

AVRUPA KONSEYİ'NİN KİŞİSEL VERİLER AÇISINDAN SAĞLADIĞI TEMEL GÜVENCELER

Songül ATAĞ*

I. GENEL OLARAK

On Avrupa devleti tarafından 1949 yılında kurulan Avrupa Konseyi'nin temel amacı üye devletlerde demokrasiyi, insan haklarını ve hukuk devletini güçlendirmektir. Konsey bu amaca ulaşabilmek için 1950 yılında Avrupa İnsan Hakları Sözleşmesi'ni kabul etmiştir. Sözleşme'nin oluşturduğu etkili koruma mekanizması yoluyla üye devletlerde insan haklarının korunması konusunda önemli adımlar atılmıştır.

Kişisel verilerin korunması konusunun Avrupa Konseyi'nin gündemine ilk girişi 1960'ların sonlarına doğru olmuştur. Bu alanda yapılan çalışma ve tartışmaların sonucunda Konsey 1981 yılında "*Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme*"yi kabul etmiştir.¹ 1985 yılında yürürlüğe giren Sözleşme güçlü bir koruma mekanizması içermemekle beraber, kişisel verilerin korunması konusunda kabul edilmiş olan bağlayıcı ilk uluslararası belge olması nedeniyle büyük bir önem taşımaktadır.

Avrupa Konseyi'nin kişisel veriler açısından sağladığı koruma 108 sayılı Sözleşme'deki düzenlemelerle sınırlı kalmamıştır. Daha sonraki yıllarda özellikle Avrupa Konseyi Bakanlar Komitesi'nin yayınladığı kararlar ile birçok alanda kişisel veriler açısından etkili bir koruma sağlama yoluna gidilmiştir.

* Yrd. Doç. Dr., Dicle Üniversitesi Hukuk Fakültesi öğretim üyesi.

¹ Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, European Treaty Series-No.108.

108 sayılı Sözleşme ve Bakanlar Komitesi'nin yayınladığı kararların yanı sıra Avrupa İnsan Hakları Sözleşmesi de kişisel verilerin korunması konusunda önemli bir rol oynamıştır. Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunmasına ilişkin doğrudan bir hüküm yer almamasına rağmen, özel yaşam hakkını koruyan 8. madde bu alanı da kapsamaktadır. Nitekim Sözleşme hükümlerinin üye devletlerde uygulanmasını izlemekten sorumlu olan Avrupa İnsan Hakları Mahkemesi, 8. maddenin sağladığı korumanın kişisel verileri de kapsadığı yönünde kararlar vermiştir.

II. KİŞİSEL VERİLERİN OTOMATİK İŞLEME TABİ TUTULMA SÜRECİNDE BİREYLERİN KORUNMASINA İLİŞKİN 108 SAYILI SÖZLEŞME

A. Tarihçe

1960'larda bilgi ve iletişim teknolojileri alanında sağlanan gelişmeler, kişisel verilerin gizliliğinin güvence altına alınması konusunda mevcut hukuki ve teknik önlemlerin yetersizliği konusunda artan bir endişenin oluşmasına neden olmuştur. Dijital devrimin potansiyel etkisi güçlü bir şekilde görülmeye başlanmış ve kişisel verilerin kapsamlı bir şekilde işlenmesine karşı bireyleri korumak için önlemler alınması ihtiyacı net bir şekilde fark edilmeye başlanmıştır.²

Avrupa Konseyi ilk olarak 1960'ların sonlarında özel yaşam hakkı ve kişisel verilerin korunması sorunu ile ilgilenmeye başlamıştır. Bakanlar Komitesi ilk kez 1968 yılında, kişisel verilerin korunması konusunu ele almak ve mevcut insan hakları belgelerinin ve iç hukuklardaki düzenlemelerin verilerin gizliliğini korumaya yeterli olup olmadığını incelemek amacıyla toplanmıştır.³ Bakanlar Komitesi bu tarihten itibaren üye devletlerde özel yaşam hakkı ve kişisel verilerin korunma-

² Graham Pearce/Nicholas Platten, "Achieving Personal Data Protection in the European Union", *Journal of Common Market Studies*, Vol.36, No.4, December 1998, s. 531.

³ Fritz H. Grupa/William Kuechler/Scott Sweeney, "Dealing with Data Privacy Protection: An Issue for the 21st Century", *Law, Investigations, and Ethics*, January/February 2002, s. 46.

sıyla ilgili yasal düzenlemeleri incelemeye başlamıştır.⁴ Özellikle bilgisayar teknolojisindeki modern ilerlemelere karşı özel yaşam hakkının nasıl en iyi şekilde korunabileceği konusunda tavsiyelerde bulunması için bir Uzmanlar Komitesi kurmuştur. Komite üyeleri bu alanda tavsiyelerde bulunarak verilerin korunması çabalarında oldukça önemli bir rol oynamışlardır.⁵

Bu alanda yapılan çalışmalar, kişisel verilerin etkili bir şekilde korunabilmesi için yasal düzenlemeler yapılması gerektiğini ortaya koymuştur. Bu ihtiyaçtan yola çıkan Bakanlar Komitesi 1973 yılında “Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamalarının Korunmasına İlişkin Karar”⁶ ile 1974 yılında “Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamalarının Korunmasına İlişkin Karar”⁷ kabul etmiştir. Bu kararlar elektronik veri bankalarında tutulan kişisel bilgilerin korunması için asgari standartları ortaya koyan kararlardır. Söz konusu iki karar aynı zamanda 1981 tarihinde kabul edilen 108 sayılı Sözleşme’nin hazırlayıcısı olmuştur.

Sözleşme’nin tasarı metni Uzmanlar Komitesi tarafından 1979 yılında hazırlanmıştır. Komitenin hazırladığı metin Bakanlar Komitesi tarafından 1981 yılında kabul edilmiş ve imzaya açılmıştır. Sözleşme’nin yürürlüğe girebilmesi için beş devlet tarafından onaylanması şartı aranmıştır.⁸ Sözleşme’nin Fransa, Norveç, İsveç, İspanya ve Federal Almanya tarafından onaylanması ile bu koşul gerçekleşmiş ve beşinci onayı takip eden üç aylık sürenin sonunda 1985 yılında yürürlüğe girmiştir. Sözleşme, kişisel verilerin korunması konusunda kabul edilmiş olan bağlayıcı ilk uluslararası belgedir.

Sözleşme’nin hazırlandığı dönemde, Ekonomik İşbirliği ve Kalkınma Örgütü de “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Öte-

⁴ Pearce- Platten , a. g. m., s.531

⁵ Colin J. Bennett/Charles D. Raab, *The Governance of Privacy Policy Instruments in Global Perspective*, Ashgate Publishing Company, England, 2004, s. 72.

⁶ Resolution (73) 22 on the Protection of Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector.

⁷ Resolution (74) 29 on the Protection of Individuals vis-a-vis Electronic Data Banks in the Public Sector.

⁸ Bu şart Sözleşme’nin 22. maddesinde düzenlenmiştir. Bu düzenlemeye göre, Sözleşme, Avrupa Konseyi üyesi beş devletin, Sözleşmeyle bağlanma yönündeki rızalarını açıkladıkları tarihten sonraki üç aylık sürenin bitimini izleyen ayın ilk günü yürürlüğe girer.

si *Transferine İlişkin Rehber İlkeler*” başlığıyla bir belge yayınlamıştır.⁹ Bu belge kişisel verilerin korunması konusunda dünya genelinde kabul edilen ilk belge olmakla beraber, yalnızca tavsiye niteliğindedir ve bağlayıcı özelliği yoktur.

1981 Sözleşmesi’nin hazırlandığı 1979 yılından beri Avrupa Parlamentosu da Avrupa Birliği bünyesinde kişisel veriler açısından koruma sağlanması amacıyla bir belge hazırlanması için Avrupa Komisyonu’na birkaç kez çağrı yapmıştır. Ancak Komisyon bu konuda adım atmaya uzun yıllar yanaşmamıştır.¹⁰ Avrupa Birliği’ne üye bütün devletler, Avrupa Konseyi’nin bir üyesi olarak, 1981 Sözleşmesi’ni onayladıkları için Avrupa Birliği bünyesinde ayrı bir belge hazırlanmasına gerek görülmemiştir. Ancak Birliğe üye devletlerin hepsi bu Sözleşme’yi onaylamış olmalarına rağmen, hem iç hukuklarında farklı düzenlemelere yer vermeye devam etmişler hem de bu alanda etkili bir koruma sağlamamışlardır.¹¹ Bu durum, Avrupa Birliği bünyesinde daha etkili bir koruma sağlayacak bir belgenin kabul edilmesi konusunda Avrupa Parlamentosu’nun ısrarını sürdürmesine neden olmuştur. Bu ısrarların sonucunda Avrupa Birliği tarafından 1995 yılında “*Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunması ve Bu Verilerin Özgür Dolaşımına İlişkin Yönerge*” kabul edilmiştir.¹²

Avrupa Konseyi’nin kabul etmiş olduğu 108 sayılı Sözleşme yalnızca Avrupa Konseyi üyesi olan devletlerin katılımına açık değildir. Konsey üyesi olmayan devletler de Sözleşme’ye taraf olabilir.¹³ Ancak

⁹ OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Document C (80) 58 (Final) October 1, 1980.

