekte ve hazırlanma ve mahkemeye sunulma bakımından hukuka aykırı niteliktedir. Mahkeme madde 8'in ihlal edildiğini belirtmiştir.

Örnek: **'Segerstedt-Wiberg ve Diğerleri v. İsveç'**,[183] davasında başvuranlar birtakım liberal ve komünist siyasi partiler ile ilişkilendirilmişlerdir. Başvuranlar kendileri hakkındaki bilgilerin emniyet kayıtlarına girdiğinden şüphelenmişlerdir. AİHM bu bilgilerin saklanmasının hukuki dayanağının bulunduğuna ve meşru bir amaç kapsamında tutulduklarına ikna olmuştur. AİHM, bazı başvuranlar bakımından verilerin tutulmaya devam edilmesinin bu kişilerin özel hayatlarına yönelik orantısız bir müdahale olduğuna karar vermiştir. Örneğin Bay Schmid hakkında, gösteri yürüyüşlerinde polise şiddet yoluyla mukavemeti savunduğu iddiasını içeren

[180] VK Direktifi, Gerekçe 41.
[181] *A.e.,* Madde12 (b).
[182] AİHM, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 Kasım 2008, par. 33, 42 ve 43; AİHM, *Dalea v. France,* No. 964/07, 2 Şubat 2010.
[183] AİHM, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 Haziran 2006, par. 89 ve 90; Bakınız, örneğin: AİHM, *M.K. v. France,* No. 19522/09, 18 Nisan 2013.

1969 yılına ait bir bilgi tutulmuştur. AİHM bu bilginin, özellikle de tarihi niteliği göz önüne alındığında, hiçbir ulusal güvenlik menfaatine yönelik olamayacağını ifade etmiştir. AİHM, beş başvurandan dördü bakımından AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

Bazı durumlarda, örneğin bir ismin yazılışının düzeltilmesinin, bir adresin veya telefon numarasının değiştirilmesinin veri öznesi tarafından talep edilmesi yeterli olacaktır. Ancak söz konusu taleplerin veri öznesinin yasal kişiliği veya yasal belgelerin tebligatı açısından doğru ikametgâh gibi yasal meselelere bağlı olması durumunda düzeltme talebinin yapılması yeterli olmayabilir ve veri sorumlusu iddia edilen yanlışlığa dair kanıt isteme yetkisine sahip olabilir. Bu tür istekler veri öznesinin sırtına makul olmayan bir ispat yükü yüklememeli ve veri öznelerinin verilerini düzelttirme haklarını kullanmaktan menetmemelidir. AİHM başvuranın gizli sicillerde tutulan bilgilerin doğruluğuna itiraz etme imkanının bulunmadığı birçok davada AİHS madde 8'in ihlal edildiğine karar vermiştir.[184]

Örnek: **'Ciubotaru v. Moldova'**[185] davasında başvuran, resmi kayıtlarda Moldovalı olarak kayıtlı gözüken etnik kökenini, iddiaya göre talebinin doğruluğunu kanıtlayamamaması sebebiyle, Romanyalı olarak değiştirmekte başarısız olmuştur. AİHM, Devletlerin bir bireyin etnik kimliğini kaydederken nesnel deliller talep etmelerini kabul edilebilir bulmuştur. Böyle bir iddianın tamamen öznel ve asılsız temellere dayandırılması durumunda yetkililer bu iddiayı reddedebilecektir. Ancak başvuranın iddiası etnik kökenine dair öznel bir algıdan çok daha fazlasına dayandırılmıştır; başvuran Romanyalı etknik grupla dil, isim, empati vb. nesnel olarak doğrulanabilir birçok bağlantıya sahip olduğunu ortaya koyabilmiştir. Ancak, ulusal mevzuat gereği başvuran ebeveynlerinin Romanyalı etnik grubuna ait olduğuna dair kanıt sunması gerekmiştir. Böyle bir şart, Moldova'nın tarihsel gerçekleri göz önüne alındığında, Sovyet yetkililerin başvuranın ebeveynleriyle alakalı olarak zamanında kaydettiği etnik kimlikten başka bir etnik kimliğin kaydedilebilmesinin önünde aşılamaz bir engel oluşturmuştur. Devlet, başvuranın iddiasının nesnel olarak doğrulanabilir kanıtlar ışığında incelenmesini engellediği için özel hayata etkili bir biçimde saygı gösterilmesini sağlama şeklindeki pozitif yükümlülüğünü yerine getirmemiştir. Mahkeme AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Verilerin doğru olup olmadığına ilişkin olarak bir kamu makamı nezdinde devam eden hukuk davaları veya işlemler sırasında, veri öznesi, verilerin doğruluğuna itiraz edildiği ve resmi kararın henüz verilmediğine ilişkin bir girişin veya notun veri dosyasına yerleştirilmesi talebinde bulunabilir. Bu süreçte veri sorumlusu verileri, özellikle de üçüncü kişilere, kesin veya nihai veri olarak sunmamalıdır.

Veri öznesinin, verilerin silinmesi veya değiştirilmesi yönündeki talebinin kaynağı sıklıkla veri işlemelerinin yasal bir dayanağa sahip olmadığı iddiasına dayanmaktadır. Bu tür talepler çoğu zaman rızanın geri çekildiği veya bazı verilere veri toplama amaçlarının gerçekleştirilmesi için artık ihtiyaç olmadığı durumlardan kaynaklanmaktadır. İşleme sürecinin meşruiyetinden sorumlu olması sebebiyle, verilerin işlenmesinin meşru olduğunu ispat yükü de veri sorumlusunun omuzlarındadır. Hesap verilebilirlik ilkesi uyarınca, veri sorumlusu verilerin işlenmesinin geçerli bir yasal dayanağı olduğunu herhangi bir zamanda gösterebilecek durumda olmalıdır, aksi takdirde işlemenin durdurulması gerekir.

[184] AİHM, *Rotaru v. Romania*, No. 28341/95, 4 Mayıs 2000.
[185] AİHM, *Ciubotaru v. Moldova*, No. 27138/04, 27 Nisan 2010, par. 51 ve 59.

Verilerin yanlış olduğu veya hukuka aykırı olarak işlendiği iddiasıyla işlemeye itiraz edilmesi durumunda, veri öznesi adil işleme ilkesi gereğince söz konusu verilerin kullanımının engellenmesini talep edebilecektir. Bu ise verilerin silinmediği, ancak veri sorumlusunun engelleme süresince bu verileri kullanmaktan kaçınması gerektiği anlamına gelmektedir. Yanlış veya hukuka aykırı olarak tutulan verilerin kullanımına devam edilmesinin veri öznesine zarar verebileceği durumlarda bu engel özellikle önem taşımaktadır. Ulusal hukuk verilerin kullanımının engellenmesine dair bir yükümlülüğün ne zaman oluşabileceğine ve bu engellemenin nasıl uygulanması gerektiğine dair detayları düzenlemelidir.

Veri öznelerinin, bunlara ek olarak, veri sorumlusunun, işleme faaliyetleri öncesinde söz konusu verileri alan üçüncü kişilere engelleme, düzeltme veya silinmeyle alakalı bildirimde bulunmasını sağlama hakları bulunmaktadır. Verilerin üçüncü kişilere ifşasının veri sorumlusu tarafından belgelendirilmesi gerektiği göz önüne alındığında, veri alıcılarının tespit edilmesinin ve silinmenin talep edilmesinin mümkün olacağı söylenebilir. Ancak veriler bu arada, örneğin internette, yayınlanmışsa veri alıcıları tam olarak bulunamayacağından bütün veri örneklerinin sildirilmesi imkânsız olabilir. VK Direktifi uyarınca, "bunu yapmanın imkânsız olduğu veya aşırı bir çaba gerektireceği ortaya çıkmadıkça" düzeltme, silme veya engelleme taleplerinin iletilmesi için veri alıcılarıyla iletişime geçilmesi zorunludur.[186]

5.1.2. İtiraz hakkı

İtiraz hakkı, otomatik kararlara yapılacak itiraz hakkını, veri öznesinin özel durumu sebebiyle itiraz hakkını ve verilerin doğrudan pazarlama amaçlarıyla kullanılmasına itiraz hakkını kapsamaktadır.

Otomatik kararlara itiraz hakkı

Otomatik kararlar, otomatik işleme tabi tutulmuş verilerin kullanılması yoluyla verilen kararlardır. Bu tür kararların, ilgili oldukları bireylerin hayatları üzerinde, örneğin bireylerin kredi notlarına, iş yeri performanslarına, davranış veya güvenilirliklerine ilişkin olmaları nedeniyle göz ardı edilemeyecek etkilere sebep olmaları ihtimali yüksekse, olumsuz sonuçların önüne geçilmesi için özel koruma tedbirlerinin alınması gerekmektedir. VK Direktifi, bireyler açısından önemli olan soruların otomatik kararlarla belirlenmemesi gerektiğini ve bireyin söz konusu otomatik kararı inceleme hakkına sahip olması gerektiğini öngörmektedir.[187]

Örnek: Otomatik kararlarla alakalı uygulamaya dair önemli bir örnek kredi derecelendirmesidir. Müstakbel bir müşterinin kredi notu hakkında hızlıca karar verebilmek için meslek, aile durumu vb. bazı veriler müşteriden toplanmakta ve müşteriyle alakalı olarak kredi bilgi sistemi gibi diğer kaynaklardan elde edilebilen bilgilerle birleştirilmektedir. Bu veriler müstakbel müşterinin kredi verilebilirliğini temsil eden ortalama bir değeri hesaplayan bir derecelendirme algoritmasına otomatik olarak aktarılır. Bu sayede şirket çalışanı veri öznesinin müşteri olarak kabul edilebilir olup olmadığını saniyeler içerisinde öğrenebilir.

Buna rağmen, VK Direktifi uyarınca Üye Devletler, bir kişinin otomatik bir karara tabi tutulmasının, ya ilgili otomatik kararın veri öznesinin lehine olması nedeniyle kişinin menfaatlerinin tehlikede olmadığı ya da kişinin menfaatlerinin başka uygun yollarla güvence

[186] VK Direktifi, Madde12 (c), son cümle.
[187] *A.e.*, Madde 15 (1).

altına alınmış olduğu hallerde mümkün olmasına izin vermelidir.[188] Profil Oluşturma Tavsiye Kararı'nda da görülebileceği üzere otomatik kararlara itiraz hakkı AK mevzuatında da yer almaktadır.[189]

Veri öznesinin özel durumu sebebiyle itiraz hakkı

Veri öznelerinin kendilerine ait verilerin işlenmesine itiraz edebileceklerini düzenleyen genel bir itiraz hakkı bulunmamaktadır.[190] Ancak VK Direktifi madde 14(a), veri öznesinin kendisine ilişkin özel durumlardan kaynaklanan mücbir yasal sebeplerle itiraz hakkının bulunduğunu öngörmektedir. Benzer bir hak AK Profil Oluşturma Tavsiye Kararı'nda da tanınmıştır.[191] Bu hükümler, veri öznesinin verilerinin korunmasındaki menfaatleri ile başkalarının veri öznesinin verilerinin işlenmesindeki meşru menfaatleri arasında bir denge kurmak amacıyla getirilmiştir.

Örnek: Bir banka kredi ödemelerinde temerrüde düşen müşterilerine ilişkin verileri yedi yıl süresince saklar. Bu veri tabanında yer alan bir müşteri, tekrar bir kredi talebinde bulunur. Veri tabanına bakılır, duruma ilişkin bir mali değerlendirme yapılır ve müşterinin kredi kullanamayacağına karar verilir. Ancak müşteri, kişisel verilerinin veri tabanına kaydedilmesine itiraz edebilir ve ödemede temerrüde düşmesinin konudan haberdar olması sonrasında düzelttirmiş olduğu bir hatadan kaynaklandığını ispat ederse verilerin silinmesini talep edebilir.

Başarılı bir itirazın sonucunda verilerin veri sorumlusu tarafından işlenmesine son verilebilir. Ancak, veri öznesinin itirazından önce gerçekleştirilmiş olan işleme faaliyetleri meşru kalmaya devam ederler.

Verilerin doğrudan pazarlama amaçları için kullanılmasına itiraz hakkı

VK Direktifi madde 14(b) verilerin doğrudan pazarlama amaçları için kullanılmasına itiraz hakkını düzenlemektedir. Bu hak aynı zamanda AK Doğrudan Pazarlama Tavsiye Kararı'nda da yer almaktadır.[192] Bu itiraz hakkı, veriler doğrudan pazarlama amacıyla üçüncü kişilere ifşa olunmadan önce kullanılmak üzere getirilmiştir. Bu sebeple de veri öznesine, verilerin aktarılması öncesinde önce itiraz imkanı tanınmalıdır.

[188] *A.e.,* Madde 15 (2).

[189] Profilleme Tüzüğü, Madde 5 (5).

[190] Bakınız AİHM, *M.S. v. Sweden*, No. 20837/92, 27 Ağustos 1997, tıbbi verilerin onay alınmadan veya itiraz hakkı tanınmadan iletildiği; veya AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987; veya AİHM, *Mosley v. the United Kingdom*, No. 48009/08, 10 Mayıs 2011.

[191] Profilleme Tüzüğü, Madde 5 (3).

[192] Avrupa Konseyi, Bakanlar Komitesi (1985), Rec(85)20 Sayılı, Doğrudan Pazarlama amacıyla kullanılan kişisel verilerin korunmasıyla ilgili Üye Devletlere yönelik Öneri, 25 Ekim 1985, Madde 4 (1).

5.2. Bağımsız denetim

- Verilerin etkili bir şekilde korunmasını sağlamak için ulusal hukuk tarafından bağımsız denetim makamları oluşturulmalıdır.
- Ulusal denetim makamları tamamen bağımsız hareket etmeliler ve bu bağımsızlık kurucu kanunları ile güvence altına alınmalı ve denetim makamının teşkilat yapısı da buna göre düzenlenmelidir.
- Denetim makamlarının belirli görevleri vardır; bunlardan bazıları şu şekildedir:

1) ulusal düzeyde veri korumasını denetlemek ve desteklemek;
2) veri öznelerine, veri sorumlularına, hükümetlere ve genel olarak kamuoyuna tavsiyelerde bulunmak;
3) yapılan şikayetleri dinlemek ve verilerin korunması hakkının ihlal edilmesiyle alakalı olarak veri öznelerine destek vermek;
4) veri sorumlarını ve veri işleyenleri denetlemek;
5) gerekmesi durumunda:
   *veri sorumlularını ve veri işleyenleri ikaz, ihtar veya cezalandırma yoluyla duruma müdahale etmek.
   *verilerin düzeltilmesini, engellenmesini veya silinmesini emretmek yoluyla müdahale etmek.
   *işlemeyi yasaklamak yoluyla müdahale etmek.
6) konuları mahkemeye sevk etmek.

VK Direktifi bağımsız denetimi, verilerin etkili bir şekilde korunmasını sağlayacak önemli bir mekanizma olarak değerlendirmektedir. Direktif, verilerin korunmasının sağlanması için 108 Sayılı Sözleşme'de veya OECD Gizlilik İlkeleri'nde ilk başta yer almamış olan bir aracı kullanıma sokmuştur.

Bağımsız denetimin etkili bir veri korumanın geliştirilmesi açısından vazgeçilmez olduğu anlaşıldığındanre, OECD Gizlilik İlkeleri'nin 2013 tarihinde kabul edilen gözden geçirilmiş halinde yer alan bir düzenlemede, Üye ülkere "gizliliğin uygulanmasına yönelik makamların, yetkilerini etkili bir biçimde kullanmalarını ve nesnel, tarafsız ve tutarlı bir biçimde kararlar vermelerini mümkün kılacak yönetim, kaynaklar ve teknik uzmanlık altyapısı sağlanarak kurulması ve kalıcı hale getirilmesi" çağrısında bulunulmuştur.[193]

AK mevzuatı kapsamında, 108 Sayılı Sözleşme'nin Ek Protokolü denetim makamlarının kurulmasını zorunlu hale getirmiştir. Söz konusu düzenlemenin 1. maddesinde, Taraf Devletlerin ulusal mevzuatlarına dahil etmeleri şart olan bağımsız denetim makamlarına dair yasal çerçeve belirlenmiştir. Anılan maddede, bu makamların görevlerini ve yetkilerini açıklarken, VK Direktifi'nde kullanılmış olan yapıların benzerlerine yer verilmiştir. Kural olarak, denetim makamları AB ve AK hukuku kapsamında aynı şekilde işlev göstermelidir.

AB mevzuatı kapsamında, denetim makamlarının yetkileri ve teşkilat yapıları ilk olarak VK Direktifi madde 28(1)'de belirlenmiştir. AB Kurumları Veri Koruma Tüzüğü[194] AB kurum ve kuruluşları tarafından yapılacak veri işlemeleriyle alakalı denetim makamı olarak EDPS'yi

[193] Ekonomik İş Birliği ve Kalkınma Örgütü (2013), *Kişisel verilerin korunması ve sınır ötesi akışlarının yönetilmesine ilişkin esaslar*, par. 19 (c).

[194] Kişisel verilerin Topluluk kurumları ve organları tarafından işlenmesiyle ilgili olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı hakkında 18 Aralık 2000 tarihli ve (AT) 45/2001 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü, OJ 2001 L 8, Madde 41–48.

belirlemiştir. Tüzük, bu denetim makamının görevlerini ve sorumluluklarını ortaya koyarken, VK Direktifi'nin yayınlanmasından bu yana edinilen tecrübelerden faydalanmaktadır.

Veri koruma makamlarının bağımsızlığı Avrupa Birliğinin İşleyişi Hakkında Antlaşma'nın 16(2) maddesi ve Şart'ın 8(3) maddesi kapsamında güvence altına alınmıştır. Özellikle de Şart'ın ilgili maddesi, bağımsız bir makam tarafından yapılacak denetimi verilerin korunmasına dair temel hakkın ana unsurlarından birisi olarak görmektedir. Ek olarak, VK Direktifi Üye Devletlere, direktifin uygulamasıyla alakalı gerekli denetimleri yürütecek olan tamamen bağımsız nitelikteki denetim makamlarını kurma görevi yüklemiştir.[195] Bağımsızlık yalnızca denetim makamının kuruluşuna dair kanunlar aracılığıyla değil, makamın teşkilat yapısının da bu bağımsızlığı sağlayacak şekilde oluşturulmasıyla güvence altına alınmalıdır.

ABAD, veri koruma denetim makamlarının sahip olması gereken bağımsızlığın kapsamına dair sorularla ilk kez 2010 yılında karşı karşıya gelmiştir. [196] Aşağıdaki örnekler Mahkemenin konuyla alakalı düşünecelerini sergilemektedir.

Örnek: **'Avrupa Komisyonu v. Almanya'[197]** davasında, Avrupa Komisyonu ABAD'dan, Almanya'nın veri korumasını sağlamakla yükümlü denetim makamlarının "tam bağımsızlığı" şartını iç hukukuna yanlış bir şekilde aktardığının ve böylece de VK Direktifi madde 28(1) kapsamındaki yükümlülüklerini yerine getirmediğinin ilan edilmesini talep etmiştir. Komisyon'un görüşüne göre sorun, Almanya'nın kişisel verilerin işlenmesini denetlemekle yükümlü ve kamu sektörü dışında yer alan farklı federe devletlerdeki (Länder) makamları Devlet'in gözetimi altına koymuş olmasıdır.

Mahkeme göre, davanın esasının değerlendirilebilmesi söz konusu hükümde yer alan bağımsızlık şartının kapsamına ve dolayısıyla da bu hükmün yorumlanmasına bağlıdır.

Mahkeme direktifin 28(1) maddesinde yer alan 'tam bağımsızlıkla' ibaresinin söz konusu hükmün lafzına ve VK Direktifi'nin amaçlarına ve sistemine dayanarak yorumlanması gerektiğinin altını çizmiştir.[198] Mahkeme, denetim makamlarının, direktifte güvence altına alınan kişisel verilerin işlenmesine dair hakların 'koruyucusu' olduğunu ve Üye Devletlerde bu makamların kurulmasının "kişisel verilerin işlenmesiyle alakalı olarak bireylerin korunmasında esaslı bir bileşen" oluşturduğunu vurgulamıştır.[199] Mahkeme, "denetim makamlarının görevlerini yerine getirirken nesnel ve tarafsız hareket etmeleri gerektiği"ni ifade etmiştir. Bu amaçla da yalnızca denetlenen kurumların değil, Federal veya Federe devletlerin de doğrudan veya dolaylı etkisi gibi dış etkilerden bağımsız olmaları gerekmektedir.[200]

Mahkeme ayrıca 'tam bağımsızlık' ibaresinin anlamının AB Kurumları Veri Koruma Tüzüğü'nde tanımlandığı şekliyle, EDPS'nin bağımsızlığı kavramı ışığında değerlendirilmesi gerektiği sonucuna varmıştır.[201] Mahkeme tarafından altı çizildiği üzere, madde 44(2) bağımsızlık kavramını açıklığa kavuşturmakta ve EPDS'nin, görevlerini yerine getirmesi sırasında hiçbir kişi veya kurumdan talimat bekleyemeyeceği ve alamayacağını eklemektedir.

[195] VK Direktifi, Madde 28 (1), son cümle; 108 Sayılı Sözleşme, Ek Protokol, Madde1 (3).

[196] Bakınız, Avrupa Birliği Temel Haklar Ajansı (2010), *Temel haklar: 2010 yıllındaki karşılaşılan zorluklar ve başarılar,* Annual report 2010, s. 59. Avrupa Birliği Temel Haklar Ajansı bu konuyu daha detaylı, mayıs 2010 yılında yayınlanmış olan *Avrupa Birliği'nde veri koruması: Ulusal Veri Koruma Makamlarının rolü* isimli raporunda işlemiştir.

[197] ABAD, C-518/07, *Avrupa Komisyonu v. Federal Republic of Germany*, 9 Mart 2010, par. 27.

[198] *A.e.*, par. 17 ve 29.

[199] *A.e.*, par. 23.

[200] *A.e.*, par. 25.

[201] *A.e.*, par. 27.

Bu da bağımsız bir veri koruma denetim makamının devlet tarafından denetlenmesi ihtimalini devre dışı bırakır.

Bu bağlamda, Mahkeme, devlet makamları dışındaki merciler tarafından gerçekleştirilen kişisel veri işlemelerini denetlemekle yükümlü federal devlet düzeyindeki Alman veri koruma kurumlarının yeterince bağımsız olmadıklarını çünkü devlet denetimine tabi olduklarını ifade etmiştir.

Örnek: **'Avrupa Komisyonu v. Avusturya'**[202] davasında da ABAD, Avusturya Veri Koruma Kurumu'nun (Veri Koruma Komisyonu, DSK) bazı üyelerinin ve çalışanlarının konumlarıyla alakalı olarak da benzer sorunlara işaret etmiştir. Mahkeme, Avusturya kanunlarının, Avusturya Veri Koruma Kurumu'nun görevlerini VK Direktifi bağlamında bir tam bağımsızlıkla yerine getirmesini engellediğine karar vermiştir. Avusturya Veri Koruma Kurumu'nun bağımsızlığının yeterince güvence altına alınmadığı çünkü Federal Şansölyeliğin kuruma iş gücü sağladığı, kurumu gözetim altında bulundurduğu ve kurumun faaliyetleriyle alakalı olarak her an bilgilendirilme hakkına sahip olduğu ifade edilmiştir.

Örnek: **'Avrupa Komisyonu v. Macaristan'**,[203] davasında ABAD, "her bir denetim makamının kendine verilen görevleri tamamen bağımsız olarak yerine getirmesini sağlama şartının […], Üye Devletlerin bu makama, öngörülen görev süresinin tamamı boyunca hizmet vermesi için izin verme yükümlülüğünü de beraberinde getireceğini" belirtmiştir. Mahkeme ayrıca "denetim makamının görev süresinin kişisel verilerin korunması amacıyla sona erme tarihinden önce sonlandırılması sebebiyle Macaristan'ın, VK Direktifi kapsamındaki […] yükümlülüklerini ihlal ettiğine karar vermiştir.

Denetim makamlarına, ulusal hukuk kapsamında aşağıdaki görev ve yetkiler verilmiştir:[204]

- veri sorumlularına ve veri öznelerine veri korumayla alakalı her hürlü konuda tavsiyelerde bulunmak;
- işleme faaliyetlerini soruşturmak ve buna uygun olarak müdahale etmek;
- veri sorumlularını ikaz veya ihtar etmek;
- verilerin düzeltilmesini, engellenmesini, silinmesini veya imha edilmesini emretmek;
- işleme faaliyetine yönelik geçici veya kalıcı yasaklar koymak;
- konuları mahkemeye sevk etmek.

Bir denetim makamının, işlevlerini gerçekleştirebilmesi için bir soruşturma kapsamında gerekli olan bütün kişisel verilere, bilgilere ve veri sorumlusunun söz konusu bilgileri tuttuğu bütün tesislere erişimi olmalıdır.

Bir denetim kurumunun verdiği kararların sürecine ve yasal etkilerine dair ulusal yargı düzenleri arasında gözle görülür farklılıklar bulunmaktadır. Ombudsman benzeri tavsiye kararlarından tutun, doğrudan uygulanabilir nitelikte kararlara kadar farklı şekillerde ele alınmaktadır denetim kurumlarının kararları. Bu nedenle, bir yargı düzeni içerisinde yer alan kanun yollarının etkililiği değerlendirilirken, kanun yolları kendi bağlamları içerisinde ele alınmalıdır.

[202] ABAD, C-614/10, *Avrupa Komisyonu v. Republic of Austria*, 16 Ekim 2012, par. 59 ve 63.
[203] ABAD, C-288/12, *Avrupa Komisyonu v. Hungary*, 8 Nisan 2014, par. 50 ve 67.
[204] VK Direktifi, Madde 28; Bakınız 108 Sayılı Sözleşme, Ek Protokol, Madde 1.

5.3. Kanun yolları ve yaptırımlar

- 108 Sayılı Sözleşme ve VK Direktifi uyarınca, ulusal hukuk verilerin korunmasına hakkına yönelik ihlallere karşı gerekli kanun yolları ve yaptırımları düzenlemelidir.
- AB hukuku bağlamında etkili başvuru hakkı, bir denetim makamına başvuru imkanından bağımsız olarak ulusal hukukun, veri koruma haklarının ihlallerine yönelik kanun yollarını düzenlemesini gerektirmektedir.
- Yaptırımlar, ulusal hukuk ile belirlenmeli ve etkili, eşdeğer, orantılı ve caydırıcı olmalılar.
- Kişi, mahkemeye gitmeden önce veri sorumlusuna başvurmalıdır. Mahkemeye gitmeden önce bir denetim makamına başvuruda bulunmanın zorunlu olup olmadığı hususu ulusal mevzuatın takdirine bırakılmıştır.
- Veri özneleri, son bir çare olarak ve belirli şartlar altında, veri koruma hukuku ihlallerini ABAD'ın önüne getirebilirler.
- Ek olarak, veri öznelerinin de çok sınırlı bir kapsamda olmak üzere doğrudan ABAD'a başvuru imkanları vardır.

Veri koruma mevzuatı kapsamındaki haklar ancak hak sahipleri tarafından kullanılabilir; bu da veri öznesi olan veya en azından olduğunu iddia eden birisi olacaktır. Bu kişiler haklarını kullanırlarken, ulusal hukuk kapsamında öngörülen şartları sağlayan kişiler tarafından temsil edilebilirler. Küçükler, ebeveynleri veya vasileri tarafından temsil edilmek zorundadırlar. Bir kişi, denetim makamları önünde, veri koruma haklarını desteklemek amacıyla kurulmuş dernekler tarafından da temsil edilebilir.

5.3.1. Veri sorumlusuna yapılan talep

Bölüm 3.2'de değinilmiş olan haklar öncelikle veri sorumlusuna karşı öne sürülmelidir. Doğrudan ulusal denetim makamına veya bir mahkemeye başvurmanın da bir yararı olmayacaktır çünkü bu durumda denetim makamının tek yapabileceği şey ilk aşamada veri sorumlusuna başvurulması gerektiği tavsiyesinde bulunmak olacaktır; mahkeme ise başvuruyu kabul edilemez olarak değerlendirebilecektir. Bir veri sorumlusuna yapılacak yasal bir talepte resmi olarak bulunması gereken koşullar, özellikle de bu talebin yazılı olarak yapılıp yapılmayacağı hususu ulusal hukukla düzenlemelidir.