¹⁰ Spiros Simitis, “From the Market to the Polis: The EU Directive on the Protection of Personal Data” *IOWA Law Review*, Vol. 80, No. 3, March 1995, s.446.

¹¹ Andrew Charlesworth, “Implementing the European Data Protection Directive 1995 in UK Law: The Data Protection Act 1998”, *Government Information Quarterly*, Vol. 16, No.3, 1999, s.210.

¹² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

¹³ Sözleşme’nin 23. maddesi Avrupa Konseyi üyesi olmayan devletlerin de Sözleşme’ye taraf olmasına olanak tanımaktadır. Ancak Konsey üyesi olmayan bir devletin Sözleşme’ye taraf olabilmesi için Bakanlar Komitesi’nin bu yönde karar alması ve Komite’de temsil hakkına sahip taraf devlet temsilcilerinin oy birliği ile o devleti Sözleşme’ye katılmaya davet etmesi gerekir.

Sözleşme'ye taraf devletlerarasında Avrupa Konseyi üyesi olmayan bir devlet yer almamaktadır.

Sözleşme'yi, Ocak 2010 itibariyle Avrupa Konseyi üyesi 41 devlet onaylamıştır.¹⁴ Türkiye, Sözleşme'yi 1981 yılında imzalamış ancak henüz onaylamamıştır. Sözleşme'nin onaylanmamasının nedeni Sözleşme'nin 4. maddesindeki düzenlemedir. Bu düzenlemeye göre, taraf devletler Sözleşme'deki ilkeleri uygulayabilmek için iç hukuklarında gerekli önlemleri almalıdır. Bu önlemler en geç Sözleşme'nin taraf devlet açısından yürürlüğe girdiği tarihte alınmış olmalıdır. Türkiye'de kişisel verilerin korunmasına ilişkin yasa henüz yürürlüğe girmediği için Sözleşme'nin onaylanması mümkün olmamaktadır.

2001 yılında Sözleşme için bir Ek Protokol imzaya açılmıştır.¹⁵ Protokol, Sözleşme'ye taraf devletlerde ulusal kontrol makamlarının oluşturulmasını zorunlu kılmış ve kişisel verilerin yeterli düzeyde koruma sağlamayan ülkelere ve uluslararası örgütlere transfer edilmesini yasaklamıştır. 2004 yılında yürürlüğe giren bu Protokolü, Ocak 2010 itibariyle Avrupa Konseyi üyesi 25 devlet onaylamıştır.¹⁶

B. 108 Sayılı Sözleşme'nin Temel Amacı ve Uygulama Alanı

Sözleşme'nin temel amacı 1. maddede şöyle açıklanmıştır: Sözleşme'ye taraf devletlerin kendi egemenlik alanında bulunan bireylerin, vatandaşlık ya da oturma durumlarını dikkate almaksızın, kişisel bilgilerinin otomatik işleme tabi tutulması konusunda gerekli güvenceleri sağlayarak, başta özel yaşam hakkı olmak üzere, tüm temel hak ve özgürlüklerini korumaktır.

Bu düzenleme ile taraf devlet topraklarında bulunan yerli yabancı herkes kişiliğini ilgilendiren, kendi ismine bağlı veya isim belirtilme-

¹⁴ Bkz. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG>.

¹⁵ Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, Strasbourg, 8.XI.2001, European Treaty Series- No. 181

¹⁶ Bkz. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=ENG>

miş olsa bile kendisinin belirlenmesini sağlayabilecek her türlü verinin otomatik işleme tabi tutulmasında güvencelere sahip olmaktadır.¹⁷

Sözleşme'nin uygulama alanı ise 3. maddede belirtilmiştir. Bu düzenlemeye göre, Sözleşme kamusal ve özel sektörde kişisel verilerin otomatik yollarla işlenmesine uygulanacaktır. Bu düzenleme ile Sözleşme'nin uygulama alanı dar tutulmuştur. Yalnızca gerçek kişilere ait veriler için koruma sağlamakta ayrıca verilerin otomatik olmayan yollarla işlenmesini kapsamamaktadır.

Sözleşme'nin yalnızca otomatik yollarla işlenen kişisel veriler açısından güvenceler öngörmesi Sözleşme'nin eksikliklerinden biridir. Ancak Sözleşme'deki düzenleme bu yönde olmakla beraber, Sözleşme'ye taraf olan devletlerin Sözleşme'de öngörülen güvencelerden daha geniş güvenceleri kendi iç hukuklarında kabul etmeleri mümkündür. Nitekim Sözleşme'nin 11. maddesi, taraf devletlerin Sözleşme'de öngörülen güvencelerden daha fazla güvenceler sağlayabileceğini, Sözleşme'nin hiçbir hükmünün buna engel olmadığını belirtmiştir.

C. 108 Sayılı Sözleşme'de Yer Alan Temel Kavramlar

108 sayılı Sözleşme'de yer alan temel kavramlara 2. maddede açıklık getirilmiştir. Bu maddeye göre;

Kişisel veri: Kimliği belirlenmiş ya da belirlenebilir bir gerçek kişiyle (veri sahibi) ilgili tüm bilgileri ifade etmektedir.¹⁸

Otomatik işleme tabi tutulan veri kategorileri: Otomatik işleme konu olan bilgilerin tümü anlamına gelmektedir.

Otomatik işleme: Kısmen ya da tamamen otomatik yollarla gerçekleştirilen veri kaydını, bu verilere mantıksal ve/ya aritmetik işlem-

¹⁷ Tekin Akıllıoğlu, "İdari Usul ve Kişisel Verilerin Korunması", www.idare.gen.tr/akillioglu-idariusul.htm.

¹⁸ Bakanlar Komitesi'nin yayınlamış olduğu "Emniyet Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin (87) 15 No.lu Tavsiye Kararı"nda da, Sözleşme'nin 2. maddesinde yer alan kişisel veri tanımı tekrarlanmış ancak kimliğin belirlenmesinin makul olmayan bir zaman, masraf ve emek gerektirmesi durumunda bireyin kimliğinin "belirlenebilir" olarak kabul edilemeyeceği açıklanmıştır.

lerin uygulanmasını, bu verilerin değiştirilmesi, silinmesi, düzeltilmesi ya da açıklanmasını içerir.

Veri işlem sorumlusu: İç hukuka göre otomatik veri işlemenin amacına, hangi veri kategorilerinin kaydedileceğine ve onlara hangi işlemlerin uygulanacağına karar vermeye yetkili olan gerçek ya da tüzel kişi, kamu görevlisi, kurumu ya da diğer herhangi bir organdır.

D. 108 Sayılı Sözleşme'nin Sağladığı Temel Güvenceler

Sözleşme kişisel veriler açısından önemli güvenceler getirmekte ve bu alanda uygulanacak temel ilkeleri belirlemektedir. Kişisel verilerin otomatik yollarla işlenmesinde uygulanacak temel ilkeler 5. maddede belirtilmiştir. Bu maddeye göre, otomatik işleme tabi tutulacak kişisel veriler dürüstlük kuralına ve hukuka uygun olarak elde edilmeli ve işlenmelidir; belli ve meşru amaçlar için kaydedilmeli ve bu amaçlarla bağdaşmayan bir şekilde kullanılmalıdır; kaydetme amaçlarının gerektirdiğinden fazla olmamalı, yeterli ve bağlantılı olmalıdır; doğru olmalı ve gerektiğinde güncelleştirilmelidir; kaydetme amacının gerektirdiğinden daha uzun olmamak koşuluyla, veri sahibinin kimliğini tespiti için gerekli olanak tanıyacak bir formda saklanmalıdır.

Sözleşme hassas veriler açısından daha kapsamlı bir koruma içermektedir. Sözleşme'nin 6. maddesi ırksal kökeni, siyasi görüşleri, dinsel ya da diğer inançları açığa çıkaran kişisel veriler ile kişinin sağlığı ya da cinsel yaşamı ile ilgili olan verilerin ve cezai mahkumiyetlere ilişkin verilerin otomatik yollarla işlenmesini yasaklamaktadır. Ancak bu yasak mutlak değildir. İç hukukun yeterli güvenceyi sağlaması durumunda buna izin verilebileceği belirtilmiştir.

Sözleşme'nin 7. maddesi kişisel verilerin kazara ya da yetkisiz kişilerce imha edilmesini ya da kazara kaybedilmesini önlemek ve yetkisiz kişilerin ulaşmasını, değiştirmesini ya da açıklamasını engellemek amacıyla gerekli önlemleri alma yükümlülüğünü taraf devletlere getirmektedir.

Sözleşme'nin sağladığı güvenceler bunlarla sınırlı değildir. Sözleşme'nin 8. maddesi kişisel verilerin korunabilmesi için ek güvenceler sağlanmasını öngörmüştür. Ek güvenceler arasında şunlar yer almaktadır: Veri sahibi verilerin otomatik olarak kaydedildiği bir kişisel veri dosyasının olup olmadığını, temel amacını ve veri işlem sorumlu-

sunun kimliğini, adresini ve çalıştığı temel kurumu öğrenebilmelidir; kendisine ait verilerin kaydedilip kaydedilmediği konusunda makul aralıklarla ve aşırı gecikme ya da masraf olmaksızın bilgi edinebilmeli ve bu veriler anlaşılabilir bir tarzda kendisine iletilmelidir; şayet veriler Sözleşme’de sağlanan güvencelere aykırı bir şekilde işlenmişse, verileri düzeltebilmeli ya da sildirebilmelidir; bu maddede belirtilen güvencelerin yerine getirilmemesi durumunda hukuksal yollara başvuru hakkı tanınmalıdır.

Sözleşme’de yer alan güvencelere hangi durumlarda istisna ve sınırlamalar getirilebileceği ise 9. maddede belirtilmiştir. Bu maddeye göre; 5, 6 ve 8. maddelerde belirtilmiş olan güvencelere yalnızca bu maddelerde belirtilmiş olan sınırlamalar getirilebilir. Bunların dışında sınırlama getirilmesi ise ancak sınırlamanın yasa ile yapılması ve demokratik bir toplumda gerekli olması koşuluyla, devletin güvenliği ile kamu güvenliğini ve devletin ekonomik menfaatlerini korumak ya da suçu önlemek ya da veri sahibinin veya başkalarının hak ve özgürlüklerini korumak amacıyla yapılması durumunda mümkündür.

Sözleşme’nin 10 maddesi de, verilerin korunması konusunda Sözleşme’de düzenlenen temel ilkelerin uygulanmasını sağlamak için iç hukuklarında gerekli düzenlemeleri yapma ve bu düzenlemelerin ihlali durumunda gerekli yaptırımları ve hukuki çözümleri sağlama görevini taraf devletlere yüklemiştir.

Görüldüğü gibi 108 sayılı Sözleşme taraf devletlere önemli yükümlülükler getirmektedir. Her şeyden önce Sözleşme’ye taraf olacak ülke iç hukukunda bir yasayla verilerin hukuki rejiminin tanımlanması gereklidir. Kısaca, bu Sözleşme doğrudan uygulamaya elverişli olmayıp, bir uygulama yasası aracılığıyla hükümlerinin ayrıntılandırılması ve ülke şartlarına uydurulması gerekmektedir.¹⁹ İç hukuklarda yürürlüğe konulan bu yasalar ile hem Sözleşme’nin etkili hale gelmesi sağlanmış olacaktır hem de kişisel verilerin işlenmesi konusunda ortak temel güvenceler sağlanacaktır.²⁰

¹⁹ Akıllıoğlu, a.g.m., s. 6-7.

²⁰ Paul M. Schwartz, “European Data Protection Law and Restrictions on International Data Flows”, *IOWA Law Review*, Vol. 80, No.3, March 1995, s. 477.

E. Sınır Ötesi Veri Transferi

108 sayılı Sözleşme, bir taraf devletten diğerine yapılacak veri transferinin, özel yaşam gerekçesiyle engellenmesini ya da özel bir izne tabi tutulmasını yasaklamaktadır. Ancak bu yasağa bazı durumlarda istisnalar getirme yetkisi taraf devletlere tanınmaktadır. Konuyu düzenleyen 12. maddeye göre, taraf bir devletin mevzuatı belirli kategorilerdeki kişisel veriler için özel bir düzenleme içeriyorsa ve diğer taraf devletin mevzuatı bu konuda eşit bir koruma içermiyorsa, o devlete yapılacak veri transferine sınırlama getirebilir.

Verilerin sınır ötesi transferi konusu 2004 yılında yürürlüğe giren Ek Protokol'ün 2. maddesinde de ele alınmıştır. Bu düzenleme ile kişisel verilerin Sözleşme'ye taraf olmayan bir uluslararası örgüte ya da ülkeye gönderilmesine ancak bu devletin ya da örgütün eşit düzeyde bir koruma sağlaması koşulu ile izin verilmektedir. Ancak Sözleşme'ye taraf devletin iç hukuku veri sahibinin spesifik menfaatlerini korumak için ya da meşru menfaatleri, özellikle de önemli kamusal menfaatleri korumak için veri transferine izin veriyorsa bu şart aranmayacaktır.

F. 108 Sayılı Sözleşme'nin Öngördüğü Denetim Mekanizması

Sözleşme, kişisel verilerin korunabilmesi için uygulanması zorunlu olan temel ilkeleri ortaya koymakla beraber, bu ilkelerin uygulanmasını kontrol etmekle görevli bir denetim makamı oluşturmamıştır.

Bir denetim organının oluşturulmamış olması Sözleşme'nin diğer bir eksikliğidir. Sözleşme'deki ilkelerin uygulanmasını güvence altına almak amacıyla bir hukuki kurum oluşturulmadığı için, Sözleşme'nin onaylanması kişisel verilere ilişkin ortak bir minimum standardın gerçekten uygulanabileceği anlamına gelmemektedir.²¹

Sözleşme'nin kurulmasını öngördüğü tek organ Danışma Komitesi'dir. Sözleşme'ye taraf olan devletlerin temsilcilerinden oluşan bu organ Sözleşmedeki güvencelerin uygulanmasını denetleme yetkisine sahip değildir. Danışma Komitesi, adının da ifade ettiği gibi bir danışma organıdır.

²¹ Bennett- Raab, *a. g. e.*, s. 72-73.

Danışma Komitesinin işlevleri Sözleşme'nin 19. maddesinde şöyle açıklanmıştır: Sözleşme'nin uygulanmasını kolaylaştırmak ya da geliştirmek amacıyla önerilerde bulunabilir; Sözleşme'de değişiklik yapılmasını önerebilir; Sözleşmede yapılması öngörülen değişiklik önerileri hakkında görüş bildirir; Sözleşme'ye taraf olan devletlerin isteği üzerine, Sözleşme'nin uygulanması ile ilgili tüm sorunlar hakkında görüş bildirir.

Danışma Komitesi düzenlediği her toplantının sonunda, yaptığı çalışmalar ve Sözleşme'nin işleyişi hakkında Avrupa Konseyi Bakanlar Komitesi'ne rapor sunmaktadır. Komite'nin şimdiye kadar yaptığı çalışmalar içinde, 2002 yılında yayınladığı, *"Kişisel veriler açısından yeterli düzeyde koruma sağlamayan üçüncü ülkelere veri transferini sağlayacak sözleşme şartlarının hazırlanmasına ilişkin rehber"*²² ile 2005 yılında yayınladığı, *"Biometrik verilerin toplanması ve işlenmesine Sözleşme'deki ilkelerinin uygulanması konusunda ilerleme raporu"*²³ önem taşımaktadır.