Veri sorumlusu sıfatıyla kendisine başvuru yapılan birim, veri sorumlusu olmasa da bu talebe bir cevap vermelidir. Talepte bulunanla alakalı hiçbir verinin işlenmediği şeklindeki cevap da dahil olmak üzere bir cevap her koşulda ulusal mevzuat ile öngörülmüş olan süre içerisinde veri öznesine iletilmelidir. VK Direktifi madde 12(a) ve 108 Sayılı Sözleşme madde 8(b) uyarınca talep, 'aşırı bir gecikme olmaksızın' ele alınmalıdır. Bu sebeple, ulusal hukuk, veri sorumlusunun talebi uygun şekilde ele almasına yetecek kadar uzun olmak kaydıyla, yeterince kısa bir cevap süresi belirlemelidir.

Talebe cevap vermeden önce veri sorumlusu talepte bulunanın gerçekten belirttiği kişi olup olmadığını tespit etmeli ve böylece ciddi bir gizlilik ihlalinin önüne geçmelidir. Kimliğin tespitine dair gerekliliklerin ulusal mevzuat tarafından düzenlenmediği hallerde veri sorumlusu bu şartlara kendisi karar vermelidir. Ancak adil işleme ilkesi gereği, veri sorumluları kimlik tespiti (ve Bölüm 2.1.1'de tartışıldığı üzere, talebin güvenilirliği) için gerektiğinden fazla zorlayıcı şartlar getirmemelidir.

Ulusal hukuk ayrıca veri sorumlularının talepleri incelemeye almadan önce talepte bulunandan bir ödeme isteyip isteyemeyeceklerini düzenlemelidir: VK Direktifi madde 12(a) ve 108 Sayılı Sözleşme madde 8(b) uyarınca talepler 'aşırı bir […] masraf gerektirmeyecek şekilde' karşılanmalıdır. Birçok Avrupa ülkesinin ulusal hukukunda veri koruma mevzuatı kapsamında yapılan taleplerin, aşırı ve olağan dışı bir çaba gösterilmesini gerektirmedikçe, ücretsiz olarak karşılanması gerektiği düzenlenmiştir; buna karşılık, veri sorumluları da genellikle, taleplere cevap alma hakkının kötüye kullanımına karşı ulusal hukuk düzenleri tarafından korunmaktadır.

Veri sorumlusu olarak kendisine talepte bulunulan kişi, kurum veya merci veri sorumlusu olduğunu inkâr etmiyorsa, ulusal hukuk tarafından öngörülen süre içerisinde:

- talebi kabul etmek ve talebin gereğinin nasıl yerine getirildiğine dair talepte bulunana bilgi vermeli; veya
- talebin gereğinin neden yerine getirilmeyeceğine dair talepte bulunanı bilgilendirmeli.

5.3.2. Denetim makamlarına yapılmış olan şikayetler

Bir erişim talebinde bulunan veya bir veri sorumlusuna itiraz eden kişi gerekli süre içerisinde tatmin edici bir cevap alamazsa ulusal veri koruma denetim makamına destek talebiyle başvurabilir. Denetim makamı nezdindeki prosedürler sırasında, talepte bulunan tarafından iletişime geçilen kişi, kurum veya mercinin talebe cevap verme zorunluluğunun bulunup bulunmadığı ve verilen cevabın doğru ve yeterli olup olmadığı açıklığa kavuşturulmalıdır. Denetim makamı başvuru kapsamında verdiği kararla alakalı olarak başvuru sahibini bilgilendirmelidir.[205] Denetim makamları nezdindeki prosedürlerin sonuçlarının yasal etkileri ulusal hukuktaki düzenlemelere bağlıdır: örneğin makamın kararlarının yasal olarak uygulanabilir, yani resmi makamlar tarafından icra edilebilir olup olmadığı, veya veri sorumlusunun denetim makamının kararlarını (görüş, ihtar, vs.) yerine getirmemesi durumunda bir mahkemeye başvurmanın gerekli olup olmadığı vb. hususlar ulusal hukuk tarafından düzenlenmelidir.

ABİHA madde 16 ile güvence altına alınmış olan veri koruma haklarının AB kurumları veya kuruluşları tarafından ihlal edildiğinin iddia edilmesi durumunda, veri öznesi, EDPS'nin görev ve yetkilerini düzenleyen AB Kurumları Veri Koruma Tüzüğü uyarınca bağımsız bir veri koruma denetim makamı olarak öngörülen EDPS'ye[206] başvuruda bulunabilir. EDPS 6 ay içinde bu başvuruya cevap vermezse, şikâyet reddedilmiş olarak kabul edilir.

Ulusal denetim makamları tarafından verilen kararlara karşı mahkemeler nezdinde itiraz yolu açıktır. Bu yol veri özneleri için olduğu kadar, bir denetim makamı önündeki işlemenin taraflardan birisi olan veri sorumluları açısından da geçerlidir.

Örnek: Birleşik Krallık Bilgi Komiseri, 24 Temmuz 2013 tarihinde, Herfordshire polisi tarafından kullanılmakta olan araç plakası takip sisteminin hukuka aykırı olduğuna ve ilgili birimin bu sistemi kullanmayı durdurması gerektiğine dair bir karar verdi. Kameralar tarafından toplanan veriler hem yerel polis kayıtlarında hem de merkezi veri tabanında saklanmaktaydı. Plaka fotoğrafları iki yıl, arabaların fotoğrafları ise doksan gün boyunca tutulmaktaydı.

[205] VK Direktifi, Madde 28 (4).

[206] *Kişisel verilerin Topluluk kurumları ve organları tarafından işlenmesiyle ilgili olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı hakkında 18 Aralık 2000 tarihli ve (AT) 45/2001 Sayılı Avrupa Parlamentosu ve Konsey Tüzüğü,* OJ 2001 L 8.

Kameraların ve diğer gözetleme biçimlerinin böylesine yoğun bir şekilde kullanımının çözülmesi amaçlanan sorun ile orantısız olduğuna karar verildi.

5.3.3. Mahkemeye yapılmış olan şikayetler

VK Direktifi uyarınca, veri koruma mevzuatı kapsamında bir veri sorumlusundan talepte bulunan kişi veri sorumlusunun cevabından memnun kalmazsa, ulusal mahkemelere şikâyet hakkına sahip olmalıdır.[207]

Mahkemeye başvurmadan önce denetim makamlarına başvurulması gerekip gerekmediği hususu ulusal yasalar ile düzenlenmesi gereken bir alan olarak bırakılmıştır. Çoğu durumda, veri koruma haklarını kullanmak isteyen kişiler açısından ilk olarak denetim makamlarına başvurulması, bu makamlarda işletilen prosedür bürokratik olmayacağından ve ücretsiz olacağından, daha avantajlı olacaktır. Denetim makamının kararında (görüşünde, ihtarında, vs.) yer alacak olan uzman görüşler veri öznesinin hakkını mahkemeler önünde takibi sırasında da yararlı olabilecektir.

AK mevzuatı kapsamında, AİHS'ye Akit Taraflardan birisinin veri koruma haklarına yönelik olarak ulusal düzeyde gerçekleştirdiği iddia edilen ve aynı zamanda AİHS'nin 8. maddesine de tecavüz eden ihlallerin, iç hukuk yollarının tüketilmesini takiben AİHM önüne getirilebilmesi mümkündür. AİHS'nin 8. maddesinin ihlal edildiğine dair AİHM nezdinde ileri sürülecek bir iddianın dinlenebilir olması için başka kriterler de bulunmaktadır (AİHS madde 34-37).[208]

AİHM'ye yapılacak başvurular yalnızca Akit Taraflara yöneltilebilecek olmasına karşın, Akit Taraflardan birisinin ulusal hukukunda yer alan veri koruma haklarının ihlaline yönelik yeterli korumayı sağlayamayarak AİHS kapsamındaki pozitif yükümlülüklerini yerine getirmemesi durumunda özel hukuk kişilerinin eylem ve ihmalleri de bu başvurular kapsamında dolaylı olarak ele alınabilir.

Örnek: **'K.U. v. Finlanda'**,[209] davasında başvuran, ergin olmayan bir çocuk, bir çöpçatanlık sitesinde kendisine ilişkin olarak cinsel içerikli bir ilan yayınlandığı şikayetinde bulunmuştur. Bu ilanı yayınlayan kişinin kimliği hizmet sağlayıcı tarafından açıklanmamıştır çünkü Fin hukuku gereği hizmet sağlayıcının gizlilik yükümlülüğü bulunmaktadır. Başvuran, Fin hukukunun, kendisini töhmet altında bırakan verilerin bir gerçek kişi tarafından internete yüklenmesine yönelik olarak yeterli korumayı sağlamadığını iddia etmiştir. AİHM, devletlerin, bireylerin özel hayatlarına yönelik keyfi müdahalelerden kaçınma zorunlulukları yanında, "bireylerin birbirleri arasındaki ilişkiler kapsamında bile olsa özel hayata saygı gösterilmesini sağlamak üzere tasarlanmış önlemleri almak" gibi pozitif yükümlülükleri de olabileceğini ifade etmiştir. Başvuranın durumunda, pratik ve etkili bir korumanın sağlanabilmesi için failin kimliğinin tespiti ve kovuşturulması için gerekli adımların atılması gerekirdi. Bu koruma devlet tarafından sağlanmamıştır ve Mahkeme AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Örnek: **'Köpke v. Almanya'**,[210] davasında başvuran iş yerinde hırsızlık yaptığı şüphesiyle gizli kamera yoluyla gözetlenmiştir. AİHM, "ulusal makamların, başvuranın AİHS 8. madde kapsamındaki özel hayatına saygı gösterilmesi hakkı ile işvereninin mülkiyet haklarını

[207] VK Direktifi, Madde 22.
[208] AİHS, Madde 34–37, bakınız: www.echr.coe.int/Pages/home.aspx?p=caselaw/ analysis&c=#n1347458601286_pointer.
[209] AİHM, *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008.
[210] AİHM, *Köpke v. Germany* (dec.), No. 420/07, 5 Ekim 2010.

korumaktaki çıkarları ve adaletin sağlanmasındaki kamu yararı arasında bir denge kuramadığını gösterecek herhangi bir emare bulunmadığına" hükmetmiştir. Bu sebeple de başvurunun kabul edilemez olduğu ilan edilmiştir.

AİHM, Üye Devletin AİHS kapsamında güvence altına alınmış olan haklardan herhangi birisini ihlal ettiği kanaatine varırsa, Üye Devlet AİHM'nin kararını uygulamak zorundadır. Uygulama tedbirleri ilk olarak ihlale bir son vermeli ve ihlalin başvuran açısından doğurduğu olumsuz sonuçları olabildiğince telafi etmelidir. Kararların yerine getirilmesi ayrıca AİHM'nin tespit ettiğine benzer nitelikteki ihlallerin önlenmesine yönelik, mevzuat değişikliği, içtihat veya diğer şekillerde alınacak genel tedbirleri de gerektirebilir.

AİHM'nin AİHS'ye bir aykırılık tespit etmesi durumunda, AİHS'nin 41. maddesi, başvuranın zararlarının hakkaniyete uygun bir biçimde Taraf Devlet tarafından karşılanmasına hükmedilebileceğini düzenlemektedir.

AB mevzuatı uyarınca,[211] AB veri koruma hukukunu yürürlüğe koyan ulusal veri koruma mevzuatı ihlallerinin mağdurları, bazı durumlarda ABAD'a başvuruda bulunabilirler. Bir veri öznesinin veri koruma haklarının ihlal edildiğine dair iddiasının ABAD nezdinde bir sürece nasıl dönüşebileceğine dair iki olası senaryo vardır.

İlk senaryoya göre, veri öznesi, verilerin korunması hakkını ihlal eden bir AB idari veya düzenleyici yasasının doğrudan mağduru olmalıdır. ABİDA madde 263(4) gereğince:

'Her gerçek veya tüzel kişi, […] muhatabı olduğu veya kendisini doğrudan ve bireysel olarak ilgilendiren tasarruflar ile kendisini doğrudan ilgilendiren ve uygulama tedbirleri alınmasını gerektirmeyen düzenleyici tasarruflara karşı dava açabilir'.

Bu durumda, bir AB kurumu tarafından verileri hukuka aykırı olarak işlenen kişiler doğrudan ABAD'ın AB Kurumları Veri Koruma Tüzüğü ile alakalı konularda karar vermeye yetkili birimi olan Genel Mahkeme'ye başvurabilirler. Bir kişinin yasal durumunun bir AB yasal hükmü tarafından doğrudan etkilenmesi durumunda da ABAD'a doğrudan başvuru imkanı bulunmaktadır.

İkinci senaryo ABAD'ın ABİDA'nın 267. maddesi uyarınca ön karar verme yetkisiyle alakalıdır.

Veri özneleri, ulusal mahkemeler önünde görülen davalar sırasında ilgili mahkemeden, AB Antlaşmaları'nın ve AB kurumlarının, kuruluşlarının, ofislerinin veya ajanslarının eylemlerinin geçerliliğine dair ABAD'ın yorumunun talep edilmesini isteyebilir. ABAD'ın bu talep üzerine yaptığı açıklamalar ön karar olarak bilinmektedir. Bu yol şikâyet sahibi açısından doğrudan başvurulabilecek bir kanun yolu değildir ancak ulusal mahkemelerin AB mevzuatını doğru bir şekilde yorumladıklarından emin olmalarını sağlamaktadır.

Ulusal mahkemeler önünde görülen bir davanın taraflarından birisi ABAD'a bir soru yöneltilmesini talep ederse, yalnızca kararlarına karşı kanun yolları kapalı olan temyiz mercileri bu talebe uymakla yükümlüdürler.

[211] AB (2007), Avrupa Birliği Antlaşmasını ve Avrupa topluluklarını Kuran Antlaşmaları tadil eden Lisbon Antlaşması, Lisbon'da imzalanmış, 13 Aralık 2007, OJ 2007 C 306. Bakınız, konsolide metinler Avrupa Birliği Antlaşması, OJ 2012 C 326 ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, OJ 2012 C 326.

Örnek: **'Kartner Landesregierung ve Diğerleri' davasında**,[212] Avusturya Anayasa Mahkemesi, Şart'ın 7, 9 ve 11. maddeleri ışığında 2006/24/EC sayılı direktifin (Veri Saklama Direktifi) 3. ve 9. maddelerinin geçerliliğine ve Veri Saklama Direktifi'ni iç hukuka aktaran Telekomünikasyona İlişkin Avusturya Federal Yasası'nın VK Direktifi'nin ve AB Kurumları Veri Koruma Tüzüğü'nün bazı yönleriyle çelişip çelişmediğine dair sorular yönlendirmiştir ABAD'a.

Anayasa Mahkemesi önündeki davanın taraflarından birisi olan Bay Seitlinger, telefonu, interneti ve elektronik postayı hem iş hem de özel amaçlı olarak kullandığını ifade etmiştir. Sonuç olarak, gönderdiği ve aldığı veriler kamuya açık telekomünikasyon şebekeleri üzerinden geçmektedir. 2003 tarihli Avusturya Telekomünikasyon Yasası uyarınca, başvuranın telekomünikasyon hizmet sağlayıcısı başvuranın şebekeyi kullanımına dair verileri toplamak ve saklamakla yasal olarak yükümlüdür. Bay Seitlinger, kendisine ait kişisel verilerin saklanmasının bir bilginin şebeke üzerinde A kişisinden B kişisine aktarılması şeklindeki teknik amacı gerkçekleştirmek için hiçbir şekilde gerekli olmadığını fark etmiştir. Ayrıca bu tür bilgilerin toplanması ve saklanması faturalandırma amacı için de hiçbir şekilde gerekli olamayacaktır. Bay Seitlinger kişisel verilerinin işlenmesine kesinlikle rıza göstermemiştir. Bütün bu ekstra verilerin toplanıp saklanmasının tek sebebi 2003 tarihli Avusturya Telekomünikasyon Yasası'dır.

Bu sebeple Bay Seitlinger Avusturya Anayasa Mahkemesi'ne başvuruda bulunmuş ve müşterisi olduğu telekomünikasyon hizmet sağlayıcısı için öngörülen yasal zorunlulukların kendisinin Şart'ın 8. maddesi kapsamında korunan temel haklarını ihlal ettiği iddiasında bulunmuştur.

ABAD yalnızca, kendisine yöneltilen ön karar talebinin temelini oluşturan unsurlar hakkında karar verebilir. Davanın esasına karar verme yetkisi halen ulusal mahkemededir.

Prensip olarak, ABAD kendisine yöneltilen soruları yanıtlamakla yükümlüdür. Vereceği kararın yerinde olmayacağı veya esas dava ile aynı zamanda sonuçlandırılamayacağı gerekçesiyle ön karar vermeyi reddedemez. Ancak, soru yetki alanı dışında kalıyorsa ön karar vermeyi reddedebilir.

Sonuç olarak, ABİHA madde 16 kapsamında güvence altına alınmış olan veri koruma hakları, bir AB kurum veya kuruluşu tarafından kişisel verilerin işlenmesi sırasında ihlal edilirse veri öznesi konuyu ABAD Genel Mahkeme'ye taşıyabilir (AB Kurumları Veri Koruma Tüzüğü madde 32(1) ve (4)). Aynı durum EDPS'in bu tür ihlallere sebep olan kararları için de geçerlidir (AB Kurumları Veri Koruma Tüzüğü madde 32(3)).

AB Kurumları Veri Koruma Tüzüğü kapsamındaki konularda karar verme yetkisi ABAD Genel Mahkeme'nindir ancak bir AB kurumu veya kuruluşunda personel olan birisi tarafından yapılacak başvuruların AB Kamu Personeli Mahkemesi'ne yapılması gerekmektedir.

Örnek: **Avrupa Komisyonu v. The Bavarian Lager Co. Ltd**[213] davasında, AB kurumlarının ve kuruluşlarının kararlarına ve faaliyetlerine karşı hangi yasal yollara başvurulabileceği anlatılmaktadır.

Bavarian Lager Avrupa Komisyonu'ndan, Komisyon tarafından düzenlenmiş olan bir

[212] ABAD, Birlikte Görülen C-293/12 ve C-594/12, *Digital Rights Ireland and Seitling and Others*, 8 Nisan 2014.
[213] ABAD, C-28/08 P, *Avrupa Komisyonu v. The Bavarian Lager Co. Ltd*, 29 Haziran 2010.

toplantıya ait ve şirketle alakalı bazı yasal sorunlara ilişkin olduğu iddia edilen tutanakların tamamına erişim talebinde bulunmuştur. Üstün gelen veri koruma menfaatlerinin varlığı sebebiyle Komisyon şirketin bu talebini reddetmiştir.[214] Bu karara karşı Bavarian Lager, AB Kurumları Veri Koruma Tüzüğü'nün 32. maddesini uygulayarak ABAD nezdinde, daha da açık olmak gerekirse İlk Derece Mahkemesi (Genel Mahkeme'nin o dönemdeki adı) nezdinde bir şikâyette bulunmuştur. İlk Derece Mahkemesi, T-194/04 sayılı Bavarian Lager v. Commission dosyasında verdiği karar kapsamında Komisyon'un erişim talebinin reddine ilişkin kararını iptal etmiştir. Avrupa Komisyonu bu kararı temyiz ederek ABAD'ın Adalet Divanı'na başvurmuştur. Adalet Divanı (Büyük Daire olarak) İlk Derece Mahkemesi'nin kararını bir kenara bırakarak Avrupa Komisyonu'nun erişim talebinin reddine dair kararını onamıştır.

5.3.4. Yaptırımlar

AK mevzuatı kapsamında, 108 Sayılı Sözleşme'nin 10. maddesi, 108 Sayılı Sözleşme'de belirlenen verilerin korunmasına dair temel ilkeleri iç hukukta yürürlüğe koyan hükümlerin ihlaline karşı uygun yaptırım ve kanun yollarının Taraflarca belirlenmesi gerektiğini öngörmektedir.[215] **AB mevzuatı kapsamında**, VK Direktifi madde 24 uyarınca Üye Devletler "bu Direktifin hükümlerinin tam olarak uygulanmasına yönelik uygun tedbirleri almalılar ve özelikle de benimsenen hükümlerin ihlali durumunda uygulanacak yaptırımları düzenlemelidirler […]".

Her iki hukuki düzenleme de Üye Devletlere uygun kanun yollarının ve yaptırımların seçiminde geniş bir takdir payı bırakmaktadır. Ne AK mevzuatı ne de AB mevzuatı hangi tür ve yapıda yaptırımların uygulanacağına dair bir yol göstermemekte, yaptırımlara ilişkin örnekler sunmamaktadır.

Ancak:

"Üye Devletler bireylerin AB hukuku kapsamındaki haklarının güvence altına alınması bakımından hangi tedbirlerin en uygunu olduğu konusunda bir takdir hakkına sahip olsalar da AB Antlaşması'nın 4(3) maddesinde yer alan dürüst işbirliği ilkesine uyarınca etkinlik, eş değerlik, orantılılık ve caydırıcılık şeklindeki asgari gerekliliklere saygı gösterilmesi gerekmektedir".[216]

ABAD ulusal hukukun yaptırımları belirlemekte tamamen özgür olmadığını birçok kez tekrarlamıştır.

Örnek: **'Von Colson ve Kamann v. Land Nordrhein-Westfalen'**[217] davasında ABAD, bir direktifin muhattabı olan bütün Üye Devletler'in, bu direktifin amaçlarına uygun ve tamamen geçerli olacak şekilde ulusal hukuk sistemleri içerisinde uygulanmasını sağlayacak gerekli bütün tedbirleri almakla yükümlü olduklarını ifade etmiştir. Mahkeme, direktifin uygulanmasını sağlayacak yol ve yöntemlerinin seçimi Üye Devletler'e bırakılmış olsa da bu

[214] Bakınız: Avrupa Veri Koruma Denetçisi tarafından yayınlanan (2011), 'Bavarian Lager' kararından sonra kişisel veriler içeren metinlere kamusal erişim hakkı, Brüksel: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_ Lager_EN.pdf.

[215] AİHM, *I. v. Finland*, No. 20511/03, 17 Temmuz 2008; AİHM, *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008.

[216] Avrupa Birliği Temel Haklar Ajansı (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, 2/2012, Vienna, 1 Ekim 2012, s. 27.

[217] ABAD, C-14/83, *Sabine von Kolson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10 Nisan 1984.

seçim hakkının Üye Devletler üzerindeki yükümlülüğü etkilemeyeceğini belirtmiştir. Özelikle, etkili bir hukuki başvuru, bireyin söz konusu hakkını aramasına ve tam anlam ve kapsamıyla uygulamasına imkân vermelidir. Bu gerçek ve etkili korumayı elde edebilmek için de kanun yollarının, caydırıcı etkiye sahip yaptırımları mümkün kılacak cezai ve/veya tazmine yönelik prosedürleri başlatması gerekmektedir.

AB hukukunun AB kurumları veya kuruluşları tarafından ihlal edilmesi durumunda uygulanacak yaptırımlarla alakalı olarak, AB Kurumları Veri Koruma Tüzüğü'nün getirdiği sınırlamadan dolayı yaptırımlar ancak disiplin cezası şeklinde tasarlanabilirler. Tüzüğün 49. maddesi uyarınca "bu Tüzük kapsamındaki yükümlülüklere kasten veya ihmal yoluyla uyulmaması halinde, Avrupa Topluluğu memurları veya diğer şekillerde hizmet verenler disiplin cezasına tabi tutulacaktır […]".

6. Sınır ötesi veri akışı

AB	İşlenen konular	AK
Sınır ötesi veri akışı		
Veri Koruma Direktifi, Madde 25 (1) ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003	**Tanım**	108 Sayılı Sözleşme, Ek Protokol, Madde 2 (1)
Verilerin serbest akışı		
Veri Koruma Direktifi, Madde 1(2)	**AB Üye Devletleri arasında**	
	108 Sayılı Sözleşmeye Üye Devletler arasında	108 Sayılı Sözleşme, Madde 12 (2)
Veri Koruma Direktifi, Madde 25	**Yeterli koruma seviyesine sahip üçüncü ülkelere**	108 Sayılı Sözleşme, Ek Protokol, Madde 2(1)
Veri Koruma Direktifi, Madde 26 (1)	**Özel durumlarda üçüncü ülkelere**	108 Sayılı Sözleşme, Ek Protokol, Madde 2 (2) (a)
Üçüncü devletlere yönelik sınırlandırılmış veri akışı		
Veri Koruma Direktifi, Madde 26 (2) Veri Koruma Direktifi, Madde 26 (4)	**Sözleşme maddeleri**	108 Sayılı Sözleşme, Ek Protokol, Madde 2 (2) (b) Sözleşme hükümlerinin hazırlanmasına yönelik rehber
Veri Koruma Direktifi, Madde 26 (2)	**Bağlayıcı şirket kuralları**	
Örnekler: EU–US PNR-Antlaşması EU–US SWIFT-Antlaşması	**Özel uluslararası antlaşmalar**	

VK Direktifi Üye Devletler arasındaki serbest veri akışını düzenlemenin yanında kişisel verilerin AB dışındaki üçüncü ülkelere aktarımı için gereken koşullara dair hükümler de içermektedir. AK de üçüncü ülkere sınır ötesi veri akışına dair kuralların belirlenmesinin önemini görmüş ve 108 Sayılı Sözleşme'ye Ek Protokol'ü 2001 yılında kabul etmiştir. Bu Protokol, sınır ötesi veri akışına yönelik olarak sözleşme taraflarında ve AB Üye Devletleri'ndeki mevzuat içerisinde bulunan ana düzenleyici özellikleri benimsemiştir.

6.1. Sınır ötesi veri akışının doğası

Ana başlıklar

- Sınır ötesi veri akışı, kişisel verilerin yabancı bir ülke mevzuatına tabi olan bir alıcıya aktarılmasıdır.

108 Sayılı Sözleşme'ye Ek Protokol 2(1) maddesi, sınır ötesi veri aktarımını kişisel verilerin yabancı bir ülke mevzuatına tabi olan bir alıcıya aktarılması şeklinde tanımlamaktadır. VK Direktifi madde 25(1) ise "işleme sürecinde olan veya aktarım sonrası işlenmesi planlanan kişisel verilerin üçüncü bir ülkeye aktarımını" kurala bağlamaktadır. Bu tür veri aktarımları ancak 108 Sayılı Sözleşme'ye Ek Protokol'un 2. maddesi ve AB Üye Devletleri için de buna ek olarak VK Direktifi'nin 25. ve 26. maddelerinde belirlenen kurallar dahilinde mümkündür.

Örnek: **'Bodil Lindqvist'**[218] davasında ABAD, Bir internet sitesinde çeşitli kişilere atıfta bulunma ve bu kişilerin kimliklerini ismen veya diğer yollarla, örneğin telefon numaralarını veya çalışma şartlarına veya hobilerine dair bilgiler vererek açık etmenin 95/46 sayılı Direktif'in 3. maddesinin 1. fıkrası kapsamında 'kişisel verilerin tamamen veya kısmen otomatik olarak işlenmesine' vücut verdiğini belirtmiştir.

Mahkeme, direktifin devamındaki düzenlemelerde, Üye Devletlerin kişisel verilerin üçüncü ülkelere aktarımını denetleyebilmesine imkân sağlayacak çeşitli kuralların yer aldığına işaret etmiştir.

Ancak internetin direktifin kaleme alındığı dönemdeki gelişim aşaması ve direktifte internetin kullanımına yönelik uygulanabilecek kriterlerin yokluğu dikkate alınarak, "Topluluk mevzuatındaki '[verilerin] üçüncü bir ülkeye aktarımı' ibaresinin, söz konusu veriler üçüncü bir ülkede bulunan ve bu verilere ulaşabilecek teknik imkanlara sahip kişilerin erişimine açılmış da olsa, verilerin bir internet sayfasında yüklenmesini kapsayacak şekilde kullanıldığı söylenemez."

Aksi takdirde, direktif "kişisel veriler bir internet sayfasında yüklendiği her an üçüncü bir ülkeye veri aktarımı olduğu şeklinde yorumlanacak olsaydı, bu aktarım söz konusu verilere erişmek için gerekli teknik imkanlara sahip üçüncü ülkelerin hepsine yapılmış bir aktarım olurdu. Böylece de [direktif tarafından] öngörülen özel rejim internet üzerindeki faaliyetlere ilişkin genel uygulamaya yönelik bir rejim haline gelirdi. Bu sebeple, Komisyon […] tek bir üçüncü ülkenin bile gerekli korumayı sağlamadığını tespit ederse, Üye Devletler herhangi bir kişisel verinin internete yüklenmesini engellemekle yükümlü olacaktır."