Sözleşme, taraf devletlere iç hukuklarında Sözleşme'ye uygun olarak yürürlüğe koydukları yasal düzenlemelerin uygulanmasını izlemeden sorumlu bir kontrol makamı oluşturma yükümlüğü getirmiştir. Sözleşme'nin bu eksikliği, 2004 yılında yürürlüğe giren Ek Protokol ile giderilmiştir. Protokol'ün 1. maddesi, taraf devletlere kendi iç hukuklarında aldıkları önlemlerin Sözleşme ve Protokol'de yer alan ilkelere uygunluğunu güvence altına almaktan sorumlu olacak bir ya da birden fazla kontrol makamı oluşturma zorunluluğu getirmektedir. Bu kontrol makamları özellikle araştırma ve müdahalede bulunma yetkisine ve aynı zamanda hukuki sürece dahil olma ve kişisel verilerin işlenmesi ile bağlantılı olarak bireylerin kendi temel hak ve özgürlüklerini korumak amacıyla yaptıkları şikayetleri inceleme yetkisine sahip olacaklardır. Kontrol makamlarının görevlerini tam bir ba-

²² Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection (2002) Bkz.http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/reports_and_studies_of_data_protection_committees/

²³ Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005) Bkz.http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/reports_and_studies_of_data_protection_committees/

ğimsızlık içinde yerine getirmeleri öngörülmüş, ancak verdikleri kararlara karşı mahkemelere başvurma olanağı tanınmıştır.

III. BAKANLAR KOMİTESİNİN KARARLARI

Avrupa Konseyi bünyesinde kişisel verilerin korunması konusunda Bakanlar Komitesi tarafından alınan kararlar da büyük önem taşımaktadır. Bakanlar Komitesinin 1973 yılında yayınladığı “*Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*” ile 1974 yılında yayınladığı “*Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar*”ı 108 sayılı Sözleşme’nin hazırlanmasında önemli bir rol oynamıştır. Söz konusu bu iki karar üye devletleri bağlayıcı nitelikte olan kararlardır.

Bakanlar Komitesi bu iki karar dışında çok sayıda tavsiye kararı da kabul etmiştir. Ancak tavsiye kararları üye devletler açısından bağlayıcı olmayan kararlardır. Bunlar açıklayıcı ve yol gösterici nitelikte olan kararlardır.²⁴ Bununla birlikte, bu tavsiyeler Sözleşme’nin temel ilkelerinin verilerin işlenmesine nasıl uygulanacağını belirleyerek taraf devletlerde kişisel veriler açısından sağlanan korumanın güçlenmesine neden olmaktadır.²⁵

Bakanlar Komitesi’nin kişisel veriler alanında şimdiye kadar kabul etmiş olduğu tavsiye kararları şunlardır;

- Doğrudan Pazarlama Amacıyla Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.²⁶

- Sosyal Güvenlik Amacıyla Kişisel Verilerin Korunması Konusunda Tavsiye Kararı.²⁷

²⁴ Renate Gertz, “Is it ‘Me’ or ‘We’? Genetic Relations and the Meaning of ‘Personal Data’ under the Data Protection Directive”, *European Journal of Health Law* 11, 2004, s. 236.

²⁵ Schwartz, a.g.m., s.479.

²⁶ Recommendation No.R (85) 20 on the Protection of Personal Data Used for the Purposes of Direct Marketing, (25.10.1985)

²⁷ Recommendation No.R (86) 1 on the Protection of Personal Data for Social Security Purposes, (23.01.1986)

- Emniyet Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin Tavsiye Kararı.²⁸

- İstihdam Amacıyla Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.²⁹

- Ödeme ve Diğer İşlemler İçin Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.³⁰

- Kamu Makamlarının Elinde Bulunan Kişisel Verilerin Üçüncü Kişilere İletilmesine İlişkin Tavsiye Kararı.³¹

- Telefon Hizmetleri Alanındaki Kişisel Veriler Başta Olmak Üzere, Telekomünikasyon Hizmetleri Alanındaki Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.³²

- Tıbbi Verilerin Korunmasına İlişkin Tavsiye Kararı.³³

- İstatistiksel Amaçlarla Toplanan ve İşlenen Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.³⁴

- İnternette Özel Yaşamın Korunmasına İlişkin Tavsiye Kararı.³⁵

- Sigorta Amacıyla Toplanan ve İşlenen Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.³⁶

²⁸ Recommendation No.R (87) 15 Regulating the Use of Personal Data in the Police Sector (17.09.1987)

²⁹ Recommendation No.R (89) 2 on the Protection of Personal Data Used for Employment Purposes (18.01.1989)

³⁰ Recommendation No. R (90) 19 on the Protection of Personal Data Used for Payment and Other Operations (13.09.1990)

³¹ Recommendation No.R (91)10 on the Communication to Third Parties of Personal Data Held by Public Bodies (09.09.1991)

³² Recommendation N.R (95) 4 on the Protection of Personal Data in the Area of Telecommunication Services, With Particular Reference to Telephone Services (07.02.1995)

³³ Recommendation No. R (97) 5 on the Protection of Medical Data (13.02.1997)

³⁴ Recommendation No. R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes (30.09.1997).

³⁵ Recommendation No. R (99) 5 for the Protection of Privacy on the Internet (23.02.1999)

³⁶ Recommendation No. R (2002) 9 on the Protection of Personal Data Collected and Processed for Insurance Purposes (18.09.2002)

IV. AVRUPA İNSAN HAKLARI SÖZLEŞMESİ

A. Avrupa İnsan Hakları Sözleşmesinin Sağladığı Koruma

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi özel yaşam hakkını güvence altına alan bir düzenlemeye yer vermiştir. Özel yaşamın ve aile yaşamının korunması başlığını taşıyan 8 (1). madde şöyledir: *"Herkes özel yaşamına, aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir"*.

8. maddenin 1. fıkrasında düzenlenen hak mutlak bir hak değildir. Sözleşme'ye taraf devlet yine Sözleşme'de belirtilmiş olan neden veya nedenlere dayanarak bu hakta sınırlama yapabilecektir. Bu konudaki düzenleme 8. maddenin 2. fıkrasında yer almıştır. Buna göre: *"Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olması koşuluyla söz konusu olabilir"*.

Sözleşme kişisel verilerin korunması ile ilgili ayrı bir hüküm içermemektedir. Ancak Sözleşme'de öngörülen hakların ihlaline ilişkin iddiaları inceleme yetkisine sahip olan Avrupa İnsan Hakları Mahkemesi kişisel verilerin özel yaşam alanı içinde yer aldığını kabul etmekte ve bu konuyla ilgili başvuruları 8. madde altında incelemektedir.

8. maddenin özel yaşamın korunması konusunda taraf devletlere yüklediği yükümlülük yalnızca keyfi müdahalede bulunmayı yasaklayan negatif bir yükümlülük değildir. Maddede yer alan *"saygı gösterilmesi"* ifadesi, devletin yalnızca müdahalede bulunmamayı değil, aynı zamanda bu hakların fiilen ve gerçekten kullanılmasına olanak verecek önlemleri alma konusunda pozitif bir yükümlülük yüklediğini de ifade etmektedir.

Devletin negatif yükümlülüğü, özel yaşamın korunması amacıyla belirli eylemleri yapmaktan kaçınmasını ifade eder. Kişisel verilerin korunması açısından devletin negatif yükümlülüğü, Sözleşme'ye aykırı olarak kişisel verileri toplama, saklama ve işleme gibi müdahalelerden kaçınmasını ifade eder. Devletin pozitif yükümlülüğü ise, özel yaşam hakkına saygıyı güvence altına almak için gerekli önlemleri al-

masını ifade eder.³⁷ Devlet kişisel verilerin gizliliğini güvence altına alabilmek için, kişisel verileri koruyacak kuralları yürürlüğe koymak ve gerekli güvenceleri sağlamak yükümlülüğü altındadır.³⁸

B. Avrupa İnsan Hakları Mahkemesinin Kararları

Avrupa İnsan Hakları Mahkemesi (bundan sonra Mahkeme olarak anılacaktır), kişisel verilerin korunmasıyla bağlantılı başvurulara ilişkin verdiği kararlarda, kişisel verilerin özel yaşam alanı içinde yer aldığını belirtmekte ve kişiye ilişkin verilerin kamusal görevliler tarafından toplanması, saklanması ve açıklanmasıyla ilgili sorunları Sözleşme'nin 8. maddesi içinde ele almaktadır.

Mahkeme bu alanda yapılan başvuruları incelediğinde öncelikle yapılan işlemin ya da alınan önlemin Sözleşme'nin 8. maddesinde güvence altına alınan özel yaşam hakkına yönelik bir müdahale oluşturup oluşturmadığını değerlendirmektedir. Bir müdahalenin olduğuna kanaat getirmesi durumunda, bu müdahalenin ulusal yasalara uygunluğunu incelemektedir. Ancak müdahalenin ulusal yasalara uygunluğunu yeterli bulmamakta ayrıca ulusal yasanın hem Avrupa İnsan Hakları Sözleşmesi'ne hem de 108 sayılı Sözleşme'ye uygun olup olmadığını değerlendirmektedir.

a. Kişisel Verilerin Toplanması ve Saklanması

Kişisel verilerin toplanması ve saklanması ile ilgili sorunların Avrupa İnsan Mahkemesi'ne getirilmesi ancak 1970'li yıllarda olmuştur. Mahkeme bu alanda vermiş olduğu ilk önemli kararda kişisel veri kavramını kullanmamakla beraber kişiye ilişkin bilgilerin gizli izleme yöntemleriyle toplanması konusunu ele almıştır.

Mahkeme'nin bu konuyu ele aldığı ilk dava *Klass ve Diğerleri v. Almanya* davasıdır.³⁹ Mahkeme bu davada verdiği kararla, istihbarat örgütlerinin gizli izleme yoluyla bireylerin haklarına yönelik gerçekleştirdikleri müdahalelerin etkili bir denetime tabi olması gerektiğini

³⁷ Bkz. X and Y v. The Netherlands, 8978/80, 26.03.1985, prg. 23.

³⁸ Bkz. I v. Finland, 20511/03, 17.07.2008, prg.37.

³⁹ *Klass and Others v. Germany*, 5029/71, 06.09.1978.

kabul etmiş⁴⁰ ve ulusal güvenlikten kaynaklanan ihtiyaçlara her durumda öncelik verilemeyeceğini, Avrupa ülkelerinin casusluk ve terörizmle mücadeleyi gerekçe göstererek uygun gördükleri her türlü tedbiri alamayacaklarını açıklamıştır.⁴¹

Mahkeme bu davada, mektupların ve telgrafların okunmasına, telefon görüşmelerinin dinlenmesi ve kaydedilmesine olanak tanıyan bir yasanın Sözleşme'ye uygunluğunu incelemiştir. Mahkeme genel olarak gizli izleme yöntemlerine demokratik kurumların korunması için kesinlikle zorunlu olması durumunda başvurulabileceğini kabul etmiş, ancak bireyin 8. maddede güvence altına alınan hakkı kullanabilmesi ile demokratik bir toplumu koruma amacıyla gizli izlemenin yapılmasının gerekliliği arasında bir denge kurulması gerektiğini belirtmiştir. Mahkeme'ye göre, bu konuda devletlerin sınırsız bir takdir yetkisi yoktur. Sınırsız önlemler alınmasına izin veren bir yasa demokrasi için tehdit oluşturur. Gizli izlemeye olanak tanınması durumunda bunun kötüye kullanılmasının engellenmesi için yeterli ve etkili güvencelerin sağlanması gerekir. İzleme ancak başka bir yöntemle bilgilere ulaşılamıyorsa yapılmalı, yazılı izin şartı aranmalı ve belli bir süreyle sınırlı tutulmalıdır. İzlemeyi gerektiren nedenlerin ortadan kalması durumunda izlemeye son verilmeli, elde edilen veriler başka bir amaç için kullanılmamalı, izlemenin amacının gerçekleşmesi durumunda veriler en kısa süre içinde imha edilmelidir. Mahkeme, mevcut yasanın bu güvenceleri sağladığını saptamış ve bu nedenle 8. maddenin ihlal edilmediğine karar vermiştir.

Mahkeme'nin kişisel verilerin toplanması ve saklanması konusunu ele aldığı en önemli davalardan biri Leander v. İsveç davasıdır.⁴² Mahkeme'nin bu davada vermiş olduğu karar, yargı yolunun kullanılmasına gerek kalmaksızın da etkili bir denetim yolunun kolaylıkla sağlanabileceğini göstermektedir.⁴³ Davaya konu olan olayda başvuru- rucunun, askeri güvenlik bölgesinde yer alan denizcilik müzesindeki

⁴⁰ B. Van Loenen/J. A. Zevenbergen, "The Impact of the European Privacy Regime on Location Technology Development", *Journal of Location Based Services*, Vol.1, No.3, September 2007, s. 171.

⁴¹ Van Loenen/Zevenbergen, a.g.m., s.172.

⁴² Leander v. Sweden, 9248/81, 26.03.1987.

⁴³ Hiral Bhatt, "RIPA 2000: A Human Rights Examination", *The International Journal of Human Rights*, Vol. 10, No.3, September 2006, s. 304.

görevine son verilmiştir. Buna gerekçe olarak da kendisi hakkında yapılan güvenlik soruşturmasının sonucunun olumsuz olması gösterilmiş ancak bu bilgilerin içeriği hakkında kendisine bilgi verilmemiştir. Başvurucu, kendisi hakkında bilgi toplanmasının, toplanan bilgilerin içeriği hakkında kendisine bilgi verilmemesinin ve bu bilgilerin yanlışlığını kanıtlama hakkının kendisine tanınmamasının özel yaşam hakkını ihlal ettiğini iddia etmiştir.

Mahkeme bu davada özel yaşam hakkına yönelik bir müdahale olduğunu kabul etmiş ancak bu müdahaleyi haklı kılacak koşulların mevcut olduğu sonucuna varmıştır. Mahkeme'ye göre, söz konusu müdahale yasaya dayanılarak yapılmıştır. Konuyu düzenleyen yasa kişisel verilerin korunması açısından yeterli güvenceyi sağlamaktadır. Bu güvenceler arasında; yalnızca bağlantılı bilgilerin toplanmasına ve açıklanabilmesine izin verilmesi, bu verilere dayanılarak alınan kararlara itiraz etme hakkının tanınmış olması, bu alandaki işlemlerin Meclis Adalet Komisyonu, Meclis Ombudsmanı ve Adalet Bakanı tarafından denetlenmesi gibi güvenceler yer almaktadır. Başvurucu hakkında toplanmış olan verilerin içeriği hakkında başvurucuya bilgi verilmemiş olması, müdahaleyi Sözleşme'ye aykırı hale getirmez. Devletin bu konuda bir takdir yetkisi vardır. Bu tür bir müdahale ulusal güvenliğin korunması amacıyla demokratik bir toplumda gerekli olan bir müdahaledir ve izlenen meşru amaçla orantılıdır. Bu nedenler dikkate alındığında 8. maddenin ihlali söz konusu değildir.

Mahkeme, devletin ulusal güvenliğin korunması açısından önem taşıyan görevlere getirilecek adayların bu görevler için uygun olup olmadığını değerlendirirken, bu adaylar hakkında toplanan verileri kullanabileceğini kabul etmiştir. Ancak bu olayda, başvurusunun müzede yapacağı işin niteliği üzerinde durmamış ve bu işin ulusal güvenlik açısından tehlike taşıyıp taşımadığı konusunu incelememiştir.⁴⁴

Leander v. İsveç kararı pek çok açıdan eleştirilebilir. Ancak Mahkeme bugünkü yapısı ve anlayışı ile Leander kararından birkaç adım

⁴⁴ Leander v. İsveç kararının verildiği 1987 yılında Danıştay tarafından verilen bir karar bu açıdan ele alınmaya değerdir. Danıştay, davacının güvenlik görevlisi olarak görev yapmasına engel olarak gösterilen hususların yapacağı görevin niteliği de göz önüne alındığında görevine son verilmeyi gerektirecek ve hukuken geçerli kabul edilebilecek nitelikte olmaması nedeniyle kararın bozulmasına ve dava konusu işlemin iptaline karar vermiştir. Bkz. Danıştay 5. Daire, 19.03.1987, E. 1987/193, K. 1987/433, *Danıştay Dergisi*, S.68-69, 1988, s. 385-386.

ötede sayılabilir.⁴⁵ Bu kararın verildiği yıl Bakanlar Komitesi tarafından yayınlanmış olan “Emniyet Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin Tavsiye Kararı”nda da Mahkemenin vermiş olduğu karardan daha ileri bir yaklaşım ortaya konulduğu söylenebilir. Tavsiye Kararı’nın 2. ilkesinde verilerin polisiye amaçlarla toplanmasına ancak gerçek bir tehlikenin önlenmesi ya da belirli bir suçun engellenmesi için zorunlu olması durumunda başvurulması gerektiği belirtilmiştir. Ayrıca kişinin bilgisi dışında kişiye ilişkin verilerin toplanması ve saklanması durumunda, bu veriler silinmediği takdirde, kişiye bu konuda bilgi verilmesi istenmiştir.