(Kişisel) verilerin sırf yayınlanmalarının sınır ötesi veri akışı olarak değerlendirilemeyeceği ilkesi çevrimiçi resmi siciller veya (elektronik) gazeteler ve televizyon gibi kitle iletişim araçları açısından da uygulama alanı bulacaktır. Yalnızca belirli alıcılara yönlendirilmiş olan iletişim, 'sınır ötesi veri akışı' kavramı için uygundur.

[218] ABAD, C-101/01, *Bodil Lindqvist*, 6 Kasım 2003, par. 27, 68 ve 69.

6.2. Üye Devletler veya Akit Taraflar arasındaki serbest veri akışı

- Kişisel verilerin EEA içerisindeki başka bir üye devlete veya 108 Sayılı Sözleşme'nin Akit Taraflarından başka birisine aktarımı sınırlamalardan muaf olmalıdır.

AK mevzuatı kapsamında, 108 Sayılı Sözleşme madde 12(2) uyarınca, sözleşmenin Tarafları arasında kişisel verilerin serbest bir biçimde akışı söz konusu olmalıdır. Ulusal hukuk kişisel verilerin başka bir Akit Tarafa gönderimini kural olarak sınırlayamaz. Ancak aşağıdaki durumlarda istisnai olarak sınırlama söz konusu olabilir:

- verinin özel yapısı bunu gerektiriyorsa;[219] veya
- bu sınırlandırma, üçüncü taraflara sınır ötesi veri akışı konusunda ulusal kanun hükümlerinin dolanılmasını önlemek için gerekliyse.[220]

AB mevzuatı kapsamında, Üye Devletler arasında verilerin serbest akışına yönelik olarak verilerin korunması amacıyla sınırlama ve yasak getirilmesi VK Direktifi'nin 1(2) maddesi uyarınca yasaklanmıştır. Verilerin serbest akışının geçerli olduğu alan İzlanda, Lihtenştayn ve Norveç'i iç pazara dahil eden Avrupa Ekonomik Alanı Antlaşması (EEA)[221] ile genişletilmiştir.

Örnek: Aralarında Slovenya ve Fransa'nın da bulunduğu birçok AB üye ülkesinde ofisleri bulunan bir uluslararası şirketler grubunun iştiraklerinden birisi kişisel verileri Slovenya'dan Fransa'ya aktarmaktaysa, bu veri akışının Slovenya ulusal hukuku tarafından sınırlanmaması ve yasaklanmaması gerekir.

Ancak aynı Slovenyalı iştirak, bu kişisel verileri ABD'de yerleşik olan ana şirkete aktarmak isterse, Slovenyalı veri aktarıcısı, ana şirket yeterli veri koruma seviyesi sağlamaya yönelik ve gönüllü katılım esasına dayalı bir Davranış Kuralları düzenlemesi olan Güvenli Liman Gizlilik İlkeleri'ni imzalamamışsa, yeterli veri koruması bulunmayan üçüncü ülkere yapılacak sınır ötesi veri aktarımlarına dair mevzuat kapsamında öngörülen prosedürü işletmek durumundadır. (Bkz. Bölüm 6.3.1.)

EEA Üye Devletleri'ne iç pazarın kapsamı dışındaki amaçlar için, örneğin suçların soruşturulması amacıyla sınır ötesi veri aktarımı yapılması durumunda, bu aktarımlar VK Direktifi'nin düzenlemelerine tabi değildir ve bu sebeple de verilerin serbest akışı ilkesinin uygulama alanına girmezler. AK mevzuatına gelirsek, bütün alanlar 108 Sayılı Sözleşme'nin ve 108 Sayılı Sözleşme'ye Ek Protokol'ün kapsamına girmektedir. Ancak Akit Taraflarca istisnalar öngörülebilir. Tüm EEA üyeleri aynı zamanda 108 sayılı Sözleşme'ye de Taraftır.

6.3. Üçüncü ülkelere serbest veri akışı

[219] 108 Sayılı Sözleşme, Madde12 (3) (a).
[220] *A.e.*, Madde12 (3) (b).
[221] Avrupa Topluluklarının Üye Devletleri ve Avusturya Cumhuriyeti, Finlandiya Cumhuriyeti, İzlanda Cumhuriyeti, Lihtenştayn Prensliği, Norveç Krallığı, İsveç Krallığı ve İsviçre Konfederasyonu arasındaki Avrupa Ekonomik Alanı içerisindeki Antlaşmaya ilişkin, 13 Aralık 1993 tarihli, Avrupa Birliği Konseyi ve Komisyon Kararı, OJ 1994 L 1.

Ana başlıklar

- Kişisel verilerin üçüncü ülkelere aktarımı aşağıdaki şartların gerçekleşmesi halinde ulusal veri koruma mevzuatı uyarınca sınırlamalardan muaf olacaktır:

1) veri alıcısının yeterli veri korumasına sahip olduğu doğrulanmışsa; veya
2) verilerin aktarılması veri öznesinin hususi menfaatleri veya başkalarının üstün meşru menfaatleri, özellikle de kamu menfaatleri için gerekliyse.

- Üçüncü bir ülkede verilerin yeterince korunması, verilerin korunmasına yönelik temel ilkelerin bu ülkenin ulusal hukukunda etkili şekilde uygulandığı anlamına gelmektedir.
- AB mevzuatı uyarınca, üçüncü bir ülkede verilerin yeterince korunduğunun tespitini Avrupa Komisyonu yapmaktadır. AK mevzuatı gereğince, yeterliliğin nasıl değerlendirileceği hususu ulusal hukuk tarafından düzenlenmelidir

6.3.1. Yeterli koruma sağlandığı için serbest veri akışı

AK Mevzuatı, sözleşmeye taraf olmayan devletler açısından da, eğer alıcı devlet veya kuruluş planlanan veri transferi için yeterli bir korumanın sağlanacağı güvencesini veriyorsa, verilerin serbest akışına ulusal mevzuat kapsamında izin verilebileceğini öngörmüştür.[222] Yabancı bir ülkedeki veri koruma seviyesinin nasıl ve kim tarafından değerlendirilmesi gerektiğine karar verecek olan ulusal hukuktur.

AB Mevzuatı kapsamında, yeterli koruma sağlayan bir üçüncü ülkeye serbest veri akışı VK Direktifi'nin 25(1) maddesinde düzenlenmiştir. Eşdeğerlik yerine yeterlilik şartının aranması sayesinde farklı veri koruma yöntemlerinin kabulü de mümkün olmuştur. VK Direktifi'nin 25(6) maddesi uyarınca Avrupa Komisyonu yabancı ülkelerin veri koruma yeterlilik seviyelerini yeterlilik tespitleri yoluyla belirleme konusunda yetkilidir ve bu tespiti yaparken de 25. ve 26. maddenin yorumlanmasına esaslı katkıları bulunan Madde 29 Çalışma Kurultayı'na danışarak ilerlemektedir.[223]

Avrupa Komisyonu tarafından verilen bir yeterlilik tespiti hukuken bağlayıcıdır. Belirli bir ülkenin yeterli olduğuna dair Avrupa Komisyonu tarafından Avrupa Birliği Resmî Gazetesi'nde bir tespit yayınlanırsa, bütün EEA üye ülkeleri ve onların kurumları bu karara uymakla yükümlüdür. Bu da ulusal makamlar önünde herhangi bir kontrol veya lisans prosedürü işletilmesine gerek olmaksızın veri akışının gerçekleşebileceği anlamına gelir.[224]

Avrupa Komisyonu'nun bir ülkenin yasal sisteminin parçalarını değerlendirmesi veya değerlendirme kapsamını belirli bir konuyla sınırlaması mümkündür. Örneğin, Komisyon Kanada'nın yalnızca ticaret mevzuatına yönelik bir yeterlilik tespiti yapmıştır.[225] Aynı şekilde

[222] 108 Sayılı Sözleşme, Ek Protokol, Madde 2 (1).

[223] Örneğin, Madde 29 Çalışma Kurultayı (2003), *Üçüncü ülkelere kişisel verilerin aktarılmasına ilişkin Çalışma Belgesi: AB Veri Koruma Direktifi'nin 26(2). Maddesi'ne ilişkin Uluslararası Veri Aktarımına dair bağlayıcı kurumsal kuralların uygulanması,* WP 74, Brüksel, 3 Haziran 2003; ve Madde 29 Çalışma Kurultayı (2005), 95*/46/AB Sayılı Direktifin 26(1). maddesi'nin ortak anlayışına ilişkin Çalışma Metni, 24 Ekim 1995*, WP 114, Brüksel, 25 Kasım 2005.

[224] Yeterlilik bulgusu alan listelerin güncellenmiş listesi için lütfen Avrupa Komisyonu'nun Adalet Genel Müdürlüğü ana web sayfasına bakınız: http://ec.europa.eu/justice/ data-protection/document/international-transfers/adequacy/index_en.htm.

[225] Avrupa Komisyonu (2002), 95/46/AB Sayılı, Avrupa Birliği Parlamentosu ve Konseyi, Kanada Kişisel Bilgi Koruması ve

Komisyon, AB ve yabancı devletler arasında antlaşmalara dayalı aktarımlar için de birçok yeterlilik tespitinde bulunmuştur. Bu kararlar münhasıran tek bir veri aktarımı tipine, AB'den belirli bazı denizaşırı noktalara yapılan uçuşlarda yolcu isim kayıtlarının havayolu şirketleri tarafından yabancı sınır kontrol makamlarına aktarımına yöneliktir (Bkz. Bölüm 6.4.3.). AB ve üçüncü ülkeler arasındaki antlaşmalara dayalı olarak gerçekleştirilen veri aktarımlarına dair daha güncel uygulamada yeterlilik tespiti ihtiyacı ortadan kaldırılmakta ve antlaşmanın kendisinin yeterli bir veri koruması sağladığı varsayılmaktadır.[226]

En önemli yeterlilik kararlarından biri aslında birtakım yasal hükümlere dayalı değildir.[227] Bilakis, Güvenli Liman Gizlilik İlkeleri olarak bilinen Davranış Kuralları tarzındaki kurallar ile ilgilidir. Bu ilkeler ABD şirketlerine yönelik olarak AB ve ABD arasında yapılan görüşmeler kapsamında detaylı olarak düzenlenmiştir. Güvenli Liman üyeliği ABD Ticaret Bakanlığı nezdinde yapılacak bir gönüllü bağlılık beyanı ile gerçekleştirilmekte ve Bakanlık tarafından yayınlanan bir listede belgelendirilmektedir. Yeterliliğin en önemli unsurlarından birisi veri koruma uygulamalarının etkililiği olduğundan, Güvenli Liman Düzenlemesi aynı zamanda belirli bir ölçüye kadar devlet denetimi öngörmektedir: yalnızca ABD Federal Ticaret Komisyonu'nun denetimine tabi olan şirketler Güvenli Liman'a katılabilirler.

6.3.2. Özel durumlarda serbest veri akışı

AK mevzuatı kapsamında, 108 Sayılı Sözleşme'ye Ek Protokol madde 2(2) uyarınca, yeterli veri korumasının bulunmadığı üçüncü ülkelere kişisel veri aktarımına, söz konusu aktarım ulusal hukuk tarafından düzenlendiği ve aşağıdaki unsurlar bakımından gerekli olduğu sürece izin verilecektir:

- veri öznesinin özel menfaati için gerekliyse; veya
- başkalarının üstün nitelikteki meşru menfaatleri, özellikle de kamu menfaatleri için gerekliyse.

AB mevzuatı kapsamında, VK Direktifi madde 26(1), 108 sayılı Sözleşme'ye Ek Protokol ile benzer hükümler içermektedir.

Direktif uyarınca veri öznesinin menfaatleri, aşağıdaki koşulların gerçekleşmesi halinde üçüncü bir ülkeye serbest veri akışını haklı gösterebilecektir:

- veri öznesinin verilerin gönderimine yönelik açık rızası bulunmaktaysa; veya
- veri öznesi verilerin yurt dışındaki bir alıcıya aktarımını gerektirecek bir sözleşmesel ilişkiye girer -veya girmeye hazırlanırsa- ; veya
- veri sorumlusu ve bir üçüncü kişi arasında veri öznesinin menfaatlerine yönelik bir sözleşme yapılmışsa; veya
- veri aktarımı veri öznesinin hayati menfaatlerinin korunması için gerekliyse; veya

Elektronik Belgeler Yasası tarafından sağlanan kişisel verilerin korunması Direktifi kapsamında aldığı 2002/2/AB Sayılı Karar, 20 Aralık 2001, OJ 2002 L 2.

[226] Örneğin, Amerika Birleşik Devletleri ile Avrupa Birliği arasında, Amerika Birleşik Devletleri, Ulusal Güvenlik Departmanı tarafından Yolcu İsmi Kayıtlarının kullanılması ve aktarılmasına ilişkin Sözleşme (OJ 2012 L 215, s. 5–14) veya Amerika Birleşik Devletleri ile Avrupa Birliği arasında, Avrupa Birliğinden Amerika Birleşik Devletlerine Finansal Mesajlaşma Verilerinin, Terörist Mali İzleme Programı kapsamında işlenmesi ve aktarılmasına ilişkin Sözleşme, OJ 2010 L 8, s. 11–16.

[227] Avrupa Komisyonu, *2000/520/AB Sayılı, Avrupa Birliği Parlamentosu ve Konseyinin 95/46/AB Sayılı Direktifi uyarınca, güvenli liman gizlilik ilkelerinin ve ABD Ticaret Bakanlığı tarafından yayınlanan, konuyla ilgili, sıkça sorulan soruların sağladığı korumanın yeterliliği hakkındaki, 26 Temmuz 2000 tarihli, Komisyon Kararı,* OJ 2000 L 215.

- resmî sicillerden verilerin aktarımı amacıyla; bu resmi sicillerde yer alan bilgilere erişim hakkı şeklindeki üstün nitelikli kamu yararının bir örneğidir.

Başkalarının meşru menfaatleri de verilerin sınır ötesi serbest akışını haklı gösterebilir:[228]

- VK Direktifi kapsamına girmeyen ulusal güvenlik veya kamu güvenliği meseleleri dışındaki hususlarla alakalı önemli bir kamu menfaati sebebiyle; veya
- bir hak iddiasında bulunmak, bir hakkı kullanmak veya savunmak için.

Yukarıda sunulmuş olan durumlar, diğer ülkelere serbest veri aktarımı için alıcı ülkede yeterli veri koruma seviyesinin bulunması gerekliliğinin istisnaları olarak anlaşılmalıdır. İstisnalar her daim sınırlayıcı bir biçimde yorumlanmalıdır. Madde 29 Çalışma Kurultayında VK Direktifi madde 26(1) bağlamında, özellikle de rızanın veri aktarımına temel oluşturduğu durumlar bakımından bu hususun defalarca altını çizmiştir.[229] Madde 29 Çalışma Kurultayırızanın yasal önemine dair genel kuralların direktifin 26(1) maddesi açısından da uygulama alanı bulacağı sonucuna varmıştır. Örneğin, iş ilişkileri bağlamında işçiler tarafin verilen rızanın aslen özgür iradeyle verilmiş rıza olup olmadığı belirsiz ise, bu durumda veri aktarımları direktifin 26(1)(a) maddesine dayandırılamazlar. Bu durumlarda, veri aktarımları için ulusal veri koruma makamlarının lisans çıkarması gerekliliğini öngören madde 26(2) uygulanacaktır.

6.4. Üçüncü ülkelere sınırlandırılmış veri akışı

Ana başlıklar

- Verilerin yeterli koruma seviyesine sahip olmayan üçüncü ülkere gönderilmesinden önce planlanan veri akışının, veri sorumlusu tarafından denetim makamının incelemesine sunulması gerekebilir.
- Verileri göndermek isteyen veri sorumlusu bu inceleme sırasında iki hususun varlığını ortaya koymak durumundadır:

1) verilerin veri alıcısına aktarılmasına dair yasal bir dayanağın bulunduğunu; ve
2) veri alıcısında yeterli veri korumasının sağlanması için gerekli tedbirlerin alınmış olduğunu göstermek.

- Veri alıcısında yeterli veri korumasının oluşturulması için alınabilecek tedbirlerden bazıları şunlardır:

1) veri gönderimi yapan veri sorumlusu ve yabancı veri alıcısı arasında kararlaştırılacak sözleşmesel şartlar.
2) Özelikle çok uluslu şirketler grubu dahilinde gerçekleştirilen veri aktarımlarına uygulanabilir nitelikte bağlayıcı şirket kuralları.

- Yabancı makamlara yapılacak veri aktarımları aynı zamanda özel bir uluslararası antlaşma ile de düzenlenebilir.

VK Direktifi ve 108 Sayılı Sözleşme'ye Ek Protokol, veri sorumlusu veri alıcısı tarafında yeterli veri koruma tedbirlerinin sağlanması için özel ayarlamalar yaptığı ve bu ayarlamaların yapıldığını yetkili bir makama ispatlayabildiği sürece, verilerin korunmasıyla alakalı yeterli bir koruma düzeyi sağlayamayan üçüncü ülkelere sınır ötesi veri akışına dair rejimlerin ulusal hukuklar tarafından düzenlenebilmesine izin vermiştir. Bu gereklilik açık olarak yalnızca 108

[228] VK Direktifi, Madde 26 (1) (d).
[229] Bakınız, özellikle Madde 29 Çalışma Kurultayı (2005), 95*/46/AB Sayılı Direktifin 26(1). maddesi'nin ortak anlayışına ilişkin Çalışma Metni, 24 Ekim 1995*, WP 114, Brüksel, 25 Kasım 2005.

Sayılı Sözleşme'ye Ek Protokol'de yer almaktadır; ancak VK Direktifi kapsamında da standart prosedürün bu şekilde olduğu değerlendirilmektedir.

6.4.1. Sözleşme maddeleri

Gerek **AK mevzuatı** gerekse **AB mevzuatı,** veri gönderimi yapan veri sorumlusu ve üçüncü ülkedeki veri alıcısı arasındaki sözleşme maddelerinin, veri alıcısında yeterli veri koruma düzeyinin sağlanması için kullanılabilecek yollardan birisi olduğundan bahsetmektedir.

AB düzeyinde, Avrupa Komisyonu, Madde 29 Çalışma Kurultayın'ında desteğiyle, Komisyon Kararı gereği yeterli veri korumasının bir kanıtı olarak görülecek olan bazı standart sözleşme maddeleri geliştirmiştir.[230] Komisyon kararları bütün içerikleriyle Üye Devletler açısından bağlayıcı olduklarından, sınır ötesi veri akışını denetlemekle yükümlü olan ulusal makamların bu standart sözleşme maddelerini prosedürlerine dahil etmeleri gerekmektedir.[231] Yani, veri gönderimi yapan veri sorumlusu ve üçüncü ülkedeki veri alıcısının aralarında anlaşıp bu maddeleri kabul etmeleri, gerekli güvencelerin sağlandığına ilişkin olarak denetim makamına yeterli kanıtı sunacaktır.

AB yasal çerçevesi içerisinde standart sözleşme maddelerinin varlığı veri sorumlularının diğer *ad hoc* sözleşme maddeleri düzenlemelerine engel değildir. Ancak, bu şekilde getirilecek düzenlemelerin de standart sözleşme maddeleri tarafından sağlanan koruma düzeyinin aynısını sağlaması gerekmektedir. Standart sözleşme maddelerinin en önemli unsurları şunlardır:

- veri öznelerinin, sözleşmenin tarafı olmasalar da sözleşmeden kaynaklanan haklarını kullanabilmelerini sağlayacak olan bir üçüncü taraf lehtar maddesi;
- veri alıcısı veya içe aktarıcısının, uyuşmazlık halinde veri gönderimini yapan veri sorumlusunun ulusal denetim makamı ve/veya ulusal mahkemelerinin usullerine tabi olacaklarına dair kabulü.

Şu anda, veri sorumlusudan veri sorumlusuna yapılan aktarımları düzenleyen ve veri gönderimi yapan veri sorumlusunun arasından seçim yapabileceği iki ayrı standart maddeler grubu bulunmaktadır.[232] Veri sorumlusundan veri işleyene yapılan aktarımlar için ise sadece bir çeşit standart sözleşme maddeleri grubu vardır.[233]

AK mevzuatı bağlamında, 108 Sayılı Sözleşme Danışma Komitesi sözleşme maddelerinin hazırlanmasına yönelik olarak bir kılavuz hazırlamıştır.[234]

6.4.2. Bağlayıcı şirket kuralları

[230] VK Direktifi, Madde26 (4).

[231] Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, Madde 288.

[232] Birinci Set Avrupa Birliği Komisyonu, 2001/497/AB Sayılı, 95/46/AB Sayılı Direktif uyarınca Kişisel verilerin üçüncü ülkelere aktarılması için standart sözleşme hükümlerini içermektedir, 15 Haziran 2001 tarihli, Komisyon Kararı'nın ekindedir, OJ 2001 L 181; İkinci Set Avrupa Birliği Komisyonu, 27 Aralık 2004 tarihli ve 2004/915/AB Sayılı Direktif uyarınca kişisel verilerin üçüncü ülkelere transferi için standart sözleşme hükümlerinine alternatif bir setin sunulmasına ilişkin Komisyon Kararı'nın ekindedir, OJ 2004 L 385.

[233] Avrupa Komisyonu, Avrupa Birliği Komisyonu, 2010/87/AB Sayılı, 5 Şubat 2010 tarihli, 95/46/AB Sayılı Direktif uyarınca (2010), Avrupa Birliği Parlamentosu ve Konseyi'nin *Kişisel verilerin üçüncü ülkelerde bulunan veri işleyenlere aktarılmasına ilişkin sözleşmeye dayalı hükümler, OJ* 2010 L 39.

[234] Avrupa Konseyi, 108 Sayılı Sözleşmeye Danışma Komitesi (2002), *Kişisel verilerin üçüncü şahıslara aktarımı sırasında korunmasına ilişkin sözleşme hükümlerinin hazırlanması için kullanılan rehber.*

Çok taraflı bağlayıcı şirket kuralları (BŞKler) sıklıkla birçok Avrupa veri koruma makamını birden ilgilendirir.[235] BŞKlerin uygun bulunabilmesi için BŞKler'in taslakları standart hale getirilmiş başvuru formları ile birlikte konuyla alakalı en üst makama gönderilmelidir.[236] En üst makamın hangisi olduğu standart hale getirilmiş başvuru formundan anlaşılabilir. Sonrasında bu üst makam, BŞKlerin değerlendirilme sürecindeki katılımları gönüllülük esasına dayalı olmasına karşın, grubun iştiraklerinin bulunduğu EEA üye ülkelerindeki denetim makamlarının hepsini bilgilendirir. Bağlayıcı olmamasına rağmen söz konusu veri koruma makamlarının hepsi değerlendirmenin sonucunu resmi lisanslama prosedürlerine dahil etmek durumundadır.

6.4.3. Özel uluslararası anlaşmalar

AB, iki çeşit veri aktarımına yönelik olarak özel sözleşmeler öngörmüştür:

Yolcu İsmi Kayıtları (PNR numarası)

Yolcu İsmi Kayıtları (PNR) verileri rezervasyon sürecinde hava yolu şirketleri tarafından toplanır ve yolcuların isimleri, adresleri, kredi kartı detayları ve koltuk numaraları gibi bilgileri içerir. ABD hukukuna göre, hava yolu şirketleri bu verileri yolcunun uçuşu öncesinde ABD İç Güvenlik Bakanlığı'na bildirmek zorundadır. Bu ABD'ye giden ve ABD'den gelen uçuşlar için geçerlidir.

VK Direktifi hükümlerine uygun olarak PNR verilerinin uygun şekilde korunmasını sağlamak için 2004 yılında özel bir 'PNR paketi'[237] kabul edilmiştir. Pakete ABD İç Güvenlik Bakanlığı (DHS) tarafından yürütülen veri işlemelerinin uygunluğu da dahil edilmiştir.

PNR paketinin ABAD tarafından iptalini takiben,[238] AB ve ABD aralarında PNR verilerinin ABD'ye aktarımına yasal bir dayanak oluşturmak ve alıcı ülkede yeterli veri korumasını sağlamak amaçlarıyla 2 farklı sözleşme imzalamışlardır.

AB ülkeleri ve ABD'nin verileri nasıl paylaştığı ve yönettiğine dair düzenlemeler içeren 2012 tarihli ilk sözleşme birçok hata içermekteydi ve aynı yıl içerisinde yasal belirliği sağlamak adına başka bir sözleşme ile değiştirildi.[239] Yeni sözleşme önemli iyileştirmeler içermektedir.

---

[235] Bağlayıcı kurumsal kuralların içeriği ve yapısına dair, Madde 29 Çalışma Kurultayı (2008), *Bağlayıcı kurumsal kurallar için bir çerçeve oluşturan çalışma belgesi,* düzenlemiştir, WP 154, Brüksel, 24 Haziran 2008; ve Madde 29 Çalışma Kurultayı (2008), bağlayıcı kurumsal kurallarda bulunacak unsurlar ve ilkeler içeren bir tablo oluşturan çalışma belgesi, sunmuştur, WP 153, Brüksel, 24 Haziran 2008.

[236] Madde 29 Çalışma Kurultayı, 1/2007 Sayılı, Kişisel verilerin aktarımına dair alınan bağlayıcı kurumsal kuralların onayına ilişkin standart bir uygulamanın düzenlenmesi Önerisi, WP 133, Brüksel, 10 Ocak 2007.

[237] 2004/496/AB Sayılı, Komisyon Kararı, Avrupa Topluluğu ve Birleşik Devletler arasında imzalanan, havayolu taşıyıcıları tarafından uçak yolcuların Yolcu Adı Kayıtlarının (PNR numarası) Birleşik Devletler Vatan Güvenliği Departmanı Gümrük ve Sınır Güvenliği Bürosuna gönderilmesine dair Sözleşmeye ilişkin,17 Mayıs 2004, OJ 2004 L 183, s. 83, ve 2004/535/AB Sayılı, Komisyon Kararı, Birleşik Devletler Gümrük ve Sınır Koruma Bürosuna transfer edilen uçak yolcularının, Yolcu Adı Kaydına (PNR numarası) yer alan kişisel verilerin korunmasına ilişkin, 14 Mayıs 2004, OJ 2004 L 235, s. 11-22.

[238] ABAD, Birlikte Görülen C-317/04 ve C-318/04, *European Parliament v. Council of the European Union,* 30 Mayıs 2006, par. 57, 58 ve 59, mahkeme, yeterlilik kararının ve verilerin işlenmesine ilişkin anlaşmanın Direktifin kapsamı dışında bırakıldığına karar vermiştir.

[239] 2012/472/AB Sayılı, Komisyon Kararı, Amerika Birleşik Devletleri ile Avrupa Birliği arasında, Amerika Birleşik Devletleri, Ulusal Güvenlik Departmanı tarafından Yolcu İsmi Kayıtlarının kullanılması ve aktarılmasına ilişkin Sözleşmesine ilişkin, 26 Nisan 2012, OJ 2012 L 215/4. Bu karara, sözleşme eklenmiştir, OJ 2012 L 215, s. 5-14.

Sözleşme bilgilerin hangi amaçlarla (örneğin ciddi nitelikteki sınıraşan suçlar ve terörizm) kullanılabileceğini sınırlar ve açıklığa kavuşturur ve verilerin tutulabileceği süreyi belirler: 6 ay geçtikten sonra veriler anonimleştirilmeli ve maskelenmelidir. Verilerin kötüye kullanımının söz konusu olduğu hallerde herkesin ABD hukuku kapsamında idari ve yargısal yollara başvuru hakkı bulunmaktadır. Ayrıca kişiler kendi PNR verilerine erişim hakkına ve tutulan bilgilerin doğru olmaması durumunda ABD İç Güvenlik Bakanlığı'ndan verilerinin silme seçeneği de dahil olmak üzere düzeltilmesini talep etme hakkına sahiptirler.

1 Temmuz 2012 yılında yürürlüğe giren bu sözleşme 2019 yılına kadar 7 yıl boyunca yürürlükte kalacaktır.

Avrupa Birliği Konseyi 2011 yılında PNR verilerinin işlenmesi ve aktarımına dair AB-Avustralya Antlaşması'nın güncellenmiş bir versiyonunu onaylamıştır.[240] AB ve Avusturalya arasında yapılan PNR verilerine dair bu sözleşme, küresel PNR ilkeleri[241], AB-PNR sisteminin kurulması[242] ve üçüncü devletlerle yapılan sözleşme müzakereleri[243] gibi unsurları içeren AB gündemi açısından ileri doğru atılmış bir adımdır.

Mali iletişim verileri

Avrupa'da bulunan bankalardan çıkan küresel çaptaki para aktarımlarının çoğunun veri işleyeni olan Belçika merkezli Dünya Bankalararası Finansal İletişim Topluluğu (SWIFT) ABD'de kurulu bir eş merkez üzerinden faaliyetlerini yürütmekteydi ve ABD Hazine Bakanlığı'nın terörizm soruşturmaları çerçevesinde ilettiği bir veri paylaşımı talebiyle karşı karşıya kaldı.[244]

AB perspektifinden bakıldığında, esasen Avrupa verileri olan ancak sırf SWIFT'in veri işleme merkezlerinden birisinin orada bulunmasından dolayı ABD'de erişilebilir olan bu verilerin ifşasına yönelik hukuki bir dayanak yoktu.

AB ve ABD arasında SWIFT Sözleşmesi olarak bilinen özel bir sözleşme gerekli hukuki dayanağın oluşturulması ve yeterli veri korumanın sağlanması amacıyla 2010 yılında kabul edildi.[245]

---

[240] 2012/381/AB Sayılı, Komisyon Kararı, Avusturalya ile Avrupa Birliği arasında, hava taşıyıcıları tarafından Yolcu İsmi Kart'ının (PNR numarası) Avusturalya Gümrük ve Sınır Koruma Hizmeti 'ne aktarılması ve işlenmesine Sözleşmesine ilişkin, 13 Aralık 2011, OJ 2012 L 186/3, Bir önceki 2008 sözleşmesinin yerini alan Sözleşmenin metni, bu Karara eklenmiştir, OJ 2012 L 186, s. 4–16.

[241] Bakınız, Avrupa Birliği Komisyonu tarafından 21 Eylül 2010 tarihinde, Yolcu Adı Kayıt (PNR) verilerinin üçüncü ülkelere aktarılmasına yönelik küresel yaklaşım üzerine yapılan bildirim, COM(2010) 492 final, Brüksel. Bakınız Madde 29 Çalışma Kurultayı (2010), *7/2010 Sayılı,* Avrupa Birliği Komisyonu tarafından, Yolcu Adı Kayıt (PNR) verilerinin üçüncü ülkelere aktarılmasına yönelik küresel yaklaşım üzerine yapılan bildirime ilişkin Öneri, WP 178, Brüksel Kasım 12, 2010.

[242] Avrupa Birliği Parlamentosu ve Konseyi tarafından, Terör suçlarını ve ciddi suçları önleme, tespit etme, soruşturma ve kovuşturma için kullanılan PNR verilerin kullanılmasına ilişkin Direktif Önerisi, COM(2011) 32 final, Brüksel, 2 Şubat 2011. Nisan 2011'de, Avrupa Birliği Parlamentosu, Avrupa Birliği Temel Haklar Ajansın'dan bu Önerinin Avrupa Birliği Temel Şart'ı ile uyumu konusunda görüş bildirmesini talep etmiştir. Bakınız: FRA (2011), *1/2011 Sayılı Öneri– PNR,* Viyana, 14 Haziran 2011.

[243] AB, şu anda Kanada ile, yürürlükte olan 2006 anlaşmasının yerine geçecek olan yeni bir PNR anlaşmasını müzakere etmektedir.

[244] Bu bağlamda bakınız, Madde 29 Çalışma Kurultayı (2011), *14/2011 Sayılı, Kara para aklamanın ve terörizmin finansmanının önlenmesine ilişkin veri koruma konularına ilişkin* Öneri, WP 186, Brüksel, 13 Haziran 2011; Madde 29 Çalışma Kurultayı (2006), *10/2006 Sayılı, Uluslararası Bankalar arası Finansal Telekomünikasyon Topluluğu (SWIFT) tarafından işlenen kişisel verilere ilişkin* Öneri, WP 128, Brüksel, 22 Kasım 2006; Gizliliğin korunmasına dair Belçika Komisyonu'nun Kararı (*Commission de la protection de la vie privée*) (2008), *'Şirket SWIFT'e ilişkin denetim ve tavsiye prosedürü başlatıldı',* 9 Aralık 2008.

[245] 2010/412/EU Sayılı, Konsey Kararı, Amerika Birleşik Devletleri ile Avrupa Birliği arasında, Avrupa Birliğinden Amerika Birleşik Devletlerine Finansal Mesajlaşma Verilerinin, Terörist Mali İzleme Programı kapsamında işlenmesi ve aktarılmasına ilişkin Sözleşmeye ilişkin, 13 Temmuz 2010, OJ 2010 L 195, s. 3 ve 4. Sözleşme, Karara eklenmiştir, OJ 2010 L 195, s. 5-14.

Bu sözleşme ile, SWIFT tarafından tutulan mali veriler terörizm veya terörizmin finasmanının önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması amaçlarıyla ABD Hazine Bakanlığı'yla paylaşılmaya devam etmektedir. ABD Hazine Bakanlığı talebin aşağıdaki şartları karşılaması durumunda SWIFT'ten mali veriler talep edebilir:

- mali verileri mümkün olduğu ölçüde açık bir şekilde tanımlamalı;
- verilerin gerekliliğini açık bir biçimde kanıtlamalı;
- talep edilen veri miktarını en aza indirgemek için olabildiğince dar kapsamlı olmalı;
- Avrupa Tek Ödeme Alanı'yla (SEPA) alakalı herhangi bir veri talep edilmemeli.

Europol'a ABD Hazine Bakanlığı tarafından yapılan her talebin bir kopyası verilmeli ve SWIFT Sözleşmesi'nin ilkelerine uyulup uyulmadığı kurum tarafından doğrulanmalıdır.[246] Uyumlu olduğu doğrulandığı taktirde SWIFT verileri doğrudan ABD Hazine Bakanlığı'yla paylaşmalıdır. Bakanlık, söz konusu mali verileri yalnızca terörizm veya terörizmin finansmanının soruşturulması için çalışan analiz görevlileri tarafından erişilebilecekleri güvenli bir fiziksel ortamda saklamalı ve mali veriler başka herhangi bir veri tabanı ile ilişkilendirilmemelidir. Genel olarak, SWIFT'ten alınan mali veriler alınma tarihinden itibaren en geç 5 yıl içerisinde silinmelidir. Özel soruşturmalar veya kovuşturmalarla alakalı mali veriler bu soruşturma ve kovuşturmalar kapsamında gerekli oldukları sürece tutulabilirler.

ABD Hazine Bakanlığı SWIFT'ten aldığı veriler içerisinde yer alan bilgileri, münhasıran terörizmin ve terörizmin finasmanının soruşturulması, tespiti, önlenmesi veya kovuşturulması amaçlarıyla ABD sınırları içinde veya dışında yer alan belirli kolluk, kamu güvenliği veya terörle mücadele makamlarına aktarabilir. Mali verilerin bu şekilde aktarımının AB Üye Ülkelerinden birisinin bir vatandaşıyla veya bu ülkelerde ikamet eden bir kişiyle alakalı olması halinde, bu verilerin üçüncü bir ülkede bulunan makamlarla paylaşımı ilgili Üye Devlet'in yetkili makamlarının bu paylaşıma izin vermesine bağlıdır. Verilerin paylaşımının kamu güvenliğine yönelik yakın ve ciddi bir tehdidin önlenmesi için gerekli olduğu durumlarda istisnalar yapılabilir.

Aralarında Avrupa Komisyonu tarafından atanmış bir kişinin de bulunduğu bağımsız müfettişler SWIFT Sözleşmesi ilkelerine uyulup uyulmadığını denetlemektedir.

Veri özneleri, kişisel verilerinin korunması haklarına uygun davranıldığına dair yetkili AB veri koruma makamından teyit alma hakkına sahiptirler. Veri öznelerinin ayrıca ABD Hazine Bakanlığı tarafından SWIFT Sözleşmesi kapsamında toplanan ve saklanan verilerinin düzeltilmesini, silinmesini veya engellenmesini talep etme hakları da bulunmaktadır. Ancak, veri öznelerinin erişim hakları bazı yasal sınırlamalara tabi olabilir. Verilere erişim talebinin reddedildiği durumlarda veri öznesi, bu ret kararına ve başvurulabilecek idari ve yargısal yollara ilişkin olarak yazılı şekilde bilgilendirilmelidir.

SWIFT Sözleşmesi 5 yıl için, 2015 ağustos ayına kadar geçerlidir. Sözleşme, taraflardan birisi, sözleşmenin sona ermesinden en az altı ay önce sözleşmeyi uzatmak istemediğine dair karşı tarafa bir bildirimde bulunmadıkça, otomatik olarak bir yıllık sürelerle yenilenecektir.

[246] Europol'un Ortak Denetleme Kurumu, Europol'un bu alandaki faaliyetleri hakkında denetimler yürütmüş olup, sonuçlarını bu websayfasında belirtmiştir: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

7. Kolluk ve ceza yargılaması kapsamında verilerin korunması

AB	İşlenen konular	AK
	Genel olarak	108 Sayılı Sözleşme
	Kolluk	Kolluk Alanında Kişisel Verile-rin Kullanımının Düzenlenmesine İlişkin (87) 15 Numaralı Tavsiye Kararı AİHM, *B.B. v. France*, No. 5335/06, 17 Aralık 2009 AİHM, *S. and Marper v. the United Kingdom*, Nos. 30562/04 ve 30566/04, 4 Aralık 2008 AİHM, *Vetter v. France*, No.59842/00, 31 Mayıs 2005
	Siber suçlar	Sanal Ortamda İşlenen Suçlar Sözleşmesi
AB mevzuatına göre kolluk ve adli iş birliği kapsamında verilerin korunması		
Data Protection Framework Decision	**Genel olarak**	108 Sayılı Sözleşme Kolluk Alanında Kişisel Verile-rin Kullanımının Düzenlenmesine İlişkin (87) 15 Numaralı Tavsiye Kararı
Prüm Decision	**Özel veriler için; parmak izi, DNA, holiganlık vs.**	108 Sayılı Sözleşme Kolluk Alanında Kişisel Verile-rin Kullanımının Düzenlenmesine İlişkin (87) 15 Numaralı Tavsiye Kararı
Europol Decision Eurojust Decision Frontex Regulation	**Özel kurumlar tarafından**	108 Sayılı Sözleşme Kolluk Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin (87) 15 Numaralı Tavsiye Kararı
Schengen II Decision VIS Regulation Eurodac Regulation CIS Decision	**Özel müşterek bilişim sistemleri tarafından**	108 Sayılı Sözleşme Kolluk Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin (87) 15

		Numaralı Tavsiye Kararı AİHM, *Dalea v. France*, No. 964/07, 2 Şubat 2010

Bireyin verilerinin korunmasındaki menfaatleri ile toplumun suçla mücadele ve ulusal ve kamu güvenliğinin sağlanması amacıyla verilerin toplanmasındaki menfaatleri dengeleyebilmek için AK ve AB özel yasal düzenlemeler çıkarmışlardır.

7.1. Kolluk ve ceza yargılaması kapsamında verilerin korunması

Ana başlıklar

- 108 Sayılı Sözleşme ile AK Kolluk Tavsiye Kararı kolluk faaliyetlerinin tamamını kapsayan veri koruması düzenlemeleri içermektedir.
- Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi) elektronik ağlar yoluyla veya bu ağlara karşı işlenen suçlara ilişkin bağlayıcı bir uluslararası hukuki düzenlemedir.

Avrupa düzeyinde, 108 Sayılı Sözleşme kişisel verilerin işlenmesine dair her alanı kapsar ve sözleşme hükümleri genel bağlamda kişisel verilerin işlenmesini düzenlemeye yöneliktir. Bu sebeple, Akit Taraflar uygulamasını sınırlayabilecek olsalar da 108 Sayılı Sözleşme kolluk ve ceza yargılaması alanlarındaki veri koruma konuları bakımından da uygulanırlar.

Kolluk ve ceza yargılaması yetkililerinin yasal görevleri çoğu zaman kişisel verilerin işlenmesini gerektirirler ve bu da söz konusu bireyler açısından ciddi sonuçlara yol açabilir. AK tarafından 1987 yılında kabul edilen Kolluk Verileri Tavsiye Kararı Akit Taraflara 108 Sayılı Sözleşme'de yer alan ilkeleri kişisel verilerin kolluk makamları tarafından işlenmesi bağlamında nasıl hayata geçirmeleri gerektiğine dair rehberlik etmektedir.[247]

7.1.1. Kolluk Tavsiye Kararı

AİHM birçok kararında kişisel verilerin kolluk ve ulusal güvenlik makamları tarafından saklanmasının ve tutulmasının AİHS 8(1) maddesine yönelik bir müdahale oluşturacağını belirtmiştir. Birçok AİHM kararı bu müdahalelerin meşrulaştırılması konusunu ele alır.[248]

Örnek: **'B.B. v Fransa'**[249] davasında, AİHM, cinsel bir suçtan sabıkalı bir kişinin ulusal adli veri tabanına dahil edilmesinin AİHS'nin 8. maddesi kapsamında girdiğine karar vermiştir. Ancak, verilerin korunması için, örneğin veri öznesinin verilerin silinmesini talep hakkı, verilerin sınırlı süreyle saklanması ve bu verilere sınırlı erişim gibi yeterli tedbirlerin alındığı da göz önünde tutulursa, yarışan özel ve kamu menfaatleri arasında adil bir denge kurulmuştur. Bu durumda Mahkeme AİHS madde 8'in ihlal edilmediğine dair bir karar vermiştir.

[247] Avrupa Konseyi, Bakanlar Komitesi (1987), *Üye Devletlere yönelik Polis sektöründe kişisel verilerin kullanımını düzenleyen Öneri, 17* Eylül 1987.
[248] Örneğin, AİHM, *Leander v. Sweden*, No. 9248/81, 26 Mart 1987; AİHM, *M.M. v. the United Kingdom*, No. 24029/07, 13 Kasım 2012; AİHM, *M.K. v. France*, No. 19522/09, 18 Nisan 2013.
[249] AİHM, *B.B. v. France*, No. 5335/06, 17 Aralık 2009.

Örnek: **'S. Ve Marper v. Birleşik Krallık'** davasında,[250] her iki başvuran da ceza gerektiren bir suçla suçlanmış ancak hüküm giymemiştir. Buna rağmen, parmak izleri, DNA profilleri ve hücre örnekleri alınmıştır ve polis tarafından saklanmıştır. Bir kişinin suç işlediğinden şüphelenilmesi durumunda, şüpheli sonradan beraat etmiş veya serbest bırakılmış olsa bile biyometrik verilerin sınırsız olarak tutulmasına izin veren bir kanun bulunmaktadır. AİHM, kişisel verilerin süre sınırı olmadan ve beraat eden bireylerin verilerin silinmesine yönelik sınırlı imkanları olduğu bir şekilde sınırsız ve ayrım gözetmeksizin tutulmasının, başvuranların özel hayatlarına saygı gösterilmesi hakkına yönelik orantısız bir müdahale olduğuna karar vermiştir. Bu sebeple Mahkeme, AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Birçok AİHM kararı verilerin korunması hakkına gözetleme yoluyla yapılan müdahalenin meşrulaştırılması meselesini ele almıştır.

Örnek: **'Allen v. Birleşik Krallık'**[251] davasında, bir mahkûmun cezaevi ziyaret alanında bir arkadaşı ile ve bir cezaevi hücresinde başka bir tutuklu ile olan özel konuşmaları yetkililer tarafından gizlice kayda alınmıştır. AİHM, görsel ve işitsel kayıt cihazlarının başvuranın hücresinde, cezaevi ziyaret alanında ve başka bir tutuklu üzerinde kullanılmasının başvuranın özel hayatına yönelik bir müdahale olduğuna karar vermiştir. Gizli kayıt cihazlarının kolluk tarafından kullanımını düzenlemeye yönelik o zamanda bir yasal sistem de bulunmadığından, söz konusu müdahale hukuka uygun olarak da gerçekleşmemiştir. Mahkeme, AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Örnek: **'Klass ve Diğerleri v. Almanya'**[252] davasında, başvuranlar elektronik postaların, mektupların ve haberleşmenin gizli olarak gözetlenmesine izin veren birçok Alman yasasının, özellikle de gözetlenen kişinin gözetleme tedbirleriyle alakalı olarak bilgilendirilmediği ve bu tedbirler sona erdikten sonra mahkemelerde hakkını arayamayacağı gerekçeleriyle AİHS madde 8'i ihlal ettiğini iddia etmişlerdir. AİHM bir gözetleme tehdidinin kaçınılmaz olarak mektup veya telekomünikasyon yoluyla haberleşme hizmeti alan kullanıcılar arasındaki haberleşme hürriyetine müdahale ettiğine karar vermiştir. Ancak bu davada kötüye kullanıma karşı yeterli tedbirlerin anılmış olduğu kanaatine varmıştır. Alman yasa koyucunun, bu tür müdahalelerin demokratik toplumda ulusal güvenlik menfaatleri ve düzensizliğin ve suç işlenmesinin önlenmesi açısından gerekli olduğunu değerlendirmekte haklı olduğu sonucuna varılmıştır. Mahkeme madde 8'in ihlal edilmediğine karar vermiştir.

Kolluk makamları tarafından yapılan veri işlemeleri söz konusu kişiler üzerine önemli etkilere sebep olabileceğinden, bu alandaki veri tabanlarının tutulmasına yönelik olarak detaylı veri koruma kurallarının düzenlenmesi önem taşımaktadır. AK Kolluk Tavsiye Kararı, kolluk işlerinde verilerin nasıl toplanması gerektiğine; bu alandaki veri dosyalarının nasıl saklanması gerektiğine; verilerin yabancı polis makamlarına aktarımı için gerekli koşullar da dahil olmak üzere, bu dosyalara erişim yetkisinin kime verilmesi gerektiğine; veri öznelerinin veri koruma haklarını nasıl kullanabileceklerine ve bağımsız denetim makamları tarafından kontrollerin nasıl yapılacağına ilişkin rehberlik sunarak bu meseleyi ele almayı hedeflemiştir. Yeterli veri güvenliği sağlama yükümlülüğü de bu değerlendirmeye alınmıştır.

[250] AİHM, *S. and Marper v. the United Kingdom*, Nos. 30562/04 ve 30566/04, 4 Aralık 2008, par. 119 ve 125.
[251] AİHM, *Allan v. the United Kingdom*, No. 48539/99, 5 Kasım 2002.
[252] AİHM, *Klass and Others v. Germany*, No. 5029/71, 6 Eylül 1978.

Tavsiye kararı, kolluk makamlarına ucu açık, ayrım gözetmeyen bir veri toplama imkânı sunmamaktadır. Kolluk makamları tarafından kişisel verilerin toplanması, gerçek bir tehlikenin veya belirli bir suçun önlenmesi için gerekli olma kriterleriyle sınırlandırılmıştır. Bundan başka amaçlarla yapılacak herhangi bir veri toplama faaliyetinin belirli bir ulusal kanuna dayanması gerekmektedir. Hassas verilerin işlenmesi ise belirli bir tahkikat bağlamında mutlak şekilde gerekli olan verilerle sınırlı olmalıdır.

Veri öznesinin bilgisi dahilinde olmaksızın kişisel verilerin toplandığı durumlarda, yapılacak bilgilendirme soruşturmanın seyrini artık etkilemeyecek hale gelir gelmez veri öznesi bilgilendirilmelidir. Verilerin teknik gözetleme veya diğer otomatik yollarla toplanması için belirli yasal düzenlemeler gereklidir.

Örnek: **'Vetter v. Fransa'**[253] davasında, başvuran gizli tanıklar tarafından cinayetle itham edilmiştir. Başvuran bir arkadaşının evine düzenli olarak gittiği için de polis, sorgu hakiminin izniyle eve dinleme cihazları yerleştirmiştir. Kaydedilen konuşmalara dayanılarak başvuran tutuklanmış ve cinayetle yargılanmıştır. Başvuran, dinlemenin kanun tarafından düzenlenmemiş olması sebebiyle kanıt olarak geçersiz ilan edilmesi talebinde bulunmuştur. AİHM açısından konu, dinleme cihazlarının kullanımının "kanuna uygun" olup olmadığıdır. Ceza Muhakemesi Kanunu 100. maddesi ve devamındaki düzenlemeler telefon hatlarının dinlenmesine ilişkin olduğundan özel konuta dinleme cihazı yerleştirilmesi bu maddelerin kapsamına açık bir biçimde girmemekteydi. Kanunun 81. maddesi, yetkililerin, özel konuşmaların takibine izin verme konusundaki takdir yetkilerinin kullanımına dair kapsam veya usulü makul bir açıklıkla ortaya koymamaktaydı. Dolayısıyla, başvuran, demokratik bir toplumda geçerli olan hukukun üstünlüğü ilkesi gereği vatandaşların hakkı olan asgari koruma seviyesinden yararlanamamıştır. Mahkeme AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

Tavsiye kararı, kişisel veriler saklanırken: idari veriler ve kolluk verileri arasında; şüpheliler, hükümlü kişiler, mağdurlar ve tanıklar gibi farklı veri özneleri arasında ve sağlam gerçeklere dayanan veriler ve şüpheye veya tahmine dayalı veriler arasında belirgin ayrımların yapılması gerektiğini belirtmektedir.

Kolluk verileri amaç bağlamında sıkı bir şekilde sınırlanmış olmalıdır. Bu durumun ise kolluk verilerinin üçüncü kişilere iletimiyle alakalı bazı sonuçları vardır: bu verilerin kolluk sektörü içerisinde aktarımı veya iletimi söz konusu bilgilerin paylaşımı bakımından meşru bir çıkar olup olmamasıyla belirlenmelidir. Bu tür verilerin kolluk sektörü dışına aktarılmasına veya iletilmesine sadece açık bir yasal yükümlülük veya yetki bulunduğunda izin verilmelidir. Uluslararası aktarım veya iletim, ciddi ve yakın bir tehlikenin önlenmesi için gerekli olmadıkça, yabancı kolluk makamlarıyla sınırlandırılmalı ve uluslararası antlaşmalar gibi özel yasal düzenlemelere dayanmalıdır.

Kolluk tarafından yürütülen veri işlemeleri ulusal veri koruma hukukuna uygunluğu sağlamak amacıyla bağımsız denetime tabi olmalıdır. Veri özneleri 108 Sayılı Sözleşme'de yer alan erişim haklarının hepsine sahip olmalıdır. Veri öznelerinin erişim haklarının 108 Sayılı Sözleşme'nin 9. maddesi uyarınca polis soruşturmalarının etkililiği gerekçesiyle sınırlandırıldığı durumlarda, veri öznesi ulusal hukuk kapsamında ulusal veri koruma denetim makamına veya başka bir bağımsız kuruma itiraz hakkına sahip olmalıdır.

[253] AİHM, *Vetter v. France*, No. 59842/00, 31 Mayıs 2005.

7.1.2. Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi)

Suç faaliyetleri giderek artan bir şekilde elektronik veri işleme sistemlerini kullandığı ve etkilediği için, bu gelişmeye ayak uydurmak adına yeni yasal düzenlemelerin yapılması gerekmektedir. Bu sebeple AK, elektronik ağlara karşı veya bu ağlar yoluyla işlenen suçlar konusunu ele almak amacıyla Budapeşte Sözleşmesi olarak da bilinen, Sanal Ortamda İşlenen Suçlar Sözleşmesi isimli bir uluslararası yasal düzenlemeyi kabul etmiştir.[254] Bu sözleşme AK üyesi olmayan ülkelerin de katılımına açıktır ve 2013 ortası itibariyle, AK üyesi olmayan dört devlet -Avustralya, Dominik Cumhuriyeti, Japonya ve ABD- sözleşmeye taraf olmuştur ve başka 12 üye olmayan devlet de sözleşmeyi imzalamış veya katılım için davet edilmiştir.

Sanal Ortamda İşlenen Suçlar Sözleşmesi, internet veya diğer bilişim ağları yoluyla gerçekleşen hukuk ihlallerini düzenleyen en etkili uluslararası antlaşmalardan birisi olmaya devam etmektedir. Sözleşme, tarafların ceza kanunlarını hackleme ve telif hakkı ihlali, bilgisayar yoluyla dolandırıcılık, çocuk pornografisi ve diğer yasa dışı sanal faaliyetler de dahil olmak üzere diğer güvenlik ihlallerine yönelik olarak güncellemeleri ve yeknesaklaştırılmalarını gerektirmektedir. Sözleşme ayrıca sanal ortamda işlenen suçlarla mücadele bağlamında bilgisayar ağlarının aranması ve haberleşmeye müdahale edilmesine dair prosedürle alakalı yetkileri de düzenlemektedir. Son olarak, etkili bir uluslararası işbirliğinin önünü açmaktadır. Sözleşmeye ek olarak kabul edilen bir protokol ise bilgisayar ağlarında gerçekleşen ırkçı ve yabancı düşmanlığı içerikli propagandanın suç sayılmasına yönelik düzenlemeler içermektedir.

Sözleşme aslında veri korumanın teşvik edilmesi için getirilmiş bir düzenleme olmasa da bir veri öznesinin verilerinin korunması hakkını ihlal etmesi muhtemem olan faaliyetleri suç kapsamına alarak bu işlevi de yerine getirmektedir. Ayrıca Taraf Devletlerin sözleşmeyi uygularken verilerin korunması hakkı gibi AİHS kapsamında güvence altına alınan haklar da dahil olmak üzere insan hak ve özgürlüklerine yönelik yeterli korumayı öngörmelerini de zorunlu kılmaktadır.[255]

[254] Avrupa Konseyi, Bakanlar Komitesi (2001), Siber Suç Sözleşmesi, CETS No. 185, Budapest, 23 Kasım 2001, 1 Temmuz 2004 tarihinde yürürlüğe girmiştir.
[255] *A.e.*, Madde15 (1).

7.2. Kolluk ve cezai konularda verilerin korunmasına dair AB mevzuatı

Ana başlıklar

- AB seviyesinde, kolluk ve ceza yargılaması alanında verilerin korunması sadece kolluk ve adli makamların sınır ötesi işbirliği bağlamında düzenlenmiştir.
- Yasaların sınır ötesi uygulamasını destekleyen ve teşvik eden AB kurumları olan Avrupa Polis Teşkilatı'na (Europol) ve AB yargısal işbirliğini düzenleyen birime (Eurojust) yönelik olarak da özel veri koruma düzenlemeleri bulunmaktadır.
- Yetkili kolluk makamları ve adli makamlar arasında sınır ötesi bilgi değişimi için AB seviyesinde kurulmuş olan müşterek bilişim sistemleri için de özel veri koruma düzenlemeleri bulunmaktadır. Schengen II, Vize Bilgi Sistemi (VIS) ve AB Üye Ülkeleri'nden birine sığınma talebinde bulunmuş üçüncü ülke vatandaşlarına ait parmak izlenini barındıran merkezi bir sistem olan Eurodac bu sistemlerin önemli örneklerindendir.

VK Direktifi kolluk ve ceza yargılaması alanlarını kapsamamaktadır. Bölüm 7.2.1. bu alanda var olan en önemli yasal düzenlemeleri tartışmaktadır.

7.2.1. Veri Koruma Çerçeve Kararı

2008/977/JHA sayılı cezai konularda polis ve adli işbirliği çerçevesinde işlenen kişisel verilerin korunmasına dair Konsey Çerçeve Kararı (Veri Koruma Çerçeve Kararı) bir suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya bir cezanın infazı amacıyla verileri işlenmiş gerçek kişilerin kişisel verilerinin korunmasını sağlamak amacını taşımaktadır.[256] Kolluk ve ceza yargılaması alanında çalışan yetkililer burada Üye Devletler veya AB adına hareket etmektedirler. Bu kurumlar AB ajansları, kuruluşları veya Üye Devletlerin yetkilileridir.[257] Bu çerçeve kararın uygulama alanı bu makamlar arasında gerçekleştirilecek sınır ötesi işbirliği kapsamında veri korumasının sağlanmasıyla sınırlıdır ve ulusal güvenliği kapsayacak şekilde uygulanamaz.