Mahkeme Leander v. İsveç davasında kişisel verilerin korunması konusunda devletin negatif yükümlülüğünü ele almıştır. Bu davadan kısa bir sonra incelediği Gaskin v. Birleşik Krallık⁴⁶ davasında ise kişisel verilerin korunması konusunda devlete düşen pozitif yükümlülüğü ele almıştır.

Gaskin v. Birleşik Krallık davasına konu olan olayda, çocukluğunu sosyal hizmetlerin bakımı altında geçirmiş olan başvurucu, geçmiş hakkında bilgi edinmeyi, nerelerde yaşadığı ve kimler tarafından hangi koşullarda bakıldığı konusunda tutulan raporların kendisine açıklanmasını istemektedir. Bu raporlardaki bilgilerin, kendi geçmişi hakkında bilgi edinmesini sağlayacağını ve bugün yaşamış olduğu sıkıntı ve sorunların çözümüne katkıda bulunacağını ileri sürmektedir. Ancak bu talebi, bu tür raporları hazırlayan görevlilerin söz konusu raporların ilgili kişiye açıklanmayacağını bildikleri için gerçek görüşlerini açıklıkla ortaya koydukları, eğer bu raporlar açıklanırsa bu görevlilerin yeterince açık olmaktan kaçınabileceği ve bu durumun mevcut sosyal hizmet sisteminin iyi işlemesine engel olabileceği gerekçesiyle reddedilmiştir.

Mahkeme’nin Gaskin v. Birleşik Krallık davasında verdiği karar özellikle devletin kişisel verilerin korunması konusunda pozitif yükümlülüğünü ele aldığı bir karar olması açısından önem taşımaktadır. Mahkeme’ye göre, bay Gaskin ne kendisi hakkında veri toplanmasına ve saklanmasına itiraz etmekte ne de bu verilerin kendi zararına kullanıldığını iddia etmektedir. Kendisi hakkında tutulan raporların bü-

⁴⁵ Akıllıoğlu, a. g. m., s. 7.

⁴⁶ Gaskin v. the United Kingdom, 10454/83, 07.07.1989.

tününe ulaşamamaktan şikayet etmektedir. Burada başvuruçunun şikayet ettiği şey devletin eylemi değil, eylemsizliğidir. Bu nedendir ki, başvuruçunun kendisi hakkında tutulan raporlara ulaşması talebini reddeden devletin, 8. maddenin getirdiği pozitif yükümlüğü ihlal edip etmediğinin incelenmesi gerekir. Davayı bu açıdan ele alan Mahkeme, başvuruçunun kendi çocukluğuna ilişkin bilgilere ulaşabilmesinde yaşamsal bir menfaatinin olduğunu kabul etmiştir. Mahkeme'ye göre, raporları hazırlayan kişilere ulaşamaması ya da bu kişilerin açıkça itiraz etmemesi durumunda, bu raporlara ulaşmak isteyen bireyin menfaatleri güvence altına alınmalıdır. Şayet raporların hazırlanmasına katkıda bulunan kişiler raporların açıklanmasına rıza göstermiyor ya da cevap vermiyorlarsa bu durumda, raporların açıklanmasına ilişkin nihai kararı bağımsız bir otoritenin vermesi sağlanmalıdır. Mevcut olayda bu sağlanmamıştır. Bu nedenle 8. maddenin öngördüğü pozitif yükümlülüğün ihlali söz konusudur.

Birleşik Krallık'ta yaşayan yaklaşık 350.000 yetişkinin çocukluk döneminin tamamını ya da bir kısmını sosyal hizmetlerin bakımı altında geçirdiği bilinmektedir. Bunların hepsi hakkında tutulmuş raporlar mevcuttur. Bu raporlardaki veriler o kişiler için çok büyük bir önem taşımaktadır. Bu verilere ulaşılması, kişinin ailesini araştırma ya da çocukluk deneyimlerini öğrenme sürecinde çok önemli bir rol oynayabilmektedir.⁴⁷ Gaskin v. Birleşik Krallık davasında tartışma konusu olan veriler de başvuruçunun psikolojik sağlığı açısından özel bir öneme sahip olan verilerdir. Bu verilere ulaşmasının reddedilmesi başvuruçunun kişisel gelişimini önemli ölçüde engelleyecektir. Bu nedenle, bu karar bireyin kendisine ait her türlü kişisel veriye ulaşmasına olanak tanıyan bir hakkın varlığını kabul eden bir karar şeklinde yorumlanamaz.⁴⁸

Kişisel verilerle ilgili diğer önemli bir karar da Amann v. İsviçre⁴⁹ kararıdır. Bir iş adamı olan başvuruçuyu Sovyet Büyükelçiliği'nde çalışan bir bayan telefonla arayarak bir ürün siparişi vermiştir. Büyükelçilik telefonlarını dinleyen İsviçre Federal Savcılığı başvuruçunun hakkın-

⁴⁷ Christine Horrocks/Jim Goddard, "Adults Who Grew Up in Care: Constructing the Self and Accessing Care Files", *Child and Family Social Work*, 2006, No. 11, s. 264.

⁴⁸ Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, Vol.6, No.3, s.278

⁴⁹ Amann v. Switzerland, 27798/95, 16.02.2000.

da bir fiş oluşturmuştur. Söz konusu olay 1981 yılında gerçekleşmiştir. Kendisi hakkında tutulan fişin varlığını 1990 yılında öğrenen başvuru tazminat talebinde bulunmuş ancak bu talebi İsviçre makamları tarafından reddedilmiştir. Başvuruyu inceleyen Mahkeme, telefon görüşmelerinin dinlenmesi ve kayda alınmasının ve bireyin özel yaşamına ilişkin bilgilerin kamu görevlileri tarafından saklanması özel yaşama bir müdahale oluşturduğunu kabul etmiştir. Mahkeme, yapılan müdahalenin yasaya dayanılarak yapıldığını saptamış ancak mevcut yasal düzenlemenin yeterli korumayı sağlamadığını açıklamıştır. Mevcut yasa savcılık makamının veri toplama, kaydetme ve saklama yetkisini kullanma koşullarını ve kapsamını belirlememekte, hangi bilgilerin saklanacağı ve nasıl bir yöntem izleneceği konusunda açıklık içermemektedir. Bu nedenden dolayı 8. maddenin ihlali söz konusudur.

Rotaru v. Romanya davasında⁵⁰ ise Romanya İstihbarat Örgütü'nün başvuru hakkında tuttuğu gizli dosya ele alınmıştır. Bu dosyada, başvuru aşırı sağcı ve Yahudi düşmanı olan bir grubun mensubu olduğu belirtilmiştir. Bu bilgilerin gerçek dışı olduğunu iddia eden başvuru, dosyadaki bilgilerin silinmesini ya da düzeltilmesini istemiş ve tazminat talep etmiştir. İstihbarat Örgütü dosyadaki bilgilerin ilgili kişiye ait olmadığını, bir isim yanlışlığı olduğunu açıklamıştır. Ancak bu düzeltmeye rağmen ulusal mahkeme tazminata karar vermemiştir.

Avrupa İnsan Hakları Mahkemesi'nde görülen bu davada ilgili devlet, dosyada yer alan bilgilerin özel yaşama ilişkin bilgileri içermediğini kamusal alandaki faaliyetlerle ilgili olan bilgileri içerdiğini ileri sürmüştür. Mahkeme bu itirazın kabul görmeyeceğini çünkü 108 sayılı Sözleşme'nin kişisel veriyi, kimliği belirlenmiş ya da belirlenebilir bir gerçek kişiyle ilgili her türlü bilgi olarak tanımladığını belirtmiş, ayrıca, kamusal bilgilerin yetkililer tarafından sistematik bir şekilde toplanıp dosyalarda saklanması durumunda bu bilgilerin özel yaşam alanına girdiğinin kabul edileceğini açıklamıştır. Müdahalenin yasaya dayanılarak yapıldığını kabul eden Mahkeme, yürürlükte olan yasanın ulusal güvenliği etkileyecek bilgilerin toplanmasına, kaydedilmesine ve gizli dosyalarda arşivlenmesine izin verdiğini saptamış ancak bu yasanın Avrupa İnsan Hakları Sözleşmesi ile uyumlu olmadığını

⁵⁰ Rotaru v. Romania, 28341/95, 04.05.2000.

belirtmiştir. Çünkü söz konusu yasanın hiçbir hükmü bu yetkinin kullanılmasına herhangi bir sınır getirmemiştir. Örneğin, hangi tür bilgilerin kaydedebileceğini, bilgi toplama ve saklama gibi izleme önlemlerinin hangi kategorideki insanlara uygulanabileceğini, bu tür önlemlerin hangi koşullarda alınabileceğini ve nasıl bir yöntemin izleneceğini açıklamamıştır. Ayrıca, bilgilerin ne kadar süreyle saklanacağına da açıklık getirmemiştir. Bu nedenle 8. maddenin ihlali söz konusudur.