Veri Koruma Çerçeve Kararı büyük ölçüde 108 Sayılı Sözleşme'de ve VK Direktifi'nde yer alan ilkelere ve tanımlara dayanmaktadır.

Veriler yalnızca yetkili bir makam tarafından ve yalnızca iletilmelerine veya erişime açılmalarına sebep olan amaca yönelik olarak kullanılmalıdır. Verileri alan Üye Devlet, verilerin takasına yönelik olarak gönderen Üye Devlet tarafından kanunlarla getirilen sınırlamalara saygı duymalıdır. Verilerin alıcı devlet tarafından başka amaçlar için kullanılması bazı şartların yerine getirilmesi halinde mümkün olabilir. İletimlerin kaydının ve belgelerinin şikayetler sebebiyle oluşabilecek sorumluluklarının netleştirilmesinde kullanılmak amacıyla tutulması yetkili makamlara özel sorumluluklardan birisidir. Sınır ötesi işbirliği kapsamında iletilen verilerin üçüncü kişilere aktarılması için, acil durumlardaki istisnalar saklı kalmak kaydıyla, verilerin çıkış noktası olan Üye Devletin rızası gereklidir.

[256] Avrupa Birliği Konseyi, 2008/977/JHA Sayılı cezai konularda polis ve adli işbirliği çerçevesinde işlenen kişisel verilerin korunmasına dair Konsey Çerçeve Kararı, 27 Kasım 2008, OJ 2008 L 350.

[257] *A.e.*, Madde2 (h).

Yetkili makamlar kişisel verilerin herhangi bir yasa dışı işlemeye karşı korunması için gerekli güvenlik tedbirlerini almakla yükümlüdürler.

Her Üye Devlet, Veri Koruma Çerçeve Kararı kapsamında kabul edilen düzenlemelerin uygulamasına danışmanlık vermek ve uygulamayı takip etmek üzere bir veya birden çok bağımsız ulusal denetim makamının görevlendirildiğinden emin olmalıdır. Bu makamlar ayrıca, kişisel verilerin yetkili makamlar tarafından işlenmesi kapsamındaki hak ve özgürlüklerinin korunmasıyla alakalı olarak yapılan şikayetleri de incelemek zorundadır.

Veri öznesi, kişisel verilerinin işlenmesiyle alakalı bilgi alma ve verilerine erişim, verilerin düzeltilmesi, silinmesi veya engellenmesi hakkına sahiptir. Bu hakların kullanılmasının mücbir sebeplerle reddedildiği durumlarda veri öznesi yetkili ulusal denetim makamına ve/veya bir mahkemeye itiraz hakkına sahip olmalıdır. Bir kişi Veri Koruma Çerçeve Kararı'nı iç hukuka aktaran yasanın ihlali sebebiyle bir zarara uğrarsa, bu kişi veri sorumlusundan tazminat talep etme hakkına sahiptir.[258] Genel olarak, veri özneleri, Veri Koruma Çerçeve Kararı'nı iç hukuka aktaran ulusal yasa kapsamında güvence altına alınmış olan haklarından herhangi birisinin ihlal edilmesi halinde bir yargı yoluna başvurma hakkına sahip olmalıdır.[259]

Avrupa Komisyonu, Genel Veri Koruma Tüzüğü[260] ve Genel Veri Koruma Direktifi[261]nden oluşan bir reform paketi önermiştir. Bu yeni Direktif mevcut Veri Koruma Çerçeve Kararı'nın yerine geçecek ve cezai konularda kolluk ve adli işbirliğine yönelik genel ilke ve kurallar getirecektir.

7.2.2. Kolluk ve sınır ötesi adli işbirliği alanlarında veri korumasına yönelik diğer özel hukuki düzenlemeler

Üye Devletler arasında belirli alanlardaki bilgi değişimleri, Veri Koruma Çerçeve Kararı'na ek olarak, sabıka kayıtlarından derlenen bilgilerin Üye Devletler arasında takası ile ilgili organizasyon ve içeriğe dair 2009/315/JHA sayılı Konsey Çerçeve Kararı ve bilgi değişimi ile ilgili olarak Üye Devletlerin mali istihbarat birimleri arasında işbirliğine yönelik düzenlemelere ilişkin 2000/642/JHA sayılı Konsey Kararı gibi çeşitli yasal metinlerle düzenlenmiştir.[262]

Bu noktada önemli olan husus, göçmenliğe dair verilerin takasının yetkili makamlar arasındaki sınır ötesi iş birliği[263] kapsamında giderek artan bir orana sahip olmasıdır. Hukukun bu alanı kolluk ve cezai işlere yönelik değildir ancak çoğu bakımdan kolluk ve adalet makamlarının işleriyle alakalıdır. Aynı durum AB'ye ithal veya AB'den ihraç edilen mallara dair veriler bakımından da geçerlidir. AB içerisinde yer alan iç sınırların kaldırılması dolandırıcılık riskini artırmış, Üye Devletlerin ulusal ve AB gümrük mevzuatına yönelik ihlalleri daha etkili bir

[258] *A.e.*, Madde 19.
[259] *A.e.*, Madde 20.
[260] Avrupa Komisyonu (2012), *Kişisel verilerin işlenmesi bakımından gerçek kişilerin korunması ve bu kişisel verilerin serbest dolaşımına ilişkin Tüzük önerisi*, COM(2012) 11 final, Brüksel, 25 Ocak 2012.
[261] Avrupa Komisyonu (2012), *Kişisel verilerin işlenmesi bakımından gerçek kişilerin korunması ve bu kişisel verilerin serbest dolaşımına, cezai suçların önlenmesine, soruşturulmasına, tespit edilmesine veya kovuşturulmasına veya para cezalarının infaz edilmesine ilişkin Direktif Önerisi*, COM(2012) 11 final, Brüksel, 25 Ocak 2012.
[262] Avrupa Birliği Konseyi (2009), 26 Şubat 2009 tarihli ve 2009/315/ JHA Sayılı, Üye Devletler arasındaki sabıka kaydından alınan bilgilerin aktarılmasına ilişkin organizasyonu ve içeriği hakkında Konsey Çerçeve Kararı, OJ 2009 L 93; Avrupa Birliği Konseyi (2000), 17 Ekim 2000 tarihli ve 2000/642 / JHA Sayılı, Üye Devletlerin bilgi istihbarat birimlerinin bilgi alışverişi açısından işbirliğine yönelik düzenlemeler hakkında Konsey Kararı, OJ 2000 L 271.
[263] Avrupa Komisyonu (2012), Komisyon'dan Avrupa Parlamentosu ve Konseye Bildirim - AB'de kolluk kuvvetlerinin güçlendirilmesi: Avrupa Bilgi Paylaşımı Modeli (EIXM), COM(2012) 735 final, Brüksel, 7 Aralık 2012.

şekilde tespiti ve kovuşturabilmesi için, özellikle de sınır ötesi bilgi takasını geliştirme yoluyla, işbirliğini kuvvetlendirmesini gerekli kılmıştır.

Prüm Kararı

Ulusal olarak saklanan verilerin takası yoluyla kurumsallaşmış sınır ötesi işbirliğinin önemli örneklerinden birisi Prüm Antlaşmasını 20008 yılında AB hukuku içerisine dahil eden, özellikle terörizm ve sınırı aşan suçlarla mücadelede sınırı aşan işbirliğini geliştirmeye dair 2008/615/JHA sayılı Konsey Kararıdır. (Prüm Kararı).[264] Prüm Antlaşması, 2005 yılında Avusturya, Belçika, Fransa, Almanya, Lüksemburg, Hollanda ve İspanya tarafından imzalanmış olan bir uluslararası polis işbirliği antlaşmasıdır.[265]

Prüm Kararı'nın amacı üç farklı alanda suçun önlenmesi ve suçla mücadele amacıyla bilgi paylaşımının geliştirilmesi için Üye Devletlere yardım etmektir: terörizm, sınır ötesi suç ve yasa dışı göç. Bu amaçla, karar aşağıdaki konularla alakalı hükümler öngörmektedir:

- DNA profillerine, parmak izi verilerine ve bazı ulusal araç sicil verilerine otomatik erişim;
- Sınır ötesi boyuta sahip büyük ölçekli vakalara ilişkin verilerin sağlanması;
- Terör suçlarını engellemek adına bilgilerin sağlanması;
- Sınır ötesi polis işbirliğini artıracak diğer yollar.

Prüm Kararı kapsamında sağlanan veri tabanlarına dair hususlar tamamen ulusal hukuk tarafından belirlenmiştir ancak verilerin takası Prüm Kararı ve güncel olarak Veri Koruma Çerçeve Kararı tarafından düzenlenmektedir. Bu şekildeki veri akışlarının denetimiyle alakalı olarak yetkili kuruluşlar ulusal veri koruma denetim makamlarıdır.

7.2.3. Europol ve Eurojust'ta Veri Koruma
Europol

AB'nin polis teşkilatı olan Europol'ün merkezi Lahey'de olup her bir Üye Devlet'te Europol Ulusal Birimleri (EUBler) bulunmaktadır. Europol 1998 yılında kurulmuştur; bir AB kuruluşu olarak mevcut yasal statüsü Avrupa Polis Teşkilatı'nın kuruluşuna dair Konsey Kararı'na dayanmaktadır (Europol Kararı).[266] Europol'ün görevi, iki veya daha fazla Üye Devlet'i etkileyen ve Europol Kararı'nın ekinde listelenmiş olan organize suç, terörizm ve diğer ağır suç türlerinin önlenmesi ve soruşturulması konularında destek vermektir.

[264] Avrupa Birliği Konseyi (2008), Özellikle terörizm ve sınır ötesi suçlarla mücadelede sınır ötesi işbirliğinin artırılmasına ilişkin, 23 Haziran 2008 tarihli ve 2008/615 / JHA Sayılı Konsey Kararı, OJ 2008 L 210.

[265] Belçika Krallığı, Almanya Federal Cumhuriyeti, İspanya Krallığı, Fransa Cumhuriyeti, Lüksemburg Büyük Dükalığı, Hollanda Krallığı ve Avusturya Cumhuriyeti arasında sınır ötesi işbirliğinin artırılması, özellikle de Terör, sınır ötesi suç ve yasadışı göçle mücadeleye ilişkin Sözleşme; bkz.:
http://register.consilium.europa.eu/pdf/en/05/st10/ st10900.en05.pdf.

[266] Avrupa Birliği Konseyi (2009), Avrupa Polis Teşkilatını kuran 6 Nisan 2009 tarihli Konsey Kararı, OJ 2009 L 121 (Europol). Komisyon'un yönetmelik önerisini Bakınız, Avrupa Polis Bürosunu (Europol) kuran 6 Nisan 2009 tarihli, 2009/371 / JHA Sayılı, Konsey Kararı ile kurulan Europol'ün Ve Avrupa Polis Kolejini (CEPOL) kuran, 2005/681 / JHA Sayılı, Konsey Kararı ile kurulan CEPOL'ün yerine geçen yeni bir Europol için yasal bir çerçeve oluşturmaktadır, COM (2013) 173 final.

Europol bu amaçlarını yerine getirebilmek adına, Üye Devletler'in EUBleri aracılığıyla cezai istihbaratlarını ve bilgilerini takas edebilecekleri bir veri tabanı sağlayan Europol Bilgi Sistemi'ni kurmuştur. Europol Bilgi Sistemi, şüpheli konumundaki veya Europol'ün yetki alanı kapsamındaki bir suçtan hüküm giymiş kişiler veya haklarında bu tür suçları işleyeceklerine dair gerçeklere dayalı emareler bulunan kişilerle alakalı verilerin temini için kullanılabilir. Europol ve EUBler Europol Bilgi Sistemi'ne doğrudan veri girebilir ve sistemden veri çekebilirler. Sisteme girilmiş olan bir veriyi yalnızca o girişi yapan taraf değiştirebilir, düzeltebilir veya silebilir.

Görevlerini yerine getirmesi için gerekli olması durumunda Europol, suçlara dair verileri analiz çalışma dosyalarında saklayabilir, değiştirebilir ve kullanabilir. Analiz çalışma dosyaları, Europol'ün AB Üye Devletleri ile birlikte yürüttüğü somut cezai soruşturmaların desteklenmesi amacına yönelik olarak verilerin birleştirilmesi, işlenmesi veya kullanılması için açılırlar.

Yeni gelişmeler karşısında, 1 Ocak 2013 tarihinde Europol'de Avrupa Siber Suç Merkezi kurulmuştur.[267] Bu merkez AB'nin siber suçlara yönelik bilgi merkezi olarak hizmet vermektedir ve çevrimiçi suçlar karşısında verilecek tepkilerin hızlandırılmasına, adli bilişim altyapısının geliştirilmesine ve yayılmasına ve sanal ortamda işlenen suçların soruşturulmasıyla alakalı en iyi uygulamanın ortaya konmasına katkı sağlamayı hedeflemektedir. Merkez aşağıdaki nitelikleri taşıyan siber suçlar üzerinde yoğunlaşmaktadır:

- Bir örgüt tarafından büyük ölçekte yasa dışı menfaat sağlamak amacıyla işlenmiş olma, örneğin çevrimiçi dolandırıcılık;
- Mağdura ciddi zarar verme, örneğin çocuklara yönelik olarak çevrimiçi yollarla gerçekleştirilen cinsel istismar;
- AB'de bulunan hassas altyapıları ve bilgi sistemlerini etkileme.

Europol'ün faaliyetlerini düzenleyen veri koruma rejimi geliştirilmiştir. Europol Kararı'nın 27. maddesinde, 108 Sayılı Sözleşme ve otomatik veya otomatik olmayan yollarla işlenen verilerle alakalı olarak Kolluk Verileri Tavsiye Kararı kapsamında belirlenen ilkelerin uygulama alanı bulacağı belirtilmektedir. Europol ve Üye Devletler arasında gerçekleştirilecek veri aktarımları bakımından Veri Koruma Çerçeve Kararı'nda yer alan kurallara da uyulması gerekmektedir.

Geçerli veri koruma hukukuna uyumun sağlanması ve özellikle de bireylerin haklarının kişisel verilerin işlenmesi sebebiyle ihlal edilmemesi adına bağımsız nitelikteki Europol Ortak Denetim Organı (ODO) Europol'ün faaliyetlerini gözden geçirir ve denetler.[268] Herkes, Europol tarafından tutulan kendisine ait kişisel verilere erişim hakkına ve ayrıca verilerin kontrol edilmesini, düzeltilmesini veya silinmesini isteme hakkına sahiptir. Kişi bu hakların kullanılmasıyla alakalı olarak Europol'ün verdiği karardan memnun kalmazsa ODO Temyiz Komitesi'ne itiraz edebilir.

Kişi, Europol tarafından saklanan ve işlenen kişisel verilerdeki yasal veya fiili bir hatadan dolayı zarara uğrarsa, sadece zarara sebebiyet veren olayın gerçekleştiği Üye Devletin yetkili mahkemesine başvurmak yoluyla tazminat talebinde bulunabilir.[269] Zararın Europol'ün yasal

[267] Bakınız Avrupa Veri Güvenliği Gözetmeni (EDPS) (2012), Veri Güvenliği Gözetmeni'nin Avrupa Komisyonundan Konseye ve Avrupa Parlamentosuna, Avrupa Siber Suç Merkezi'nin kurulmasına ilişkin Bildirimin üzerine verdiği Görüş, Brüksel, 29 Haziran 2012.
[268] Europol Kararı, Madde34.
[269] *A.e.*, Madde52.

yükümlülüklerinden birisini yerine getirmemesi sebebiyle oluşmuş olması durumunda Europol, Üye Devlet'in yaptığı masrafları karşılayacaktır.

Eurojust

2002 yılında kurulmuş olan ve merkezi Lahey'de bulunan Eurojust, en az iki Üye Devlet'i ilgilendiren ağır suçların kovuşturma ve soruşturma aşamalarında adli işbirliğini teşvik eden bir AB organıdır.[270] Eurojust'ın yetkileri şöyledir:

- çeşitli Üye Devletlerin yetkili makamları arasında soruşturma ve kovuşturmaların koordinasyonu teşvik etmek ve geliştirmek;
- adli işbirliğine ilişkin taleplerin ve kararların yürütülmesini kolaylaştırmak.

Eurojust'ın işlevleri ulusal üyeler tarafından yerine getirilmektedir. Her Üye Devlet statüsü ulusal hukuka tabi olan ve adli işbirliğini teşvik ve geliştirme için gereken görevleri yerine getirmeye yetecek yetkilerle donatılmış bir yargıç veya savcıyı Eurojust'a temsilci olarak atar. Buna ek olarak, ulusal üyeler özel Eurojust görevlerini yürütmek için bir birlik halinde hareket ederler.

Eurojust, amaçlarına ulaşması için gerekli olduğu kapsamda kişisel verileri işleyebilir. Ancak bu işleme, Europol'ün yetki alanına giren bir suç işlediği veya böyle bir suça karıştığından şüphelenilen veya böyle bir suçtan mahkûm olmuş kişilere ilişkin bilgilerle sınırlıdır. Eurojust kendi yetki alanına giren suçlara şahit olmuş veya bu suçların mağduru olmuş kişilerle alakalı bazı bilgileri de işleyebilir.[271] Eurojust, istisnai durumlarda ve belirli bir süreyle sınırı olmak üzere, verilerin devam eden bir soruşturmayla doğrudan doğruya alakalı olması halinde bir suça ilişkin kişisel verileri daha kapsamlı olarak işleyebilir. Europol, yetki alanı içerisindeki konularla alakalı olarak diğer AB kuruluşları, organları ve ajansları ile işbirliği yapabilir ve kişisel verileri bu kurumlarla takas edebilir. Eurojust üçüncü ülkeler ve kurumlarla da işbirliği yapabilir ve kişisel veri alışverişinde bulunabilir.

Verilerin korunmasına ilişkin olarak, Eurojust en azından 108 Sayılı Sözleşme ve bu sözleşmede sonradan yapılan değişikliklerde yer alan ilkelere eşdeğer bir koruma seviyesini garanti etmelidir. Veri alışverişi durumlarında, Eurojust Konsey Kararları ve Eurojust Veri Koruma Kuralları'na uygun olarak yürürlüğe konmuş olan işbirliği sözleşmeleri veya çalışma düzenlemeleri içerisindeki özel kurallar ve sınırlamalara riayet edilmelidir.[272]

Eurojust içerisinde, Eurojust tarafından yürütülen kişisel veri işlemelerini denetlemekle görevli bağımsız bir ODO bulunmaktadır. Bireyler, Eurojust'un kişisel verilere yönelik olarak yapılan bir erişim, düzeltme, engelleme veya sildirme talebine verdiği cevaptan memnun olmazlarsa ODO'ya itirazda bulunabilirler. Eurojust kişisel verileri hukuka aykırı olarak işlerse, veri öznesine vermiş olduğu her türlü zarardan dolayı merkezinin bulunduğu yer olan Hollanda'nın ulusal hukuku uyarınca sorumlu olacaktır.

---

[270] Avrupa Birliği Konseyi (2002), Ağır suçlarla mücadeleyi güçlendirmek amacıyla Eurojust'i kuran 28 Şubat 2002 tarihli ve 2002/187/JHA Sayılı Konsey Kararı, OJ 2002 L 63; Avrupa Birliği Konseyi (2003), Ciddi suçlarla mücadeleyi güçlendirmek amacıyla Eurojust'i kuran 2002/187/JHA Sayılı kararını değiştiren 18 Haziran 2003 tarihli ve 2003/659 / JHA Sayılı Konsey Kararı, OJ 2003 L 44; Avrupa Birliği Konseyi (2009), Eurojust'i güçlendirme ve 2002/187/JHA Sayılı kararını değiştirmeye ilişkin 16 Aralık 2008 tarihli ve 2009/426 / JHA Sayılı Konsey Kararı, ağır suçla mücadeleyi güçlendirmek amacıyla Eurojust'i kurdu, OJ 2009 L 138 (Eurojust Kararları).

[271] 2003/659/JHA Sayılı Konsey Kararı ve 2009/426/JHA Sayılı, Madde15 (2) Konsey Kararı ile değiştirilen 2002/187/JHA Konsey Kararının konsolide versiyonu.

[272] Kişisel Verilerin İşlenmesine ve Korunmasına İlişkin Usul Kuralları Eurojust, OJ 2005 C 68/01, 19 Mart 2005, s. 1.

7.2.4. AB düzeyindeki ortak bilgi sistemlerinde verilerin korunması

Üye Devletler arasındaki bilgi alışverişi ve sınır ötesi suçla mücadeleye yönelik özel AB makamlarının yaratılmasına ek olarak, göç ve gümrük hukuku kapsamındakiler de dahil olmak üzere kolluğun görevlerini yerine getirebilmesi amacıyla, yetkili ulusal ve AB makamları arasında veri alışverişi için bir platform oluşturmak üzere birçok ortak bilgi sistemi kurulmuştur. Bu sistemlerden bazıları, sonradan Schengen Bilgi Sistemi, Vize Bilgi Sistemi, Eurodac, Eurosur veya Gümrük Bilgi Sistemi gibi AB yasal düzenlemeleri ve sistemler tarafından eklemeler yapılan çok taraflı sözleşmelerle ortaya çıkmıştır.

2012 yılında kurulmuş olan Avrupa Büyük ölçekli bilişim teknolojisi sistemleri ajansı (eu-LISA),[273] ikinci nesil Schengen Bilgi Sistemi'nin (SIS II), Vize Bilgi Sistemi'nin (VIS) ve Eurodac'ın uzun vadedeki operasyonel yönetiminden sorumludur. Eu-LISA'nın ana görevi bilişim teknolojileri sistemlerinin etkili, güvenli ve sürekli çalışmasını sağlamaktır. Ayrıca sistemlerin ve verilerin güvenliğini sağlamak için gerekli tedbirlerin alınmasından da sorumludur.

Schengen Bilgi Sistemi

1985 yılında, eski Avrupa Toplulukları Üye Devletleri'nin birkaçı bir araya gelmiş ve Benelüks Ekonomik Birliği, Almanya ve Fransa devletleri arasında, kişilerin serbest ve Schengen bölgesindeki sınır kontrolleriyle engellenmeksizin dolaşımının söz konusu olacağı bir alan yaratmak amacıyla ortak sınırların kademeli olarak ortadan kaldırılmasına yönelik bir Antlaşma'yı (Schengen Antlaşması) kabul etmişlerdir.[274] Sınırların kaldırılması sebebiyle kamu güvenliğine yönelik olarak oluşabilecek tehditleri dengelemek için de Schengen bölgesinin dış sınırlarındaki kontroller sıkılaştırılmış ve ulusal emniyet ve yargı makamları arasında yakın işbirliği kurulmuştur.

Schengen Antlaşması'na yeni devletlerin katılımının bir sonucu olarak, Schengen sistemi en sonunda Amsterdam Antlaşması ile AB yasal çerçevesi içerisine dahil edilmiştir.[275] Bu kararın uygulamaya geçişi 1999 yılında gerçekleşmiştir. Schengen Bilgi Sisteminin yeni hali SIS II, 9 Nisan 2013'te faaliyete geçmiştir. Şu anda tüm AB Üye Devletleri ve buna ek olarak İzlanda, Lihtenştayn, Norveç ve İsviçre tarafından kullanılmaktadır.[276] Europol ve Eurojust'ın da SIS II'ye erişimi bulunmaktadır.

SIS II, merkezi bir sistemden (C-SIS), her Üye Devlette bulunan bir ulusal sistemden ve merkezi sistem ile ulusal sistemler arasındaki bir iletişim altyapısından oluşmaktadır (N-SIS). C-SIS kişilere ve nesnelere ilişkin olarak Üye Devletler tarafından kaydedilen bazı verileri

[273] Avrupa Birliği Parlamentosu ve Konseyi'nin, 1077/2011 Sayılı, Özgürlük, güvenlik ve adalet alanında büyük ölçekli BT sistemlerinin operasyonel yönetimi için bir Avrupa Ajansı'nın kurulmasına ilişkin Tüzüğü, 25 Ekim 2011, OJ 2011 L 286.

[274] Benelüks Ekonomik Birliği, Federal Almanya Cumhuriyeti ve Fransa Cumhuriyeti Devletlerinin Hükümetleri arasındaki ortak sınırlardaki kontrollerin kademeli olarak kaldırılması üzerine yapılan anlaşma, OJ 2000 L 239.

[275] Avrupa Toplulukları (1997), Avrupa Birliği Antlaşmasını tadil eden Amsterdam Antlaşması, Avrupa Topluluklarını Kuran Antlaşmalar ve diğer ilgili kanunlar, OJ 1997 C 340.

[276] Avrupa Birliği Parlamentosu ve Konseyi'nin, 1987/2006 Sayılı, 20 Aralık 2006 tarihli, İkinci nesil Schengen Bilgi Sisteminin kurulması, işletilmesi ve kullanımı hakkında Tüzüğü, (*SIS II*), OJ 2006 L 381, ve Avrupa Birliği Konseyi (2007), 2007/533/JHA Sayılı, 12 Haziran 2007 tarihli, ikinci nesil Schengen Bilgi Sisteminin (SIS II) kurulması, işletilmesi ve kullanımı hakkında Konsey Kararı OJ 2007 L 205.

içerir. C-SIS, Schengen bölgesinde yer alan ulusal sınır kontrolü, polis, gümrük, vize ve yargı makamlarının tamamı tarafından kullanılmaktadır. Her bir Üye Devlet, C-SIS'in Ulusal Schengen Bilgi Sistemi (N-SIS) olarak da bilinen ve sürekli olarak güncellenen ve dolayısıyla C-SIS'i de güncelleyen ulusal bir kopyası üzerinden çalışır. Aşağıda N-SIS'e başvurulmasını gerektirecek ve aynı zamanda sistemin uyarı vermesine sebep olacak durumlar listelenmektedir:

- kişinin Schengen bölgesine giriş veya bölgede kalma hakkı bulunmuyorsa; veya
- kişi adli makamlar veya kolluk kuvvetleri tarafından aranmakta ise; veya
- kişi kayıp olarak görünmekte ise; veya
- banknotlar, arabalar, kamyonetler, ateşli silahlar ve kimlik belgeleri gibi malların çalıntı veya kayıp olarak raporlanmış olduğu durumlarda.

Sistemin uyarı vermesi durumunda, akabinde izlenecek prosedür Ulusal Schengen Bilgi Sistemleri aracılığıyla başlatılacaktır.

SIS II'nin parmak izi ve fotoğraf gibi biyometrik verileri veya çalıntı tekneler, uçaklar, konteyner veya ödeme araçları şeklinde yeni uyarı kategorilerini ve kişilere ve nesnelere ilişkin gelişmiş uyarıları; tutuklama, teslim veya iade için aranan kişilere ait Avrupa Tutuklama Emirleri'nin (ATEler) kopyalarını sisteme girme gibi yeni işlevleri de bulunmaktadır.

İkinci kuşak Schengen Bilgi Sistemi'nin (SIS II) kurulması, işletilmesi ve kullanılmasına ilişkin 2007/533/JHA sayılı Konsey Kararı (Schengen II Kararı) 108 Sayılı Sözleşme'yi de uygulama kapsamına dahil etmiştir: "Bu kararın uygulaması sırasında işlenen kişisel veriler 108 Sayılı Sözleşme uyarınca korunmalıdır".[277] Kişisel verilerin Schengen II Kararı'nın uygulaması kapsamında ulusal emniyet makamları tarafından kullanımı söz konusu olduğunda, 108 Sayılı Sözleşme'nin hükümleri ve Kolluk Veri Tavsiye Kararı ulusal hukuk içerisinde uygulanmalıdır.

Her bir Üye Devlet'te bulunan yetkili denetim makamı ulusal N-SIS'i denetler. Özellikle, Üye Devlet'in N-SIS aracılığıyla C-SIS'e girdiği verilerin kalitesini kontrol etmelidir. Ulusal denetim makamı, ulusal N-SIS içerisinde yapılan veri işleme faaliyetlerinin en az dört senede bir denetimden geçtiğinden emin olmalıdır. Ulusal denetim makamları ve EDPS işbirliği yaparlar ve SIS'in eşgüdümlü bir şekilde denetlenmesini sağlarlar. C-SIS'in denetlenmesi yükümlülüğü EDPS'ye aittir. Şeffaflığı sağlamak adına bir ortak faaliyet raporu her iki senede bir Avrupa Parlamentosu'na, Avrupa Konseyi'ne ve eu-LISA'ya gönderilir.