Mahkeme, Segerstedt-Wiber ve Diğerleri v. İsveç davasında da⁵¹ kişisel verilerin kamusal makamlar tarafından toplanması ve saklanması konusunu ele almıştır. Bu davada başvuruçular, kendilerine ait kişisel verilerin Gizli Polis kayıtlarında saklanmasının ve bunların tam içeriği hakkında kendilerine bilgi verilmemesinin 8. maddeyi ihlal ettiğini ileri sürmüşlerdir. Mahkeme, Gizli Polis kayıtlarında saklanan bilgilerin açık bir şekilde özel yaşam alanına giren veriler olduğunu saptamıştır. Ancak ilk başvuruçuya ilişkin saklanan veriler arasında, ona ve başkalarına yönelik bir bombalı saldırı tehdidinde ilişkin bilgiler yer almaktadır. Mahkeme bu bilginin saklanmasının suçun önlenmesi amacıyla yönelik olduğunu ve bu nedenle 8. maddenin ihlalinin söz konusu olmadığını açıklamıştır. Diğer başvuruçular hakkında toplanan ve saklanan veriler ise, üye oldukları siyasi partiler ve katıldıkları mitingler gibi, siyasi faaliyetlerine ilişkin bilgileri içermektedir. Bu tür faaliyetlerin devletin ulusal güvenliğine yönelik ciddi bir tehdit oluşturduğuna ilişkin yeterli kanıt hükümet ortaya koyamadığı için, bu verilerin sürekli bir şekilde saklanması başvuruçuların özel yaşamına yönelik orantısız bir müdahale oluşturmaktadır. Saklanan verilerin tamamının başvuruçulara açıklanmaması konusunda ise, yasanın buna olanak tanıdığı ve bu veriler açısından yeterli güvencenin sağlanmış olduğu gerekçesiyle 8. maddenin ihlal edilmediğine karar vermiştir.

b. Telefonların Dinlenmesi, Ses, Fotoğraf ve Görüntünün Kaydedilmesi

aa. Telefonların Dinlenmesi ve Ses Kaydı

Mahkeme'nin telefonların dinlenmesi ve bu yolla elde edilen verilerin kaydedilmesi ve kullanılmasının Sözleşme'ye uygunluğu konu-

⁵¹ Segerstedt/Wiberg and Others v. Sweden, 62332/00, 06.06.2006.

sunu ele aldığı davalar içinde Malone v. Birleşik Krallık davası⁵² önemli bir yer tutmaktadır. Mahkeme bu davada, telefon dinlemeye izin veren yasanın nasıl olması gerektiği üzerinde durmuştur. Mahkeme'ye göre, Sözleşme'de belirtilmiş olan "yasayla öngörülmuş olma şartı" yalnızca iç hukukta bir yasal düzenlemenin mevcudiyetini zorunlu kılmamakta ayrıca bu yasanın hukukun üstünlüğüne de uygun olmasını gerektirmektedir. İç hukukta kamusal makamların keyfi müdahalelerine karşı koruyacak hukuki önlemlerin olması gerekir. Yasa, özel yaşama ve haberleşmeye saygı hakkına yönelik gizli ve tehlikeli olma olasılığı olan bir müdahalede bulunma yetkisinin kamusal makamlara hangi durumlarda ve koşullarda verildiği konusunda vatandaşlara yeterli bilgiyi verecek şekilde gerekli açıklığı içermelidir. Yasa, kamusal makamlara takdir hakkı tanıyorsa bunun alanını da net bir şekilde belirlemelidir.

Mahkeme telefonların dinlenmesiyle ilgili olan başvurulara ilişkin verdiği diğer kararlarda da yasanın niteliğine ilişkin Malone v. Birleşik Krallık kararında ortaya koyduğu ilkeleri tekrarlamıştır.⁵³

Mahkeme yalnızca ev telefonuyla yapılan görüşmelerin değil, aynı zamanda iş yerinden yapılan görüşmelerin dinlenmesi ve konuşmaların kaydedilmesi durumunda da özel yaşama saygı hakkının ihlal edilebileceğine karar vermiştir.⁵⁴

bb. Gizli Dinleme Cihazı ile Ses Kaydı

Mahkeme, telefon görüşmelerinin dinlenmesi ve görüşmelerin kaydedilmesi dışında, gizli dinleme cihazı ile yapılan dinlemeler sonucunda veri toplanması ve bu verilerin kullanılması sorununu da incelemiştir.

Bu konunun ele alındığı Khan v. Birleşik Krallık⁵⁵ davasında polis tarafından yerleştirilen gizli dinleme cihazı ile elde edilen verilerin de-

⁵² Malone v. the United Kingdom, 8691/79, 26.04.1985.

⁵³ Bkz. Kruslin v. France, 11801/85, 24.04.1990; Huvig v. France 11105/84, 24.04.1990; Halford v. the United Kingdom, 20605/92, 26.06.1997; Kopp v. Switzerland, 23224/94, 25.03.1998; Copland v. the United Kingdom, 62617/00, 03.04.2007.

⁵⁴ Bkz. Halford v. the United Kingdom, 20605/92, 26.06.1997; Copland v. the United Kingdom, 62617/00, 03.04.2007; Kopp v. Switzerland, 23224/94, 25.03.1998.

⁵⁵ Khan v. the United Kingdom, 35394/97, 12.05.2000.

lil olarak kullanılması sonucu mahkum edilmiş olan bir kişinin başvurusu incelenmiştir. Bu dinlemenin yasal bir bağlayıcılığı olmayan ve kamu tarafından ulaşılabılır olmayan bir rehberle dayandırıldığını saptayan Mahkeme 8. maddenin ihlal edildiğine karar vermiştir.

Mahkeme daha sonraki yıllarda da gizli ses kaydı ile veri toplamanın Sözleşme'ye uygunluğunu incelediği kararlarında gizli ses kaydı yapılmasının iç hukukta yasal dayanağının olması gerektiği üzerinde önemle durmuştur.

P. G. ve J. H. v. Birleşik Krallık⁵⁶ davasına konu olan olayda başvurucuların silahlı soygun yapacaklarına ilişkin ihbar alan polis, başvurucuların bulduklarını düşündükleri bir eve dinleme cihazı yerleştirmiştir. Bu işlem önce sözlü bir emre dayanılarak yapılmış ancak daha sonra geriye dönük olarak yazılı izin alınmıştır. Ayrıca bu evde bulunan telefonla hangi numaralarla görüşme yapıldığının saptanabilmesi için telefon kayıtları incelenmiştir. Bu olaylardan kısa bir süre sonra başvurucular hırsızlık eyleminde kullanılabilecek malzemelerin bulunduğu bir çalıntı otomobilde yakalanmış ve tutuklanmışlardır. Evde yapılan dinleme sonucunda kaydedilen seslerin başvuruculara ait olup olmadığını saptanabilmesi için, başvurucuların kaldıkları hücreye, onların bilgisi ve izni olmadan bir ses kayıt cihazı yerleştirilmiştir. Ses kayıtlarını inceleyen bir uzman evde kaydedilen seslerden birinin "*muhtemelen*" ilk başvurucuya diğerinin de "*çok muhtemelen*" ikinci başvurucuya ait olduğunu belirtmiştir. Bu veriler yargılama sırasında delil olarak kullanılmış ve başvuruculara ceza verilmiştir. Mahkeme, başvurucuların buldukları eve ve kaldıkları hücreye dinleme cihazı yerleştirilmesinin yasal bir dayanağı olmadığı için 8. maddenin ihlal edildiğine karar verirken, telefon kayıtlarının incelenmesinin yasal olduğuna ve demokratik bir toplumda gerekli bir önlem olduğuna karar vererek bu açıdan 8. maddenin ihlal edilmediğine karar vermiştir.

Mahkeme, Lewis v. Birleşik Krallık⁵⁷ ile Chalkley v. Birleşik Krallık⁵⁸ davasında da yasal bir dayanağı olmadan gizli dinleme cihazı yerleştirilmesinin ve bu dinlemeden elde edilen verilere dayanılarak veri-

⁵⁶ P. G. and J.H. v. the United Kingdom, 44787/98, 25.09.2001.