N-SIS'lerin her biri C-SIS sisteminin eksiksiz birer kopyası olduğundan, bireylerin SIS II'ye erişim hakları Üye Devletler'den herhangi birisinde kullanılabilir.

Örnek: **'Dalea v. Fransa'**[278] davasında, başvuranın Fransa'yı ziyaret etmek için yapmış olduğu vize başvurusu, Fransız makamları'nın başvurunun reddedilmesi gerektiği yönünde Schengen Bilgi Sistemi'ne yaptıkları bildirim sebebiyle reddedilmiştir. Başvuran Fransız Veri Koruma Komisyonu ve son olarak Danıştay nezdinde erişim ve düzeltme veya silme talebinde bulunmuştur ancak bu başvurular olumsuz sonuçlanmıştır. AİHM başvuranla alakalı olarak Schengen Bilgi Sistemi'ne bildirimde bulunulmasının kanuna uygun olduğunu ve ulusal güvenliğini koruma şeklindeki meşru bir amaçla yapıldığını ifade etmiştir. Başvuran Schengen

[277] Avrupa Birliği Konseyi (2007), 2007/533 / JHA Sayılı, 12 Haziran 2007 tarihli, İkinci nesil Schengen Bilgi Sistemi' nin kurulması, işletilmesi ve kullanılması hakkında Konsey Kararı, OJ 2007 L 205, Madde 57.
[278] AİHM, *Dalea v. France* (dec.), No. 964/07, 2 Şubat 2010.

bölgesine giriş talebinin reddi sebebiyle ne şekilde bir zarara uğradığını ortaya koyamadığından ve başvuranı keyfi kararlardan korumak için yeterli olan tedbirler alınmış olduğundan, başvuranın özel hayatına saygı gösterilmesi hakkına yapılan bu müdahale orantılıdır. Bu sebeple ilgilinin AİHS madde 8 kapsamındaki başvurusu kabul edilemez bulunmuştur.

Vize Bilgi Sistemi

Eu-LISA tarafından da işletilen Vize Bilgi Sistemi (VIS), ortak bir AB vize politikasının uygulamasını desteklemek amacıyla geliştirilmiştir.[279] VIS, Schengen devletlerinin AB üyesi olmayan ve Schengen bölgesinin dış sınırında geçiş noktalarına sahip bütün ülkelerdeki konsolosluklarını birbirine bağlayan bir sistem üzerinden devletlerin vize verilerini takas edebilmelerine imkân tanımaktadır. VIS Schengen bölgesini ziyaret veya transit geçiş amaçlı kısa süreli vize başvurularıyla alakalı verileri işler. VIS, sınır makamlarının vizeyi elinde tutan kişinin gerçek hak sahibi olup olmadığını biyometrik verilerin de yardımıyla doğrulayabilmelerini ve herhangi bir belgeye sahip olmayan veya sahte belgeler sunan kişilerin kimliklerini tespit edebilmelerini sağlamaktadır.

Vize Bilgi Sistemi (VIS) ve kısa süreli vizelere istinaden Üye Devletler arasındaki veri değişimine ilişkin Avrupa Parlamentosu ve Konseyi'nin (EC) 767/2008 sayılı Tüzüğü (VIS Tüzüğü) uyarınca yalnızca başvurana ilişkin veriler, vizeleri, fotoğrafları, parmak izleri, önceki başvurularının numaraları, ve başvurana eşlik eden kişilerin başvuru dosyaları VIS'e kaydedilebilir.[280] VIS'e veri girme, düzeltme veya silme amacıyla erişim yetkisi Üye Devletler'in vize makamlarıyla sınırlıyken, verilere danışma amacıyla erişim yetkisi vize makamlarına ve dış sınır geçiş noktalarında sınır, göç ve iltica kontrolü yapmaya yetkili makamlara tanınmıştır. Belirli şartlar altında, ulusal yetkili emniyet makamları ve Europol da VIS'e girilmiş olan verilere, terörist aktiviteler ve suçların önlenmesi, tespiti ve soruşturulması amacıyla erişim talep edebilir.[281]

Eurodac

Eurodac'ın adı daktilogram olarak da bilinen parmak izlerine göndermede bulunmaktadır. AB Üye Devletleri'nden birisine sığınma talebinde bulunan üçüncü ülke vatandaşlarına ait parmak izi verilerini barındıran merkezi bir sistemdir.[282] Sistem 2003 Ocak ayından beri faaliyettedir ve amacı da belirli bir sığınma başvurusunu Üçüncü bir ülke vatandaşı tarafından Üye

[279] Avrupa Birliği Konseyi (2004), Vize Bilgi Sistemini (VIS) kuran 8 Haziran 2004 tarihli Konsey Kararı, OJ 2004 L 213; 767/2008 Sayılı, Avrupa Parlamentosu ve Konseyi, Vize Bilgi Sistemi (VIS) ve kısa süreli vizelere ilişkin Üye Devletler arasındaki veri alış verişi ile ilgili olarak düzenlenen Tüzük, 9 Temmuz 2008, OJ 2008 L 218; Avrupa Birliği Konseyi (2008), 2008/633/JHA Sayılı, Terör suçlarının ve diğer ağır cezai suçların önlenmesi, tespiti ve soruşturulması amacıyla Üye Devletlerin belirlenmiş mercileri ve Europol tarafından Vize Bilgi Sistemine (VIS) erişim konusunda Konsey Kararı, 23 Haziran 2008, OJ 2008 L 218.

[280] Avrupa Parlamentosu ve Konseyi, 767/2008 Sayılı, Vize Bilgi Sistemi (VIS) ve kısa süreli vizelere ilişkin Üye Devletler arasındaki veri alış verişi ile ilgili olarak düzenlenen Tüzük, 9 Temmuz 2008, OJ 2008 L 218,Madde 5.

[281] Avrupa Birliği Konseyi (2008), 2008/633/JHA Sayılı, Terör suçlarının ve diğer ağır cezai suçların önlenmesi, tespiti ve soruşturulması amacıyla Üye Devletlerin belirlenmiş mercileri ve Europol tarafından Vize Bilgi Sistemine (VIS) erişim konusunda Konsey Kararı, 23 Haziran 2008, OJ 2008 L 218.

[282] 2725/2000(AT) Sayılı, Dublin Sözleşmesi'nin etkili bir şekilde uygulanması için parmak izlerinin karşılaştırılmasına dair Eurodac'ın kurulmasına ilişkin Konsey Tüzüğü,11 Aralık 2000, OJ 2000 L 316; (AT) 407/2002 Sayılı, 2725/2000 (AB) Sayılı Yönetmeliğin uygulanmasına yönelik Dublin Sözleşmesinin etkili bir şekilde uygulanması ve parmak izlerinin karşılaştırılması için Eurodac'ın kurulmasına ilişkin belirli kuralların belirlenmesine dair Konsey Tüzüğü, 28 Şubat 2002, OJ 2002 L 62 (Eurodac Yönetmelikleri).

Devletler'den birinde yapılan iltica başvurularının incelenmesinden sorumlu devletin saptanması için kriter ve mekanizmaların kurulmasına yönelik 343/2003/EC sayılı Konsey Tüzüğü (Dublin II Tüzüğü) uyarınca hangi Üye Devlet'in incelemekle sorumlu olduğunu belirleme konusunda destek sunmaktır.[283] Eurodac'ta bulunan kişisel veriler sadece Dublin II Tüzüğü'nün uygulamasını kolaylaştırmak amacıyla kullanılabilirler; başka herhangi bir kullanım cezaya tabidir.

Eurodac eu-LISA tarafından işletilen ve parmak izlerinin saklanması ve karşılaştırılması ve Üye Devletler ve merkezi veri tabanı arasında elektronik veri aktarımı için kurulmuş merkezi bir birimden oluşmaktadır. Üye Devletler, kendilerine sığınma talebinde bulunan veya dış sınırı izinsiz olarak geçtiği sırada yakalanmış ve AB vatandaşı olmayan veya vatansız konumdaki 14 yaşını doldurmuş bütün kişilerin parmak izlerini alır ve aktarır. Üye Devletler izinsiz olarak sınırları içerisinde kaldığını tespit ettikleri AB dışı bir ülkenin vatandaşı veya vatansız bütün kişilerin parmak izlerini alabilir ve aktarabilirler.

Eurodac veri tabanındaki parmak izi verileri yalnızca takma isim ile değiştirilmiş biçimde saklanırlar. Bir eşleşme durumunda takma isim, parmak izi verisini aktaran ilk Üye Devlet'in de ismiyle birlikte ikinci Üye Devlet'e ifşa olunur. Söz konusu ikinci Üye Devlet sonrasında birinci Üye Devlet'e başvuracaktır çünkü Dublin II Tüzüğü uyarınca ilk Üye Devlet sığınma başvurusunu işleme koymak ve incelemekle sorumludur.

Sığınma başvurusunda bulunanlara ilişkin olarak Eurodac'ta saklanan kişisel veriler, veri öznesi bir AB Üye Devleti'nin vatandaşlığına geçmediği takdirde, parmak izlerinin alındığı tarihten itibaren on yıl süreyle tutulurlar. Eğer başvuru sahibi Üye Devletlerden birisinin vatandaşı olursa, veriler derhal silinmelidir. Dış sınırları izinsiz olarak geçtiği için tutuklanan yabancı ülke vatandaşlarına ilişkin veriler iki yıl boyunca tutulurlar. Veri öznesinin oturma izni alması, AB bölgesinden ayrılması veya bir Üye Devletin vatandaşlığına geçmesi durumunda bu veriler derhal silinmelidir.

AB Üye Devletleri'nin hepsine ek olarak ayrıca İzlanda, Norveç, Lihtenştayn ve İsviçre de uluslararası sözleşmeler çerçevesinde Eurodac kullanmaktadırlar.

Eurosur

Avrupa Sınır Gözetleme Sistemi (Eurosur) yasadışı göçün ve sınır ötesi suçların tespiti, önlenmesi ve bunlarla mücadele yoluyla Schengen dış sınırlarının kontrolünü geliştirmek için tasarlanmıştır.[284] Bilgi değişimini ve ulusal koordinasyon merkezleri ve entegre sınır yönetimi isimli yeni konsepti geliştirmek ve uygulamakla görevli AB ajansı olan Frontex arasındaki operasyonel işbirliğini geliştirme amacını taşır.[285] Genel hedefleri şunlardır:

- AB'ye fark edilmeden giren yasa dışı göçmenlerin sayısını azaltmak;
- denizde daha fazla hayat kurtarmak yoluyla yasa dışı göçmen ölümlerini azaltmak;

[283] 343/2003 Sayılı, Üçüncü ülke vatandaşları tarafından yapılan sığınma başvuruları'nın incelenmesinden sorumlu Üye Devletin belirlenmesine yönelik kriterleri ve mekanizmaları belirleyen Konsey Tüzüğü, OJ 2003 L 50 (Dublin II Tüzüğü).
[284] Avrupa Sınır Gözetim Sistemi (Eurosur)'ni tesis eden, Avrupa Parlamentosu ve Konseyi'nin 1052/2013/AB Sayılı ve 22 Ekim 2013 tarihli Tüzüğü, OJ 2013 L 295.
[285] 1168/2011 Sayılı, 25 Ekim 2011 tarihli, Avrupa Birliği Parlamentosu ve Konseyi, Avrupa Birliği'nin Üye Devletlerinin Dış Sınırlarda Operasyonel İşbirliği Yönetimi Ajansını tesis eden 2007/2004/AB Sayılı ve 26 Ekim 2004 tarihli Konsey Tüzüğü'nün değiştirilmesi üzerine yayınlanan Tüzük, OJ 2011 L 394 (*Frontex Tüzüğü*).

- sınır ötesi suçların önlenmesine katkıda bulunmak yoluyla AB'nin iç güvenliğini bir bütün olarak artırmak.[286]

Sistem, dış sınırlara sahip tüm Üye Devletlerde 2 Aralık 2013 tarihinde faaliyete geçti ve 1 Aralık 2014 tarihinden itibaren de kalan üye devletlerde kullanılmaya başlayacak. Tüzük, Üye Devletler'in kara ve deniz dış sınırları ve hava sahası sınırı bakımından uygulama alanı bulacaktır.

Gümrük Bilgi Sistemi

AB düzeyinde kurulan bir diğer önemli ortak bilgi sistemi Gümrük Bilgi Sistemi'dir (CIS).[287] İç pazarın kuruluşu sırasında malların AB bölgesinde dolaşımına ilişkin tüm kontrollerin ve formalitelerin kaldırılması dolandırıcılık riskini artırmıştır. Bu risk, Üye Devletler'in gümrük idareleri arasındaki güçlendirilmiş işbirliği ile dengelenmiştir. CIS'in amacı, özelikle ulusal ve AB gümrük ve tarım mevzuatına yönelik ağır ihlallerin önlenmesi, soruşturulması ve kovuşturulmasında Üye Devletlere yardımcı olmaktır.

CIS'te yer alan bilgiler mallara, taşıma araçlarına, işletmelere, kişilere, muhafaza edilen, haczedilen veya el koyulan mallara ve nakde ilişkin kişisel verilerden oluşmaktadır. Bu bilgiler sadece gümrük hükümlerini ihlal ettiğinden şüphelenilen kişilerle ilgili inceleme, raporlama ve belirli denetimlerin yapılması veya stratejik veya operasyonel analizlerin yapılması amacıyla kullanılabilir.

CIS'e erişim Europol ve Eurojust'ün yanı sıra, ulusal gümrük, vergilendirme, tarım, kamu sağlığı ve polis yetkililerine tanınmaktadır.

Kişisel verilerin işlenmesi VK Direktifi, AB Kurumları Veri Koruma Tüzüğü, 108 Sayılı Sözleşme ve Kolluk Veri Tavsiye Kararı hükümleri yanında 515/97 sayılı Tüzük ve CIS Antlaşması ile de uyum içinde olmalıdır.[288] EDPS, CIS'in (EC) 45/2001 sayılı Tüzük ile uyumunun denetlenmesinden sorumludur ve CIS ile bağlantılı denetimsel konular bakımından yetkili tüm ulusal veri koruma denetim kurumlarıyla senede bir kere olmak üzere toplantı yapmaktadır.

---

[286] Bakınız: Avrupa Komisyonu (2008), Avrupa Birliği Komisyonu tarafından Avrupa Birliği Parlamentosu, Konseyi ve Avrupa Ekonomik ve Sosyal Bölgeler Komitesi'ne yapmış olduğu, Avrupa Sınır Gözetim Sistemi (Eurosur)'un kuruluşu konulu bildirim, COM(2008) 68 final, Brüksel, 13 Şubat 2008; Avrupa Komisyonu (2011), Avrupa Sınır Gözetim Sistemini (Eurosur) kuran Avrupa Parlamentosu ve Konseyi'nin Tüzüğüne ek Etki Değerlendirmesi, Çalışma Belgesi, SEC(2011) 1536 final, Brüksel,12 Aralık 2011, s. 18.

[287] Avrupa Birliği Konseyi (1995), 26 Temmuz 1995 tarihli, Gümrük birimlerinde bilgi teknolojisi kullanımına ilişkin Sözleşme'nin hazırlanmasına ilişkin Konsey Yasası, OJ 1995 C 316, Avrupa Birliği Konseyi (2009) tarafından değiştirildi, Gümrük ve tarımsal konularda yasanın doğru bir şekilde uygulanmasını sağlamak için, Üye Devletlerin idari makamları arasındaki karşılıklı yardım ve Komisyon ve Üye Devletler arasındaki karşılıklı yardım üzerine, 13 Mart 1997 tarihli ve 515/97 Sayılı Tüzük, Gümrük amaçlı bilgi teknolojilerinin kullanımı ile ilgili, 30 Kasım 2009 tarihli, 2009/917/JHA Sayılı Konsey Kararı, OJ 2009 L 323 (*CIS Kararı*).

[288] *A.e.*

8. Avrupa veri koruma hukunda yer alan diğer düzenlemeler

AB	İşlenen konular	AK
Veri Koruma Direktifi Gizlilik ve Elektronik Haberleşme Direktifi	**Elektronik haberleşme**	108 Sayılı Sözleşme Haberleşme Hizmetleri Tavsiye Kararı
Veri Koruma Direktifi, Madde 8 (2) (b)	**İstihdam ilişkileri**	108 Sayılı Sözleşme İstihdam Tavsiye Kararı AİHM, *Copland v. the United Kingdom*, No. 62617/00, 3 Nisan 2007
Veri Koruma Direktifi, Madde 8 (3)	**Tıbbi veriler**	108 sayılı Sözleşme Tıbbi Veriler Tavsiye Kararı AİHM, *Z. v. Finland*, No. 22009/93, 25 Şubat 1997
Klinik Araştırmalar Direktifi	**Klinik araştırmalar**	
Veri Koruma Direktifi, Madde 6 (1) (b) ve (e), Madde 13 (2)	**İstatistikler**	108 Sayılı Sözleşme İstatiksel Veriler Tavsiye Kararı
(EC) 223/2009 sayılı Avrupa İstatistikleri Tüzüğü ABAD, C-524/06, *Huber v. Germany*, 16 Aralık 2008	**Resmi istatistikler**	108 Sayılı Sözleşme İstatiksel Veriler Tavsiye Kararı
2004/39/EC sayılı Finansal Araç Piyasaları Hakkında Avrupa Parlamentosu ve Konseyi Direktifi (EU) 648/2012 sayılı Tezgahüstü Türevler, Merkezi Karşı Taraflar ve Türev Kayıt Kuruluşları Tüzüğü 1060/2009 sayılı Kredi Derecelendirme Kuruluşları	**Finansal veriler**	108 Sayılı Sözleşme R (90) 19 sayılı Ödeme Ve Benzer Amaçlı Öteki İşlemlerde Kişisel Verilerin Korunması Hakkında Tavsiye Kararı AİHM, *Michaud v. France*, No. 12323/11, 6 Aralık 2012

Tüzüğü 2007/64/EC sayılı İç Pazarda Ödeme Hizmetleri Hakkında Direktif		

108 Sayılı Sözleşme veya VK Direktifi'nde belirlenen genel kuralları belirli durumlara yönelik olarak daha detaylı şekilde uygulayan özel yasal düzenlemelerin Avrupa düzeyinde kabul edildiği çok sayıda örnekle karşılaşmak mümkündür.

8.1. Elektronik Haberleşme

Ana başlıklar

- Haberleşme alanında, özelikle de telefon hizmetleri konusunda veri korumasına ilişkin özel kurallar 1995 tarihli AK Tavsiye Kararı içerisinde yer almaktadır.
- Haberleşme hizmetlerinin AB düzeyinde yerine getirilmesine ilişkin olarak kişisel verilerin işlenmesi konusu gizlilik ve elektronik haberleşme Direktifinde düzenlenmektedir.
- Elektronik haberleşmenin gizliliği bir iletişimin yalnızca içeriğine değil, aynı zamanda kimin kiminle, ne zaman ve ne kadar süreyle iletişime geçtiğine ve verilerin nereden iletildiğine dair konum bilgisine de ilişkindir.

Haberleşme ağları, bu ağlar üzerinden gerçekleştirilen iletişimin dinlenmesi ve gözetlenmesine yönelik yeni teknik imkânlar sunduklarından, kullanıcıların özel alanlarına haksız müdahale potansiyeli bakımından daha yüksek risk taşırlar. Bunun sonucu olarak, haberleşme hizmetleri kullanıcılarının karşılaştıkları özel riskleri giderebilmek için özel veri koruma düzenlemelerinin gerekli olduğuna karar verilmiştir.

1995 yılında, AK haberleşme alanında verilerin korunması için, özellikle de telefon hizmetlerine ilişkin olarak bir **Tavsiye Kararı yayınladı.**[289] Bu Karara göre, haberleşme bağlamında kişisel verilerin toplanması ve işlenmesi şunlarla sınırlı olmalıdır: bir kullanıcıyı şebekeye bağlamak, belirli bir haberleşme hizmetini sunmak, faturalama yapmak, doğrulamak, en uygun teknik operasyonu sağlamak ve şebeke ve hizmeti geliştirmek.

Doğrudan pazarlama mesajlarının gönderilmesi amacıyla haberleşme şebekelerinin kullanılması konusuna da özel bir ilgi gösterilmiştir. Genel bir kural olarak, tanıtım mesajı gönderim listesinden açık bir şekilde ayrılmış olan herhangi bir aboneye doğrudan pazarlama mesajları gönderilemez. Önceden kaydedilmiş tanıtım mesajlarını ileten otomatik arama cihazları ancak abonenin açık rızasını vermiş olması durumunda kullanılabilir. Ulusal hukuk bu alanda ayrıntılı kurallar sağlayacaktır.

AB yasal çerçevesine ilişkin olarak, 1997 yılındaki ilk denemeden sonra, gizlilik ve elektronik haberleşme Direktifi 2002 yılında kabul edilmiş ve VK Direktifi'nin haberleşme sektörü özelindeki hükümlerini tamamlamak ve ayrıntılandırmak amacı ile 2009 yılında

[289] Avrupa Konseyi, Bakanlar Komitesi (1995), Rec(95)4 Sayılı, Telekomünikasyon hizmetleri alanında kişisel verilerin korunması konusunda üye ülkelere, özellikle telefon hizmetlerine atıfta bulunarak verdiği Öneri, 7 Şubat 1995.

değiştirilmiştir.[290] Gizlilik ve elektronik haberleşme Direktifinin uygulaması kamusal elektronik şebekeler üzerinden verilen haberleşme hizmetleriyle sınırlıdır.

Gizlilik ve elektronik haberleşme Direktifi, haberleşme sürecinde oluşturulan verileri üç ana kategoriye ayırır:

- haberleşme sırasında gönderilen mesajların içeriğini oluşturan veriler; bu veriler çok gizlidir;
- trafik verileri olarak da bilinen, haberleşmenin kurulması ve sürdürülmesi için gereken veriler; örneğin haberleşmenin tarafları hakkında bilgiler, haberleşmenin zamanı ve süresi;
- trafik verileri içerisinde, konum verileri olarak da bilinen ve haberleşme cihazının özel olarak konumuna ilişkin veriler bulunur; bu veriler aynı zamanda haberleşme cihazlarının kullanıcılarının konumlarına ilişkin verilerdir ve özellikle de mobil haberleşme cihazlarının kullanıcıları bakımından önemlidir.

Trafik verileri hizmet sağlayıcısı tarafından sadece faturalandırma ve hizmeti teknik olarak sunmak amacıyla kullanılabilir. Ancak veri öznesinin rızası ile bu veriler, örneğin kullanıcının konumuna bağlı olarak en yakın metro istasyonu veya eczane veya hava tahminine dair bilgiler verme gibi katma değerli hizmetler sunan diğer veri sorumlularına ifşa edilebilirler.

Elektronik şebekeler üzerinden gerçekleşen haberleşmeye dair verilere yönelik suçların soruşturulması için erişim vb. diğer erişimler ise e-Gizlilik Direktifi'nin 15. maddesi uyarınca AİHS madde 8(2)'de yer verilen ve sonrasında Şart'ın 8. ve 52. maddeleri ile onaylanan verilerin korunması hakkına yönelik meşru müdahalelerde bulunması gereken koşulları karşılamalıdır.

Gizlilik ve elektronik haberleşme Direktifinde[291] 2009 yılında yapılan değişiklikle aşağıdaki düzenlemeler getirilmiştir:

- Doğrudan pazarlama amacıyla e-posta gönderimlerine yönelik kısıtlamalar kısa mesaj hizmetleri, çoklu ortam mesajlaşma hizmetleri ve benzer uygulamaları kapsayacak şekilde genişletilmiştir; önceden rıza alınmaksızın pazarlama e-postalarının gönderilmesi yasaklanmıştır. Böyle bir rıza yoksa, e-posta adreslerini vermiş olmaları ve gönderime itiraz etmemeleri kaydıyla yalnızca önceki müşterilere pazarlama e-postaları gönderilebilecektir.
- İstenmeyen haberleşmeye yönelik yasağın ihlaline karşı kanun yollarının sunulması sorumluluğu Üye Devletler'e yüklenmiştir.[292]

---

[290] Avrupa Parlamentosu ve Konseyinin, 12 Temmuz 2002 tarihli, 2002/58/AB Sayılı, Elektronik İletişim Sektöründe Kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin Direktifi, OJ 2002 L 201(Elektronik iletişim ve Gizlilik Direktifi), 2009/136/AB Sayılı, Avrupa Parlamentosu ve Konseyi Direktifi ile 25 Kasım 2009 tarihinde, 2002/22/AB Sayılı, Evrensel hizmet ve elektronik haberleşme şebekeleri ve hizmetleri ile ilgili kullanıcı hakları, 2002/58/AB Sayılı, Elektronik İletişim Sektöründe Kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin Direktif ve tüketici koruma kanunlarının uygulanmasından sorumlu ulusal makamlar arasındaki işbirliğine ilişkin 2006/2004 Sayılı Direktif değiştirilmiştir, OJ 2009 L 337.

[291] 2009/136/AB Sayılı, 25 Kasım 2009 tarihli, Avrupa Birliği Parlamentosu ve Konseyi Direktifi, 2002/22/AB Sayılı, Elektronik haberleşme şebekeleri ve hizmetleri ile ilgili evrensel hizmet ve kullanıcı hakları Direktifinde, 2002/58/AB Sayılı, Elektronik İletişim Sektöründe Kişisel verilerin işlenmesi ve gizliliğin korunmasına ilişkin Direktifte ve tüketici koruma kanunlarının uygulanmasından sorumlu ulusal makamlar arasındaki işbirliğine ilişkin 2006/2004 Sayılı Direktif değiştirilmiştir, OJ 2009 L 337.

[292] Değiştirilen Direktife bkz., Madde13.

- Bilgisayar kullanıcısının rızası olmaksızın, bir bilgisayar kullanıcısının hareketlerini izleyen ve kaydeden çerez ve yazılımların kullanılmasına artık izin verilmemektedir. Yeterli korumanın sağlanabilmesi için rızanın nasıl açıklanması ve alınması gerektiğiyle alakalı olarak ulusal hukukun detaylı düzenlemeler yapması gerekmektedir.[293]

Yetkisiz erişim, verilerin kaybı veya yok olması sonucunda bir veri ihlalinin gerçekleşmesi durumunda yetkili denetim makamı derhal bilgilendirilmelidir. Bu şekilde bir veri ihlalinin sebep olabileceği zararlarla alakalı olarak risk altında bulunan aboneler bilgilendirilmelidir.[294]

Veri Saklama Direktifi[295] (8 Nisan 2014 tarihinde iptal edilmiştir; bkz. aşağıda yer alan karar örneği) haberleşme hizmet sağlayıcılarını, özellikle de ağır suçlarla mücadele amacıyla, trafik verilerini bu verilere faturalandırma veya hizmeti teknik olarak sağlama amaçları için ihtiyaç kalıp kalmadığına bakmaksızın, en az altı ay ve en fazla yirmi dört aylık bir süreyle saklamakla yükümlü kılmıştır.

AB Üye Devletleri saklanan verilerin güvenliğinin denetiminden sorumlu bağımsız kamu makamlarını belirleyecektir.

Haberleşme verilerinin saklanması açık bir biçimde verilerin korunması hakkına müdahale etmektedir.[296] Yapılan bu müdahalenin haklı olup olmadığı hususu AB Üye Devletleri'nde çeşitli davalar kapsamında tartışılmıştır.[297]

Örnek: **'Digital Rights İrlanda ve Seitlinger ve Diğerleri'[298]** davasında, ABAD Veri Saklama Direktifi'nin hükümsüz olduğunu ilan etti. Mahkemeye göre, "direktifin dava konusu temel haklara yönelik geniş çaplı ve özellikle ağır müdahalesinin çerçevesi, müdahalenin yalnızca gerekli olanla sınırlı olmasının sağlanmasına yetecek kesinlikte çizilmemiştir."

Elektronik haberleşme bağlamında hayati bir konu kamu makamları tarafından yapılan müdahalelerdir. Cihaz takibi ve dinlemesi gibi gözetleme veya haberleşmeye müdahale yöntemleri ancak kanunla düzenlenmiş olmaları ve demokratik bir toplumda şu menfaatlere yönelik olmaları halinde mümkündür: devlet güvenliğinin korunması, kamu güvenliği, devletin mali çıkarları veya suçların önlenmesi veya veri öznelerinin veya başkalarının hak ve özgürlüklerinin korunması.

Örnek: **'Malone v. Birleşik Krallık'**[299] davasında, başvuran, çalıntı malların dürüstlüğe aykırı biçimde kullanılmasıyla alakalı birden çok suçla itham edilmiştir. Dava sürecinde başvurana ait

[293] Bakınız *a.e.,* Madde5; Bakınız Madde 29 Çalışma Kurultayı (2012), *04/2012 Sayılı, Çerez onayından muafiyet konulu Öneri*, WP 194, Brüksel, 7 Haziran 2012.

[294] Bakınız Madde 29 Çalışma Kurultayı (2011), *01/2011 Sayılı, Mevcut AB kişisel veri ihlali çerçevesinde ve gelecekteki politika gelişmeleri için öneriler üzerine Çalışma Belgesi,* WP 184, Brüksel, 5 Nisan 2011.

[295] Direktif 2006/24/AB Sayılı, 15 Mart 2006 tarihli, Avrupa Birliği Parlamentosu ve Konseyi, Kamuya açık elektronik iletişim servislerinin veya kamu iletişim ağlarının sağlanmasıyla bağlantılı olarak üretilen veya işlenen verilerin tutulması konulu Direktifin ve 2002/58/AB Sayılı Direktifin değiştirilmesi üzerine dair Direktif, OJ 2006 L 105.

[296] Avrupa Veri Güvenliği Gözetmeni (EDPS) (2011), *31 Mayıs 2011 tarihli, Komisyon'dan Konseye ve Avrupa Parlamentosuna gönderilen 2006/24/AB Sayılı Veri Saklama Direktifi hakkındaki değerlendirme raporuna ilişkin Görüşü*, 31 Mayıs 2011.

[297] Almanya, Federal Anayasa Mahkemesi (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 Mart 2010; Romanya, Federal Anayasa Mahkemesi (*Curtea Constituþională a României*), No. 1258, 8 Ekim 2009; Çek Cumhuriyeti, Anayasa Mahkemesi (*Ústavní soud České republiky*), 94/2011 Coll., 22 Mart 2011.

[298] ABAD, Birlikte Görülen C-293/12 ve C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 Nisan 2014, par. 65.

[299] AİHM, *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984.

bir telefon görüşmesinin İç İşleri Bakanı tarafından verilmiş iznin verdiği yetkiye dayanılarak dinlendiği ortaya çıkmıştır. Başvuranın haberleşmesinin dinlenmesi ulusal hukuk bakımından yasal olsa da, AİHM kamu makamları tarafından bu alanda sahip olunan takdir yetkisinin kullanımına dair kapsam ve usullere ilişkin yasal kurallar bulunmadığına ve söz konusu uygulama neticesinde meydana gelen müdahalenin bu sebeplerle 'hukuka uygun olmadığı'na karar vermiştir. Mahkeme AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

8.2. İstihdam verileri

Ana başlıklar

- İstihdam ilişkilerinde verilerin korunmasına ilişkin özel hükümler AK İstihdam Verileri Tavsiye Kararı'nda yer almaktadır.
- VK Direktifi'nde istihdam ilişkileri sadece hassas olan kişisel verilerin işlenmesi bağlamında ele alınmıştır.
- İşçi ve işveren arasındaki ekonomik dengesizlik dikkate alınırsa, verilerin işlenmesinin yasal dayanağını teşkil edecek olan ve özgür olarak verilmesi gereken rızanın geçerliliği şüpheli olabilir. Rıza gösterilmesine dair koşullar dikkatli bir biçimde değerlendirilmelidir.

AB'de istihdam bağlamındaki veri işlemelerini düzenleyen özel bir yasal çerçeve bulunmamaktadır. VK Direktifi'nde istihdam ilişkileri direktifin yalnızca 8(2) maddesinde anılır ve söz konusu madde hassas verilerin işlenmesine yöneliktir. AK mevzuatında ise, İstihdam Verileri Tavsiye Kararı 1989'da yayınlanmıştır ve şu an güncellenmektedir.[300]

İstihdam bağlamında özel olarak görülen en yaygın veri koruma sorunlarına dair bir anketi Madde 29 Çalışma Kurultayın'ınbir çalışma belgesinde görmek mümkündür.[301] Çalışma Kurultayıistihdam verilerinin işlenmesine yönelik yasal bir dayanak olarak rızanın önemini analiz etmiştir.[302] Çalışma grubu, rızayı talep eden işveren ve rıza gösteren işçi arasındaki ekonomik dengesizliğin rızanın özgür olarak verilip verilmediğine dair soru işaretleri doğuracağını belirtmiştir. Bu sebeple rızanın istihdam ilişkileri bağlamında geçerliliği değerlendirilirken rızanın talep edildiği şartların da göz önünde bulundurulması gerekmektedir.

Günümüz iş hayatında sıklıkla karşılaşılan veri koruma sorunlarından birisi işçilerin işyerinde gerçekleştirdikleri elektronik haberleşmelerinin denetlenmesine dair meşruiyet sınırlarıdır. Bu sorunun işyerindeki haberleşme olanaklarının özel amaçla kullanımının yasaklanması yoluyla çözülebileceği önerilmektedir. Ancak böyle bir genel yasaklama orantısız ve gerçek dışı olabilir. Aşağıdaki karar özel olarak bu konuya değinmektedir:

Örnek: **'Copland v. Birleşik Krallık'[303]** davasında, bir üniversite çalışanının telefon, e-posta ve internet kullanımı, üniversite olanaklarının kişisel amaçlarla aşırı bir biçimde kullanılıp

[300] Avrupa Konseyi, Bakanlar Komitesi (1989), Rec(89)2 Sayılı, Üye Devletlere İstihdam amacıyla kullanılan kişisel verilerin korunmasıyla ilgili verdiği Öneri, 18 Ocak 1989. Ayrıca, 108 Sayılı Sözleşmeye Danışma Komitesi'nin verdiği, istihdam amacıyla kullanılan kişisel verilerin korunması hakkında ve yukarıda belirtilen Önerinin revize edilmesi için verdiği, R (89) 2 Sayılı Tavsiyelerine bakınız, 9 Eylül 2011.

[301] Madde 29 Çalışma Kurultayı (2001), *8/2001 Sayılı, İstihdam alanında kişisel verilerin işlenmesine ilişkin Öneri,* WP 48, Brüksel, 13 Eylül 2001.

[302] Madde 29 Çalışma Kurultayı (2005), *95/46/AB Sayılı Direktifin 26(1). maddesi'nin ortak anlayışına ilişkin Çalışma Metni, 24 Ekim 1995*, WP 114, Brüksel, 25 Kasım 2005.

[303] AİHM, *Copland v. the United Kingdom*, No. 62617/00, 3 Nisan 2007.

kullanılmadığını belirlemek amacıyla gizlice izlenmiştir. AİHM işyerinde yapılan telefon görüşmelerimin özel hayat ve haberleşme kavramları kapsamında kaldıklarının altını çizmiştir. Bu sebeple, işyerinde gerçekleştirilen bu aramalar, e-posta gönderimleri ve kişisel internet kullanımının takibinden elde edilen bilgiler AİHS'nin 8. maddesi kapsamında korunmaktadır. Başvuranın durumunda, işverenlerin hangi şartlar altında işçilerin telefon, e-posta ve internet kullanımlarını denetleyebileceğine dair bir düzenleme bulunmamaktaydı. Bu yüzden de gerçekleştirilen müdahale hukuka uygun değildi. Mahkeme AİHS madde 8'in ihlal edildiği kanaatine varmıştır.

AK İstihdam Tavsiye Kararı uyarınca, istihdam amaçlarıyla toplanan verilerin doğrudan çalışan bireyden alınması gerekmektedir.

İşe alım için toplanan kişisel veriler adayların uygunluğunu ve kariyer potansiyelini değerlendirmek için gerekli bilgiler ile sınırlı olmalıdır.

Tavsiye kararı ayrıca çalışan kişilerin performans veya potansiyelini değerlendiren kanıya dayalı verilerden bahsetmektedir. Kanıya dayalı veriler adil ve dürüst değerlendirmelere dayanmalı ve meydana getiriliş biçimleri itibariyle aşağılayıcı nitelikte olmamalıdır. Verilerin adil işlenmesi ve doğruluğu ilkeleri gereğince de bu böyledir.

İşveren-işçi ilişkisi bakımından veri koruma hukukunun özel bir yönü de işçi temsilcilerinin rolüyle alakalıdır. Bu temsilciler, işçilerin menfaatlerini temsil amacıyla gerekli olduğu ölçüde işçilerin kişisel verilerini alabilirler.

İstihdam amaçlarıyla toplanan hassas kişisel veriler sadece özel durumlarda ve ulusal hukuk tarafından belirlenmiş korumalara uygun olarak işlenebilir. İşveren sadece bu durumlarda işçilerden veya iş başvurusunda bulunanlardan sağlık durumlarına dair bilgiler talep edebilir veya tıbbı bir incelemeye tabi tutabilir: işe uygunluğunu belirlemek için; önleyici sağlık hizmetleri şartlarını yerine getirmek için veya sosyal yardımlardan faydalanılmasını sağlamak adına. Sağlığa dair veriler, bilgilendirilmeye dayalı ve açık rızanın bulunduğu durumlar veya ulusal hukuk tarafından öngörülen haller saklı kalmak kaydıyla, söz konusu işçi dışındaki bir kaynaktan toplanamazlar.

İstihdam Tavsiye Kararı uyarınca, işçilerin kişisel verilerin işlenme amacına, saklanan kişisel verilerin türüne, verilerin düzenli olarak iletildiği birimlere ve bu iletimin amacı ve yasal dayanağına ilişkin olarak bilgilendirilmeleri gerekmektedir. İşverenler ayrıca, işçilerin kişisel verilerinin işlenmesi veya işçilerin hareketlerinin veya verimliliklerinin denetlenmesi amacıyla kurulacak veya uygulanacak olan otomatik sistemlere ilişkin olarak işçileri önceden bilgilendirmelidir.

İşçiler istihdam verilerine ilişkin olarak erişim, düzeltme ve silme haklarına sahip olmalıdır. Kanıya dayalı verilerin işlenmesi durumunda, işçilerin bu kanıya itiraz hakkı da bulunmalıdır. Bu haklar, iç soruşturmalar kapsamında geçici olarak sınırlanabilir. İşçinin istihdam verilerine yönelik erişim, düzeltme veya silme talebinin reddedildiği durumlarda ulusal hukuk tarafından bu ret kararına itiraz edilebilmesi için uygun prosedürler sağlanmalıdır.

8.3. Tıbbi veriler

Ana başlıklar

- Tıbbi veriler hassas verilerdir, bu sebeple de özel bir korumadan yararlanırlar.

Veri öznesinin sağlık durumuna ilişkin kişisel veriler VK Direktifi madde 8(1) ve 108 Sayılı Sözleşme madde 6 uyarınca hassas veriler olarak nitelendirilmektedir. Buna bağlı olarak, tıbbi veriler hassas olmayan verilerden farklı olarak daha katı bir veri işleme rejimine tabidirler.

Örnek: **'Z. V. Finlanda'**[304] davasında, başvuranın HIV hastası eski kocası birtakım cinsel suçlar işlemiştir. Sonrasında ise, mağdurlarına bilerek HIV bulaştırdığı gerekçesiyle, taksirle ölüme sebebiyet vermekten mahkûm olmuştur. Ulusal mahkeme, gerekçeli kararın ve dava dosyasının, başvuranın daha uzun bir gizlilik süresi belirlenmesi taleplerine karşın, on yıl süreyle gizli kalması gerektiğine karar vermiştir. Bu talepler akabinde temyiz merci tarafında da reddedilmiş ve temyiz sonucu verilen kararda başvuranın ve eski kocasının isimlerine açıkça yer verilmiştir. AİHM, tıbbi verilerin ve özellikle de HIV enfeksiyonlarına dair bilgilerin korunmasının, birçok toplumda bu hastalıkla ilişkilendirilen olumsuz anlamlar da dikkate alınırsa, özel ve aile hayatına saygı gösterilmesi hakkından yararlanılabilmesi bakımından temel bir öneme sahip olduğunu, bu sebeple de müdahalenin demokratik bir toplumda gerekli olarak değerlendirilmediğini ifade etmiştir. Bu nedenle, AİHM, temyiz makamının kararında belirtildiği şekliyle başvuranın kimliğine ve tıbbi durumuna dair bilgilerin karardan yalnızca on sene sonra erişime açılmasının AİHS'nin 8. maddesini ihlal ettiği kanaatine varmıştır.

VK Direktifi Madde 8(3), önleyici tedavi, tıbbi teşhis, bakım veya tedavinin düzenlenmesi veya sağlık hizmetlerinin yönetimi için gerekli olması durumunda tıbbi verilerin işlenmesine imkan tanımaktadır. Ancak verilerin işlenmesine izin verilebilmesi için bunun meslek sırrı yükümlülüğü altında bulunan bir sağlık çalışanı veya eş değerde bir yükümlülüğe tabi bir kişi tarafından yapılması gerekmektedir.[305]

AK Tıbbi Veriler Tavsiye Kararı 108 Sayılı Sözleşme'nin verilerin işlenmesine ilişkin olarak getirdiği ilkeleri tıbbi alandaki verilerin işlenmesine yönelik olarak daha detaylı bir şekilde benimsemektedir.[306] Tıbbi verilerin meşru amaçlarla işlenmesine, sağlık verilerini kullanan kişilerde bulunması gereken meslek sırrı yükümlülüklerine ve veri öznelerinin şeffaflık, erişim, düzeltme ve silme haklarına ilişkin olarak önerilen kurallar VK Direktifi'nde yer alan kurallarla uyumludur. Bunun da ötesinde, sağlık çalışanları tarafından hukuka uygun olarak işlenen tıbbi veriler, "AİHS'nin 8. maddesi kapsamında güvence altına alınmış olan […] özel hayata saygı hakkına uygun olmayacak ifşaların önlenmesi için yeterli tedbirler alınmış olmadıkça" kolluk makamlarına aktarılamaz.[307]

[304] AİHM, *Z. v. Finland*, No. 22009/93, 25 Şubat 1997, par. 94 ve 112; Bakınız AİHM, *M.S. v. Sweden*, No. 20837/92, 27 Ağustos 1997; AİHM, *L.L. v. France*, No. 7508/02, 10 Ekim 2006; AİHM, *I. v. Finland*, No. 20511/03, 17 Temmuz 2008; AİHM, *K.H. and others v. Slovakia*, No. 32881/04, 28 Nisan 2009; AİHM, *Szuluk v. the United Kingdom*, No. 36936/05, 2 Haziran 2009.

[305] Bakınız AİHM, *Biriuk v. Lithuania*, No. 23373/03, 25 Kasım 2008.

[306] Avrupa Konseyi, Bakanlar Komitesi (1997), Rec(97)5 Sayılı, Üye Devletlerin sağlık verileri'ni korumasına ilişkin Öneri, 13 Şubat 1997.

[307] AİHM, No. 1585/09, *Avilkina and Others v. Russia*, No. 1585/09, 6 Haziran 2013, par. 53.

Ayrıca, Tıbbi Veriler Tavsiye Kararı doğmamış çocukların ve ehliyetsiz kişilerin tıbbi verilerine ve genetik verilerin işlenmesine yönelik olarak özel hükümler içermektedir. Bilimsel araştırma, verilerin ihtiyaç olunan süreden daha uzun bir süre saklanabilmesi için geçerli bir sebep olarak kabul edilse de bu durumda genellikle verilerin anonim hale getirilmesi gerekecektir. Tıbbi Veriler Tavsiye Kararı'nın 12. maddesi araştırmacıların kişisel verilere ihtiyaç duyduğu ancak anonim hale getirilmiş verilerin yeterli olmadığı durumlara yönelik olarak detaylı düzenlemeler önermektedir.

Takma isim ile değiştirme yöntemi bilimsel ihtiyaçları karşılamak için uygun bir yol olabilir ve aynı zamanda söz konusu hastaların menfaatlerini de korur. Verilerin korunması bağlamında takma isimle değiştirme kavramı Bölüm 2.1.3'te daha ayrıntılı olarak açıklanmıştır.

Bir hastaya ilişkin tıbbi tedavi verilerinin elektronik bir sağlık dosyasında saklanmasına yönelik girişimlerle alakalı olarak ulusal düzeyde ve Avrupa düzeyinde yoğun tartışmalar yapılmaktadır.[308] Ülke çapında elektronik sağlık dosyaları sistemlerine sahip olmanın özel bir yönü de bu verilerin sınır ötesinde de erişilebilir olmalarıdır: Sınır ötesi sağlık hizmetleri bağlamında AB içerisinde özel ilgiye mazhar olmuş bir konu başlığıdır bu.[309]

Yeni düzenlemelerin tartışma konusu olduğu bir başka alan ise klinik araştırmalar, yani yeni ilaçların kayıt altına alınan bir araştırma ortamı içerisinde hastalar üzerinde denenmesidir; tekrar altını çizmek gerekirse, bu alanın veri koruma bakımından önemli sonuçları bulunmaktadır. İnsan kullanımına yönelik ilaçlar üzerinde yapılacak klinik araştırmalar, Avrupa Birliği'nin ilaçlarla ilgili mevzuatının İyi Klinik Uygulamaları hakkındaki 2001/20/EC sayılı ve 4 Nisan 2001 tarihli Avrupa Parlamentosu ve Avrupa Konseyi Direktifi (Klinik Araştırmalar Direktifi) tarafından düzenlenmiştir.[310] Avrupa Komisyonu, 2012 yılı Aralık ayında, araştırma prosedürlerini tek tip hale getirmek ve daha etkili kılabilmek amacıyla Klinik Araştırmalar Direktifi'nin yerini alacak bir tüzük teklifinde bulunmuştur.[311]

Sağlık sektöründeki kişisel verilere yönelik olarak AB düzeyinde birçok başka düzenleme ve girişim bulunmaktadır.[312]

8.4. İstatistiksel amaçlar için verilerin işlenmesi

Ana başlıklar

- İstatiksel amaçlar için toplanan veriler başka amaçlarla kullanılamaz.
- Herhangi bir meşru amaç için toplanan kişisel veriler, ulusal hukukta yeterli güvencelerin bulunması ve bunların veriyi kullanacaklar tarafından yerine getirilmesi şartıyla, daha sonra istatiksel amaçlar için de kullanılabilir. Bu amaçla, verilerin

[308] Madde 29 Çalışma Kurultayı (2007), *Sağlıkla ilgili kişisel verilerin elektronik sağlık kayıtlarında işlenmesine ilişkin Çalışma Belgesi*, WP 131, Brüksel, 15 Şubat 2007.

[309] Avrupa Birliği Parlamentosu ve Konseyi, 2011/24/EU Sayılı, Sınır ötesi sağlık alanında hasta haklarının uygulanmasına ilişkin Direktif, 9 Mart 2011, OJ 2011 L 88.

[310] Avrupa Birliği Parlamentosu ve Konseyi, 2001/20/AB Sayılı, 4 Nisan 2001 tarihli, İnsan kullanımı için hazırlanan tıbbi ürünler üzerinde klinik araştırmaların yürütülmesine ve iyi klinik uygulamaların uygulanmasına dair Üye Devletlerin kanunları, yönetmelikleri ve idari hükümlerinin yakınlaştırılmasına ilişkin Direktif, OJ 2001 L 121.

[311] Avrupa Komisyonu (2012), İnsan kullanımı için hazırlanan tıbbi ürünler üzerinde klinik araştırmaların yürütülmesine ilişkin Avrupa Birliği Parlamentosu ve Konseyi tarafından alınacak, ve 2001/20/AB Sayılı Direktifi yürürlülükten kaldıracak Tüzük Önerisi, COM(2012) 369 final, Brüksel, 17 Temmuz 2012.

[312] Avrupa Veri Güvenliği Gözetmeni (EDPS) (2013), Komisyon tarafından 'e-Sağlık Eylem Planı 2012-2020 - 21. Yüzyıl için Yenilikçi Sağlık' üzerine yaptığı Bildirime ilişkin Öneri, Brüksel, 27 Mart 2013.

üçüncü kişilere aktarılmadan önce anonim hale getirilmesi veya takma ad ile değiştirilmesi yasalar kapsamında öngörülmelidir.

VK Direktifi'nde, kişisel verilerin istatiksel amaçlar için işlenmesi, veri koruma ilkelerine dair olası istisnalar bağlamında ele alınmaktadır. VK Direktifi madde 6(1)(b) uyarınca, ulusal hukuk kapsamında amaçla sınırlılık ilkesinden verilerin istatistiksel amaçlarla kullanımı yararına vazgeçilebilir. Bunun mümkün olabilmesi için gerekli bütün güvencelerin ulusal hukuk tarafından sağlanmış olması gerekmektedir. Direktifin 13(2) maddesi ise verilerin münhasıran istatistiksel amaçlar için işlenecek olması durumunda erişim hakkının ulusal hukuk tarafından, yine uygun tedbirlerin alınmış olması koşuluyla, sınırlanabileceğini öngörmektedir. Bu bağlamda, VK Direktifi, elde edilen veya istatistiksel araştırma sürecinde yaratılmış olan verilerin hiçbirisinin veri özneleri hakkında somut kararlar almak için kullanılamayacağı şeklinde özel bir şart belirlemiştir.

Veri sorumlusu tarafından hukuka uygun bir şekilde herhangi bir amaçla toplanan kişisel veriler daha sonra aynı veri sorumlusu tarafından kendi istatiksel amaçları -ikincil istatistikler olarak bilinirler- için kullanılabilecek olsalar da istatistiksel amaçlarla üçüncü kişilere aktarılmadan önce, veri öznesi rıza göstermiş olmadıkça veya ulusal mevzuatta buna yönelik özel bir düzenleme bulunmadıkça, duruma bağlı olarak anonim hale getirilmeleri veya takma isim ile değiştirilmeleri gerekir. Bu gereklilik VK Direktifi madde 6(1)(b)'deki uygun tedbirlerin alınması şartından kaynaklanmaktadır.

Verilerin istatistiksel amaçlarla kullanımına dair en önemli örnekler ulusal ve AB istatistik büroları tarafından ulusal ve AB resmi istatistik mevzuatına dayalı olarak meydana getirilen resmi istatistiklerdir. Bu kanunlara göre, vatandaşlar ve işletmeler genellikle istatistik makamlarına verileri ifşa etmek zorundadırlar. İstatistik bürolarında çalışan memurlar, verilerin istatistik makamlarının erişimine sunulabilmesi bakımından gerekli olan güven unsurunun vatandaşlar nezdinde yüksek bir seviyede oluşmasında hayati önem taşımaları sebebiyle dikkatli bir şekilde uyulan özel meslek sırrı yükümlülükleriyle bağlıdır.

223/2009 sayılı Tüzük[313] (Avrupa İstatistikleri Tüzüğü) resmi istatistikler bakımından verilerin korunmasına dair temel kuralları içermektedir; bu bağlamda ulusal düzeydeki resmi istatistiklere dair düzenlemeler bakımından da bağlantılı görülebilir. Tüzük resmi istatistiksel operasyonların yeterli derecede açık bir yasal temele dayandırılması gerektiği ilkesini benimsemiştir. [314]

Örnek: **'Huber v. Almanya'**[315] davasında, ABAD kişisel verilerin yetkili bir makam tarafından istatistiksel amaçlar kapsamında toplanmasının ve saklanmasının, verilerin işlenmesini tek başına meşru kılan bir gerekçe olmadığı kanaatine varmıştır. Verilerin işlenmesine olanak veren kanunların gereklilik şartına da ayrıca değinmesi gerekirdi; ilgili kanunlar bağlamında böyle bir durumdan bahsetmek mümkün değildir.

[313] Avrupa Birliği Parlamentosu ve Konseyi, 223/2009 Sayılı, Avrupa istatistiklerine ilişkin, ve Avrupa Topluluklarının İstatistik Bürosu'na istatistiksel gizlilik getiren verilerin iletimi hakkındaki Avrupa Parlamentosu ve Konseyinin 1101/2008 Sayılı Tüzüğü (AB, Euratom) yürürlükten kaldıran, Topluluk İstatistikleri Üzerine 322/97 Sayılı ve Euratom tarafından Avrupa Toplulukları İstatistik Programları Komitesi kurulması, 89/382/ABT Sayılı Konsey Kararına ilişkin Tüzüğü, Mart 2009, OJ 2009 L 87.

[314] Bu ilke, Eurostat'ın Uygulama Usulü'nde daha detaylı olarak açıklanacak olup, Avrupa İstatistik Tüzüğü'nün 11. maddesine uygun olarak kişisel verilerin resmi istatistikler açısından nasıl kullanılacağı konusunda etik bir rehber oluşturacaktır: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

[315] ABAD, C-524/06, *Huber v. Germany*, 16 Aralık 2008; Özellikle bakınız par. 68.

AK mevzuatı bağlamında, 1997 yılında yayınlanmış olan İstatistiksel Veriler Tavsiye Kararı istatistiklerin kamu ve özel sektörde icrasını kapsamaktadır.[316] Bu tavsiye kararı yukarıda anlatılan VK Direktifi'nin temel kuralları ile örtüşen ilkeler içermektedir. Tavsiye kararı aşağıdaki konular hakkında daha detaylı bilgiler içermektedir.

Bir veri sorumlusu tarafından istatistiksel amaçlarla toplanan veriler başka bir amaçla kullanılamayacak olsa da istatistiksel olmayan amaçlarla toplanmış olan veriler sonrasında istatistiksel amaçlar için kullanılabilirler. İstatistiksel Veriler Tavsiye Kararı verilerin istatistiksel amaçlar kapsamında üçüncü kişilere aktarımına da izin vermektedir. Bu durumlarda, taraflar istatistiksel amaçlar için sonradan gerçekleştirilecek meşru kullanımın kapsamını yazılı olarak kararlaştırmalıdır. Bu yazılı anlaşma veri öznesinin rızasının yerini tutamayacağından, kişisel verilerin kötüye kullanılması riskini en aza indirgeyecek, verilerin üçüncü kişilere aktarılmadan önce anonim hale getirilmesi veya takma isim ile değiştirilmesi gibi uygun tedbirlerin ulusal hukuk tarafından öngörülmesi gerektiği kabul edilebilir.

İstatistiksel araştırma ile profesyonel olarak uğraşan kişiler ulusal hukuk kapsamında özel meslek sırrı yükümlülükleri ile bağlı olmalıdırlar. Bu yükümlülük, veri öznelerinden veya diğer kişilerden veri toplamakla görevlendirilmiş olmaları durumunda ilgili görüşmeleri yapan kişileri de kapsamalıdır.

Kişisel verileri kullanan istatistiksel bir anket kanuna dayanılarak yapılmıyorsa, kişisel verilerin kullanımının meşru olabilmesi için veri öznelerinin buna rıza göstermiş olması veya veri öznelerine en azından itiraz etme imkanının tanınmış olması gerekir. Eğer kişisel veriler mülakatları gerçekleştiren kişiler tarafından istatistiksel amaçlarla toplanıyorsa, bu kişiler ulusal hukuk gereği verilerin ifşasının zorunlu olup olmadığıyla alakalı olarak net bir şekilde bilgilendirilmiş olmalıdır. Ulusal hukuk açıkça müsaade etmediği sürece, hassas veriler hiçbir zaman kişilerin kimliğini deşifre edecek şekilde toplanmamalıdır.

İstatistiksel bir anketin anonim hal getirilmemiş veri olmaksızın yapılamayacağı ve kişisel verilerin mutlaka gerekli olduğu hallerde, bu amaçla toplanan veriler olabildiğince anonim hale getirilmiş olmalıdır. İstatistiksel anketin sonuçları, aksi ihtimalin gerçekleşmesinin hiçbir risk taşımadığı durumlar hariç, veri öznelerinin kimliklerinin ortaya çıkmasına bir nebze bile olsa izin vermemelidir.

İstatistiksel analizler tamamlandıktan sonra, kişisel veriler ya silinmeli ya da anonim hale getirilmelidir. Bu durumda, İstatistiksel Veriler Tavsiye Kararı kimlik belirleyici verilerin diğer kişisel verilerden ayrı tutulmasını önermektedir. Bu da, verilerin takma isim ile değiştirilmesi ve kimliği tespite yarayacak isim eşleşmelerini içeren şifreleme anahtarı veya listenin takma isim ile değiştirilmiş verilerden ayrı bir yerde saklanması gerektiği anlamına gelir.

8.5. Mali veriler

Ana başlıklar

[316] Avrupa Konseyi, Bakanlar Komitesi (1997), Rec(97)18 Sayılı, Üye Devletlere yönelik, istatistiki amaçlar için toplanan ve işlenen kişisel verilerin korunmasına ilişkin Öneri, 30 Eylül 1997.

- Mali veriler 108 Sayılı Sözleşme veya VK Direktifi bağlamında hassas veriler olmasalar da işlenebilmeleri için veri doğruluğunu ve güvenliğini sağlayacak belirli tedbirlerin alınmış olması gerekmektedir.
- Elektronik ödeme sistemleri, tasarım yoluyla gizlilik olarak adlandırılan yerleşik bir veri korumasına sahip olmalıdır.
- Kimlik doğrulama ihtiyacına yönelik uygun mekanizmaların bulunması gerekliliğinden bu alana özel veri koruma sorunları çıkmaktadır.

Örnek: **'Michaud v. Fransa'**[317] davasında, Fransız bir avukat olan başvuran, müvekkiller tarafından gerçekleştirilen kara para aklamalarıyla alakalı şüpheleri ihbar etmeye yönelik Fransız hukukundan kaynaklanan yükümlülüğe itiraz etmiştir. AİHM, avukatları, başka bir kişiyle alakalı olarak ve doğrudan o kişiyle konuşarak edindikleri bilgileri idari makamlara bildirmekle yükümlü kılmanın, avukatların AİHS 8. madde kapsamında yazışmalarına ve özel hayatlarına saygı gösterilmesi olarak bilinen ve mesleki veya işletmesel faaliyetleri de kapsayan haklarına bir müdahale teşkil ettiğine karar vermiştir. Ancak müdahale kanuna uygun olarak ve düzensizliğin ve suçun önlenmesi şeklindeki meşru bir amaç uğruna yapılmıştır. Avukatlar ancak çok sınırlı koşullarda bu yükümlülüğe tabi olacağından, AİHM yükümlülüğün orantılı olduğuna ve 8. maddenin ihlal edilmediğine karar vermiştir.

Veri korumaya ilişkin genel yasal çerçevenin ödemeler bağlamında bir uygulaması, 108 Sayılı Sözleşme'de yer aldığı üzere, AK'nin 1990 tarihli ve Rec(90)19 sayılı Tavsiye Kararı ile geliştirilmiştir. Bu tavsiye kararı ödemeler ve özellikle de kartla yapılan ödemeler bağlamında verilerin hukuka uygun olarak toplanması ve kullanılmasının kapsamını netliğe kavuşturmaktadır. Ulusal yasa koyuculara, ödeme verilerinin üçüncü kişilere aktarımının sınırlarına, verilerin saklanacağı süre sınırlarına, şeffaflığa, veri güvenliği ve sınır ötesi veri akışlarına ve son olarak da denetime ve kanun yollarına ilişkin detaylı düzenlemeler önermektedir. Burada önerilen çözümler sonradan AB'nin VK Direktifi'ndeki genel veri koruma çerçevesini oluşturmuştur.

Mali araçları ve kredi kurumları ve yatırım firmalarının faaliyetlerini düzenlemek için birçok yasal düzenleme yapılmıştır.[318] Bunun dışındaki hukuki düzenlemeler ise kamuya açıklanmamış bilgiye dayalı ticaret ve pazar/fiyat manipülasyonlarıyla mücadeleye destek olmaya yöneliktir.[319] Bu alanlardaki sorunlar arasında verilerin korunması üzerinde etkiye sahip olan en ciddi sorunlar şunlardır:

- mali işlemlere dair kayıtların saklanması;
- kişisel verilerin üçüncü ülkelere aktarılması;

[317] AİHM, *Michaud v. France*, No. 12323/11, 6 Aralık 2012; Bakınız AİHM, *Niemietz v. Germany*, No. 13710/88, 16 Aralık 1992, par. 29, ve AİHM, *Halford v. the United Kingdom*, No. 20605/92, 25 Haziran 1997, par. 42.

[318] Avrupa Komisyonu (2011), *Avrupa Parlamentosu ve Konseyin 2004/39/AB Sayılı Direktifini yürürlükten kaldıran finansal araçlara ilişkin Avrupa Parlamentosu ve Konsey Yönergesi için teklif*, COM(2011) 656 final, Brüksel, 20 Ekim 2011; Avrupa Komisyonu (2011), Avrupa Parlamentosu ve Konseyinin finansal araçlarla ilgili pazarlara ilişkin ve OTC türevlerine, merkezi taraflar ve ticaret depolarını düzenleyen *[EMIR] Tüzüğü'nün değiştirilmesine dair Tüzük teklifi*, COM(2011) 652 final, Brüksel, 20 Ekim 2011; Avrupa Komisyonu (2011), Kredi kuruluşlarının faaliyetlerine erişim ve kredi kuruluşlarının ve yatırım firmalarının ihtiyatlı denetimi hakkındaki Avrupa Parlamentosu ve Konsey Direktifi ve Avrupa Parlamentosu ve Konseyi'nin, 2002/87/AB Sayılı, Kredi kuruluşlarının, sigorta şirketlerinin ve yatırım firmalarının finansal bir holding içindeki ek denetimine ilişkin Direktifi'nin değiştirilmesi için teklif, COM(2011) 453 final, Brüksel, 20 Temmuz 2011.

[319] Avrupa Komisyonu (2011), *AB iç pazar ve pazar manipülasyonu (pazar kötüye kullanımı) hakkında Avrupa Parlamentosu ve Konsey Tüzüğüi için teklif*, COM(2011) 651 final, Brüksel, 20 Ekim 2011; Avrupa Komisyonu (2011), *AB iç pazar ve pazar manipülasyonu için cezai yaptırımlar konusunda Avrupa Parlamentosu ve Konsey Direktifi için teklif*, COM(2011) 654 final, Brüksel, 20 Ekim 2011.

- yetkili makamların telefon ve veri trafiği kayıtlarını talep yetkisi de dahil olmak üzere telefon görüşmelerinin veya elektronik haberleşmenin kayda alınması;
- cezaların yayınlanması da dahil olmak üzere kişisel bilgilerin ifşası;
- yerinde denetim ve belgelere el koymak adına özel konuta girme de dahil olmak üzere yetkili mercilerin denetim ve soruşturma yetkileri;
- ihlalleri raporlamak için geliştirilmiş mekanizmalar, örneğin ispiyonlama sistemleri;
- Üye Devletler'in yetkili makamları ve Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (ESMA) arasındaki işbirliği.

Bu alanlar kapsamında özel olarak ele alınmış, veri öznelerinin mali durumuna dair verilerin toplanması[320] veya banka transferleri yoluyla sınır ötesi ödemeler gibi kaçınılmaz olarak kişisel verilerin akışına yol açan başka sorunlar da bulunmaktadır.[321]

İLAVE KAYNAKLAR

BÖLÜM 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Frei- heit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brüksel, available at: www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Con- vention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

[320] Avrupa Birliği Parlamentosu ve Konseyi, 1060/2009 Sayılı, 16 Eylül 2009 tarihli, Kredi derecelendirme kuruluşlarına ilişkin Tüzük, OJ 2009 L 302, Avrupa Komisyonu, Avrupa Komisyonu, kredi derecelendirme kuruluşları hakkında 1060/2009 Sayılı Tüzüğü değiştiren Avrupa Parlamentosu ve Konsey Yönetmeliği için teklif, COM(2010) 289 final, Brüksel, 2 Haziran 2010.

[321] Avrupa Birliği Parlamentosu ve Konseyi, 2007/64/AB Sayılı, 13 Kasım 2007 tarihli, AB iç pazardaki ödeme hizmetlerine ilişkin olan ve 97/7/AB, 2002/65/AB, 2005/60/AB ve 2006/48/AB Sayılı Direktifleri değiştiren, 97/5/AB Sayılı Direktifin yürürlükten kaldıran Direktifi, OJ 2007 L 319.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union euro- péenne et convention européenne des droits de l'homme*, Brüksel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, s. 281–288.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review*, Vol. 4, No. 5, s. 193–220, available at: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

BÖLÜM 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, s. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

BÖLÜM 3-5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/ privacy_impact_assessment.

BÖLÜM 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Rein- venting data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

BÖLÜM 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, availa- ble at: www.europol.europa.eu/sites/default/files/publications/europol_dpo_book- let_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Drewer, D. and Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime*, ERA Forum, Vol. 13, No. 3, s. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, Vol. 36, No. 5, s. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of

External Relations, CLEER Working Papers 2013/2, available at: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

BÖLÜM 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, Vol. 36, No. 5, s. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

İÇTİHATLAR

AİHM

Verilere erişim

Gaskin v. the United Kingdom, No. 10454/83, 7 Temmuz 1989 *Godelli v. Italy*, No. 33783/09, 25 Eylül 2012 *K.H. and Others v. Slovakia*, No. 32881/04, 28 Nisan 2009 *Leander v. Sweden*, No. 9248/81, 26 Mart 1987 *Odièvre v. France* [GC], No. 42326/98, 13 Şubat 2003

Veri korumasını ifade özgürlüğü ile dengelemek

Axel Springer AG v. Germany [GC], No. 39954/08, 7 Şubat 2012 *Von Hannover v. Germany*, No. 59320/00, 24 Haziran 2004 *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 Şubat 2012

Çevrimiçi veri korumasındaki zorluklar

K.U. v. Finland, No. 2872/02, 2 Aralık 2008

Haberleşme

Amann v. Switzerland [GC], No. 27798/95, 16 Şubat 2000 *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 Mart 2013 187
Handbook on European data protection law
Cemalettin Canli v. Turkey, No. 22427/04, 18 Kasım 2008 *Dalea v. France*, No. 964/07, 2 Şubat 2010 *Gaskin v. the United Kingdom*, No. 10454/83, 7 Temmuz 1989 *Haralambie v. Romania*, No. 21737/03, 27 Ekim 2009 *Khelili v. Switzerland*, No. 16188/07, 18 Ekim 2011 *Leander v. Sweden*, No. 9248/81, 26 Mart 1987

Malone v. the United Kingdom, No. 8691/79, 2 Ağustos 1984 *McMichael v. the United Kingdom*, No. 16424/90, 24 Şubat 1995 *M.G. v. the United Kingdom*, No. 39393/98, 24 Eylül 2002 *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 Aralık 2008 *Shimovolos v. Russia*, No. 30194/09, 21 Haziran 2011 *Turek v. Slovakia*, No. 57986/00, 14 Şubat 2006

Adli sicil kaydı veri tabanları
B.B. v. France, No. 5335/06, 17 Aralık 2009 *M.M. v. the United Kingdom*, No. 24029/07, 13 Kasım 2012

DNA veri tabanları
S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 Aralık 2008.

GPS verileri
Uzun v. Germany, No. 35623/05, 2 Eylül 2010

Sağlık verileri
Biriuk v. Lithuania, No. 23373/03, 25 Kasım 2008 *I. v. Finland*, No. 20511/03, 17 Temmuz 2008 *L.L. v. France*, No. 7508/02, 10 Ekim 2006 *M.S. v. Sweden*, No. 20837/92, 27 Ağustos 1997 *Szuluk v. the United Kingdom*, No. 36936/05, 2 Haziran 2009 *Z. v. Finland*, No. 22009/93, 25 Şubat 1997

Kimlik
Ciubotaru v. Moldova, No. 27138/04, 27 Nisan 2010 188
Godelli v. Italy, No. 33783/09, 25 Eylül 2012 *Odièvre v. France* [GC], No. 42326/98, 13 Şubat 2003

Profesyonel faaliyetlere ilişkin bilgiler
Michaud v. France, No. 12323/11, 6 Aralık 2012 *Niemietz v. Germany*, No. 13710/88, 16 Aralık 1992

Haberleşmenin dinlenmesi
Amann v. Switzerland [GC], No. 27798/95, 16 Şubat 2000 *Copland v. the United Kingdom*, No. 62617/00, 3 Nisan 2007 *Cotlet v. Romania*, No. 38565/97, 3 Haziran 2003 *Kruslin v. France*, No. 11801/85, 24 Nisan 1990
Lambert v. France, No. 23618/94, 24 Ağustos 1998 *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 Temmuz 2008 *Malone v. the United Kingdom*, No. 8691/79, 2 Ağustos 1984 *Halford v. the United Kingdom*, No. 20605/92, 25 Haziran 1997 *Szuluk v. the United Kingdom*, No. 36936/05, 2 Haziran 2009

Yükümlülük sahipleri için zorunluluklar
B.B. v. France, No. 5335/06, 17 Aralık 2009 *I. v. Finland*, No. 20511/03, 17 Temmuz 2008 *Mosley v. the United Kingdom*, No. 48009/08, 10 May 2011

Fotoğraflar
Sciacca v. Italy, No. 50774/99, 11 Ocak 2005 *Von Hannover v. Germany*, No. 59320/00, 24 Haziran 2004

Unutulma hakkı
Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 Haziran 2006

İtiraz hakkı
Leander v. Sweden, No. 9248/81, 26 Mart 1987 *Mosley v. the United Kingdom*, No. 48009/08, 10 May 2011 *M.S. v. Sweden*, No. 20837/92, 27 Ağustos 1997 *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000

Hassas veri kategorileri
I. v. Finland, No. 20511/03, 17 Temmuz 2008 *Michaud v. France*, No. 12323/11, 6 Aralık 2012 *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 Aralık 2008

Denetim ve yaptırım (veri koruma makamları da dahil olmak üzere değişik aktörlerin rolleri)
I. v. Finland, No. 20511/03, 17 Temmuz 2008 *K.U. v. Finland*, No. 2872/02, 2 Aralık 2008 *Von Hannover v. Germany*, No. 59320/00, 24 Haziran 2004 *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 Şubat 2012

Gözetleme araçları
Allan v. the United Kingdom, No. 48539/99, 5 Kasım 2002 *Association "21 Décembre 1989" and Others v. Romania*, Nos. 33810/07 and 18817/08, 24 May 2011 *Bykov v. Russia* [GC], No. 4378/02, 10 Mart 2009 *Kennedy v. the United Kingdom*, No. 26839/05, 18 May 2010 *Klass and Others v. Germany*, No. 5029/71, 6 Eylül 1978 *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 Ekim 2002 *Uzun v. Germany*, No. 35623/05, 2 Eylül 2010 *Vetter v. France*, No. 59842/00, 31 May 2005

Kamera ile gözetleme
Köpke v. Germany, No. 420/07, 5 Ekim 2010 *Peck v. the United Kingdom*, No. 44647/98, 28 Ocak 2003

Ses kayıtları
P.G. and J.H. v. the United Kingdom, No. 44787/98, 25 Eylül 2001 *Wisse v. France*, No. 71611/01, 20 Aralık 2005
190

ABAD

VK Direktifi ile alakalı mahkeme kararları
C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 Aralık 2008
[VK Direktifi, Madde 9 kapsamında "gazetecilik faaliyetleri" kavramı]

Birlikte Görülen C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eif- ert v. Land Hessen*, 9 Kasım 2010
[Belirli AB tarım fonlarının yararlanıcıları hakkında kişisel verileri yasal yükümlülükleri gereği yayınlamasına ilişkin orantılığı]

C-101/01, *Bodil Lindqvist*, 6 Kasım 2003 [İnternet üzerinden başkalarının özel hayatına ilişkin

özel bir kişi tarafından veri yayınlanması'nın meşruiyeti]

C-131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Reference for a preliminary ruling from the *Audiencia Nacional* (Spain) lodged on 9 Mart 2012, 25 May 2012, pending
[Arama motoru sağlayıcılarının, ilgili kişinin talebi üzerine, arama sonuçlarında kişisel verileri göstermemesine ilişkin yükümlülükleri]

C-270/11, *European Commission v. Kingdom of Sweden*, 30 May 2013 [Bir direktifin uygulanmadığı için verilen para cezası]

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 Ocak 2008
[İnternet erişim sağlayıcılarının, KaZaA programının kullanıcılarının kimliğini fikri mülkiyet koruma birliğine açıklama zorunluluğu]

C-288/12, *European Commission v. Hungary*, 8 Nisan 2014 [Ulusal veri koruma denetçisi'nin görevden alınmasının meşruiyeti]

C-291/12, *Michael Schwarz v. Stadt Bochum*, Opinion of the Advocate General, 13 Haziran 2013
[AB Birincil Mevzuatın, 225/02/2004 / EC sayılı Tüzük uyarınca, parmak izlerinin pasaportlarda saklanmasına ilişkin, ihlal edilmesi]

Birlikte Görülen C-293/12 and C-594/12, *Digital Rights Ireland and Seitling and Others v. Ireland*, 8 Nisan 2014
[AB Birincil Mevzuatın, Veri Saklama Direktifi tarafından ihlal edilmesi]

C-360/10, *SABAM v. Netlog N.V.*, 16 Şubat 2012 [Şebeke kullanıcıları tarafından müziki ve görsel-işitsel eserlerin yasalara aykırı kullanılmasını önlemek adına sosyal ağ sağlayıcılarının yükümlülükleri]

Birlikte Görülen C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*, 20 May 2003 [Kamu sektörü ile ilgili belirli kategorideki kurumların, çalışanların maaşlarına ilişkin kişisel verileri yayınlama yükümlülüğünün orantılılığına ilişkin]

Birlikte Görülen C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 Kasım 2011 [Veri Koruma Direktifi Madde 7 (f) 'nin doğru uygulanması -"başkalarının meşru çıkarları"- ulusal yasalarda]

C-518/07, *European Commission v. Federal Republic of Germany*, 9 Mart 2010 [Ulusal Gözlemçi Birimin bağımsızlığı]

C-524/06, *Huber v. Bundesrepublik Deutschland*, 16 Aralık 2008 [Yabancılarla ilgili verileri istatistiksel bir sicilde tutmanın meşruiyeti]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011 [Yenilenmiş rızanın önemi]

C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijke- boer*, 7 May 2009
[İlgili Kişinin verilerine erişim hakkı]

C-614/10, *European Commission v. Republic of Austria*, 16 Ekim 2012 [Ulusal denetim makamının bağımsızlığı]

AB Kurumları Veri Koruma Tüzüğü ile alakalı mahkeme kararları:
C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 Haziran 2010 [Belgelere erişim]

C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communi- ties*, 6 Mart 2003
[Belgelere erişim]

F-35/08, *Dimitrios Pachtitis v. European Commission*, 15 Haziran 2010 [AB kurumlarında istihdam bağlamında kişisel bilgilerin kullanılması]

F-46/09, *V v. European Parliament*, 5 Temmuz 2011 [AB kurumlarında istihdam bağlamında kişisel bilgilerin kullanılması]

DİZİN

ABAD İçtihatları

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, Birlikte Görülen C-468/10 ve C-469/10, 24 Kasım 2011.....18, 22, 79, 81, 85, 86, 192

Bodil Lindqvist, C-101/01, 6 Kasım 2003 .....35, 43, 47, 49, 94, 129, 130, 191

College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, C-553/07, 7 Mayıs 2009..... .....103, 108, 192

Deutsche Telekom AG v. Germany, C-543/09, 5 Mayıs 2011.....36, 59, 60, 192

Digital Rights Ireland and Seitlinger and Others, Birlikte Görülen C-293/12 ve C-594/12, 8 Nisan 2014 .....124, 169, 192

Dimitrios Pachtitis v. European Commission, F-35/08, 15 Haziran 2010..... 193

European Commission v. Federal Republic of Germany, C-518/07, 9 Mart 2010.....104, 116, 192

European Commission v. Hungary, C-288/12, 8 Nisan 2014.....104, 117, 191

European Commission v. Kingdom of Sweden, C-270/11, 30 Mayıs 2013..... 191

European Commission v. Republic of Austria, C-614/10, 16 Ekim 2012 .....104, 117, 193

European Commission v. The Bavarian Lager Co. Ltd., C-28/08 P, 29 Haziran 2010..... 13, 27, 29, 104, 125, 193

European Parliament v. Council of the European Union, Birlikte Görülen C-317/04 ve C-318/04, 30 Mayıs 2006..... 139

Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, Reference for a preliminary ruling from the Audiencia Nacional (Spain) lodged on 9 Mart 2012, 25 Mayıs 2012, henüz karara bağlanmamıştır..... 191

Huber v. Germany, C-524/06, 16 Aralık 2008.....61, 79, 81, 83, 165, 177, 192

Interporc Im- und Export GmbH v. Commission of the European Communities, C-41/00, 6 Mart 2003.....29, 193

M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority, C-152/84, 26 Şubat 1986.....104

Michael Schwarz v. Stadt Bochum, C-291/12, Opinion of the Advocate General, 13 Haziran 2013 192

Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, 29 Ocak 2008.....13, 22, 32, 35, 39, 191

Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, Birlikte Görülen C-465/00, C-138/01 ve C-139/01, 20 Mayıs 2003.....81, 192

SABAM v. Netlog N.V., C-360/10, 16 Şubat 2012 .....33, 192

Sabine von Colson and Elisabeth Kamann v. Land NordrheinWestfalen, C-14/83, 10 Nisan 1984 .....104, 127

Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, 16 Aralık 2008.....13, 23, 191

V v. European Parliament, F-46/09, 5 Temmuz 2011..... 193

Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, Birlikte Görülen C-92/09 ve C-93/09, 9 Kasım 2010.....13, 21, 29, 35, 38, 42, 61, 66, 191

Index 197 Case-law of the European Court of Human Rights Allan v. the United Kingdom, No. 48539/99, 5 Kasım 2002.....145, 190

Amann v. Switzerland [GC], No. 27798/95,
16 Şubat 2000.....37, 39, 42, 63, 187, 189

Ashby Donald and Others v. France, No. 36769/08, 10 Ocak 2013.....31

Association "21 Décembre 1989" and Others v. Romania, Nos. 33810/07 and 18817/08,
24 Mayıs 2011.....190

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,
No. 62540/00, 28 Haziran 2007 64

Avilkina and Others v. Russia, No. 1585/09, 6 Haziran 2013 (not final) 174

Axel Springer AG v. Germany [GC], No. 39954/08,
7 Şubat 2012.....13, 24, 187

B.B. v. France, No. 5335/06, 17 Aralık 2009.....143, 145, 188, 189

Bernh Larsen Holding AS and Others v. Norway, No. 24117/08,
14 Mart 2013.....35, 38, 187

Biriuk v. Lithuania, No. 23373/03, 25 Kasım 2008.....25, 104, 174, 188

Bykov v. Russia [GC], No. 4378/02, 10 Mart 2009.....190

Cemalettin Canli v. Turkey, No. 22427/04, 18 Kasım 2008.....103, 109, 188

Ciubotaru v. Moldova, No. 27138/04, 27 Nisan 2010.....103, 111, 188

Copland v. the United Kingdom, No. 62617/00, 3 Nisan 2007.....15, 165, 171, 189

Cotlet v. Romania, No. 38565/97, 3 Haziran 2003.....189

Dalea v. France, No. 964/07, 2 Şubat 2010.....109, 143, 159, 188

Gaskin v. the United Kingdom, No. 10454/83, 7 Temmuz 1989.....106, 187, 188

Godelli v. Italy, No. 33783/09, 25 Eylül 2012.....39, 106, 187, 189

Halford v. the United Kingdom, No. 20605/92, 25 Haziran 1997.....178, 189

Haralambie v. Romania, No. 21737/03, 27 Ekim 2009..... 62, 74, 188

I. v. Finland, No. 20511/03, 17 Temmuz 2008.....15, 80, 92, 126, 173, 188, 189, 190

Iordachi and Others v. Moldova, No. 25198/02, 10 Feburary 2009.....63

K.H. and Others v. Slovakia, No. 32881/04,
28 Nisan 2009.....62, 74, 106, 173, 187

K.U. v. Finland, No. 2872/02,
2 Aralık 2008.....15, 104, 122, 126, 187, 190

Kennedy v. the United Kingdom, No. 26839/05, 18 Mayıs 2010.....190

Khelili v. Switzerland, No. 16188/07, 18 Ekim 2011.....61, 65, 188

Klass and Others v. Germany, No. 5029/71, 6 Eylül 1978.....15, 146, 190

Köpke v. Germany, No. 420/07, 5 Ekim 2010.....43, 123, 190

Kopp v. Switzerland, No. 23224/94, 25 Mart 1998.....63

Kruslin v. France, No. 11801/85, 24 Nisan 1990.....189

L.L. v. France, No. 7508/02, 10 Ekim 2006.....173, 188

Lambert v. France, No. 23618/94, 24 Ağustos 1998.....189

Leander v. Sweden, No. 9248/81, 26 Mart 1987..... 15, 61, 65, 106, 113, 144, 187, 188, 189

Liberty and Others v. The United Kingdom, No. 58243/00, 1 Temmuz 2008.....38, 189

M.G. v. the United Kingdom, No. 39393/98, 24 Eylül 2002.....188

M.K. v. France, No. 19522/09, 18 Nisan 2013.....110, 144

M.M. v. the United Kingdom, No. 24029/07, 13 Kasım 2012.....73, 144, 188

M.S. v. Sweden, No. 20837/92, 27 Ağustos 1997..... 113, 173, 188, 189
Malone v. the United Kingdom, No. 8691/79,

2 Ağustos 1984.....15, 63, 170, 188, 189

McMichael v. the United Kingdom, No. 16424/90, 24 Şubat 1995.....188

Michaud v. France, No. 12323/11, 6 Aralık 2012..... 166, 178, 189, 190

Mosley v. the United Kingdom, No. 48009/08, 10 Mayıs 2011 ..... 13, 25, 113, 189

Müller and Others v. Switzerland, No. 10737/84, 24 Mayıs 1988.....30

Niemietz v. Germany, 13710/88, 16 Aralık 1992..... 37, 178, 189

Odièvre v. France [GC], No. 42326/98, 13 Şubat 2003 .....39, 106, 187, 189

P.G. and J.H. v. the United Kingdom, No. 44787/98, 25 Eylül 2001..... 43, 190

Peck v. the United Kingdom, No. 44647/98, 28 Ocak 2003.....43, 61, 64, 190

Rotaru v. Romania [GC], No. 28341/95, 4 Mayıs 2000.....37, 61, 64, 110, 188, 189, 190

S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04,
4 Aralık 2008..... 15, 73, 143, 145, 188, 190

Sciacca v. Italy, No. 50774/99, 11 Ocak 2005..... 43, 189

Index 199 Segerstedt-Wiberg and Others v. Sweden, No. 62332/00,
6 Haziran 2006.....103, 110, 189

Shimovolos v. Russia, No. 30194/09, 21 Haziran 2011.....64, 188

Silver and Others v. the United Kingdom, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75,
7113/75, 25 Mart 1983 63

Szuluk v. the United Kingdom, No. 36936/05, 2 Haziran 2009 ..... 173, 188, 189

Társaság a Szabadságjogokért v. Hungary, No. 37374/05, 14 Nisan 2009.....13, 28

Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 Ekim
2002..... 61, 64, 190

The Sunday Times v. the United Kingdom, No. 6538/74, 26 Nisan 1979.....63

Turek v. Slovakia, No. 57986/00, 14 Şubat 2006.....188

Uzun v. Germany, No. 35623/05, 2 Eylül 2010.....15, 42, 188, 190

Vereinigung bildender Künstler v. Austria, No. 68345/01,
25 Ocak 2007.....13, 30

Vetter v. France, No. 59842/00, 31 Mayıs 2005 .....64, 143, 147, 190

Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, 7 Şubat 2012
.....22, 24, 187, 190

Von Hannover v. Germany, No. 59320/00, 24 Haziran 2004.....43, 187, 189, 190

Wisse v. France, No. 71611/01, 20 Aralık 2005.....43, 190

Z. v. Finland, No. 22009/93, 25 Şubat 1997.....165, 173, 188

Ulusal mahkemelerin içtihatları

Germany, Federal Constitutional Court (Bundesverfassungsgericht), 1 BvR 256/08,
2 Mart 2010 169

Romania, Federal Constitutional Court (Curtea Constituțională a României), No. 1258,
8 Ekim 2009.....169

The Czech Republic, Constitutional Court (Ústavní soud České republiky), 94/2011 Coll., 22 Mart 2011.....169