⁵⁷ Lewis v. the United Kingdom, 1303/02, 25.11.2003.

⁵⁸ Chalkley v. the United Kingdom, 63831/00, 12.09.2003.

len mahkumiyet kararlarının Sözleşme'ye aykırı olduğuna karar vermiştir.

cc. Fotoğraf ve Kamera Çekimi

Murray v. Birleşik Krallık davasında,⁵⁹ güvenlik güçleri tarafından eve yapılan baskın sırasında başvurucuların kimliklerine ilişkin bilgilerin kayda geçirilmesi, gözaltına alınan ilk başvurucunun götürüldüğü merkezde fotoğrafının çekilmesi ve aile fertlerine ilişkin soruların sorulması konusu ele alınmıştır. Terör suçlarının özel niteliğine ve demokratik bir toplum için yarattığı tehlikeye dikkat çeken Mahkeme, ulusal makamların bu alanda alınacak önlemler konusunda takdir hakkının olduğunu, olayda kullanılan yöntemlerin izlenen amaçla orantılı ve demokratik toplumda suçla mücadele için zorunlu olduğunu, baskın sırasında evde bulunan kişilere ilişkin temel kişisel bilgilerin kayda geçirilmesinin ve gözaltına alınan kişinin fotoğrafının çekilmesinin hukuka uygun olduğunu belirtmiş ve 8. maddenin ihlal edilmediği sonucuna varmıştır.

Friedl v. Avusturya davası da⁶⁰ kişisel verilerin kaydı ve fotoğraf çekimi ile ilgilidir. Başvurucu, evsizlerin yaşadığı zorluklara kamuoyunun dikkatini çekmek amacıyla yapılan bir oturma eylemine katılmıştır. Eylemin sona erdirilmesi için yapılan çağrıya uymayan göstericilerin kimlik tespitleri yapılmış, fotoğrafları çekilmiş ve görüntüleri kameraya kaydedilmiştir. Hükümet kaydedilen kişisel bilgilerin ve çekilen fotoğrafların veri işletim sistemine dahil edilmediğini, gösteri ile ilgili oluşturulan dosyanın, normal uygulamaya göre, gerekli işlemlerin tamamlanmasının üzerinden on yıl geçtikten sonra imha edileceğini belirtmiştir. Avrupa İnsan Hakları Komisyonu 8. maddenin ihlal edilmediğini ancak kişisel bilgilerin toplanmasına karşı başvurulabilecek etkili hukuk yollarının mevcut olmamasından dolayı 13. maddenin ihlal edildiği yönünde görüş açıklamıştır. Komisyon, fotoğrafların çekilmesi ve saklanması konusunda ise 13. maddenin ihlal edildiği sonucuna varmamıştır. Davada dostça çözüm yoluna gidilmiştir. Avusturya hükümeti negatifler de dahil olmak üzere çekilmiş bütün fotoğ-

⁵⁹ Murray v. the United Kingdom, 14310/88, 24.10.1994.

⁶⁰ Friedl v. Austria, 15225/89, 31.01.1995.

rafların imha edilmesini kabul etmiş ve başvurucuya tazminat ödemiştir.

Perry v. Birleşik Krallık⁶¹ davasına konu olan olayda, gözaltına alınan başvurucunun görüntüleri polis merkezinde rutin bir şekilde görüntü alan kameralarla çekilmiştir. Ancak bu işlem yapılırken daha net görüntü alınabilmesi için gerekli ayarlamalar yapılmış ve kamera farklı bir hızla çalıştırılmıştır. Bu işlemin yapıldığı konusunda başvurucuya bilgi verilmemiş ve elde edilen net görüntülere fotomontaj yoluyla başka şahısların görüntüleri eklenerek teşhis amacıyla tanıklara gösterilmiştir. Başvurucu ve avukatına bu kaydın yapıldığı ve teşhis amacıyla kullanıldığı konusunda bilgi verilmemiştir. Mahkeme polis merkezlerinde ya da alışveriş merkezleri gibi yerlerde bulunan kameralarla rutin bir şekilde görüntü kaydı yapılmasının 8. maddeyi ihlal etmediğini açıklamış ancak olayda farklı bir durumun söz konusu olduğunu belirtmiştir. Olayda, daha net görüntü alınabilmesi için kameraların ayarı değiştirilmiş ve alınan görüntüler üzerinde fotomontaj yapılarak teşhis amacıyla kullanılmıştır. Bu tür bir hileye başvurulması bu tür kameraların olağan ya da beklenilebilir kullanımın ötesine geçmektedir. Bu nedenle, görüntü kaydı ve ileride kullanmak amacıyla fotomontaj yapılması başvurucu hakkında kişisel verinin toplanması ya da işlenmesi anlamına gelmektedir. Görüntü kaydı için başvurucunun izni alınmalı, bu görüntülerin teşhis amacıyla kullanılacağı konusunda kendisine bilgi verilmeli ve içeriğine itiraz etme hakkı tanınmalıydı. Yapılan bu uygulamayı haklı kılacak bir yasal dayanak iç hukukta mevcut değildir. Bu nedenle, kamera görüntülerinin kaydedilmesi ve kullanılması onun özel yaşamına yönelik bir müdahaledir.

Peck v. Birleşik Krallık⁶² davasında ise, kapalı devre kameralarla çekim yapılması değil, bu kameraların kaydettiği görüntülerin yayınlamasının özel yaşam hakkını ihlal ettiği ileri sürülmüştür. Başvurucu, kapalı devre kameraların kayıt yaptığı kamuya açık bir alanda intihar teşebbüsünde bulunmuştur. Bu eylemine ilişkin kaydedilen görüntüler kameraların yararlarını anlatmak amacıyla yetkililer tarafından basın mensuplarına sunulmuş ve bazı televizyon kanalları da başvurucunun yüzünü kapatmadan bu görüntüleri yayınlamıştır. Başvurucu, kaydedilen görüntülerin yayınlamasının özel yaşam hakkını ihlal etti-

⁶¹ Perry v. the United Kingdom, 63737/00, 17.10.2003.

⁶² Peck v. the United Kingdom, 44647/98, 28.01.2003.

ğini ileri sürmüştür. Mahkeme, suçları izleme ve engelleme konusunda kamera sisteminin önemli bir rol oynadığını kabul etmiş, kaydedilen görüntülerin yayınlaması konusunda da yetkili makamlara bir takdir hakkı tanınması gerektiğini belirtmiştir. Ancak kaydedilen görüntülerin başvuruçunun yüzü kapatılmadan yayınlanmış olmasını oran-tısız ve haksız bir müdahale olarak görmüş ve 8. maddenin ihlal edildiği sonucuna varmıştır.

c. Tıbbi Verilerin Saklanması ve Açıklanması

108 sayılı Sözleşme tıbbi verileri hassas veri olarak kabul etmiş ve bu verilerin ancak iç hukukta gerekli güvencelerin sağlanması koşuluyla işlenmesine izin vermiştir. Bakanlar Komitesi de 1997 yılında yayınlamış olduğu Tıbbi Verilerin Korunmasına İlişkin Tavsiye Kararı'nda, ancak iç hukukun gerekli güvenceleri sağlaması durumunda tıbbi verilerin toplanmasına ve işlenmesine izin verilebileceğini belirtmiştir (m. 3).

Söz konusu tavsiye kararında tıbbi veri kavramına açıklık getirilmiştir. Buna göre "tıbbi veri" kavramı, bireyin sağlığıyla ilgili olan bütün kişisel verileri ifade etmektedir. Tıbbi veri kavramı ayrıca genetik verilerle açık ve yakın bağlantısı olan verileri de ifade etmektedir (m. 1).

Avrupa Konseyi'nin tıbbi veriler açısından koruma sağlayan diğer bir düzenlemesi de "Biyoloji ve Tıbbin Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi"nin 10. maddesinde yer almaktadır. Madde'ye göre, herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Ancak, bireylerin bilgilendirilmeme istekleri de dikkate alınacaktır.⁶³ Genetik veriler de bu çerçevede kabul edilmektedir. Kendi geleceğini "ümitsiz" gördüğü bir vakada kişinin genetik veriler de dahil olmak üzere bilgi-

⁶³ Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, 4.IV.1997, European Treaty Series-No.164.

lenme hakkını kullanmamak hususunda irade beyanında bulunması mümkündür.⁶⁴

Avrupa İnsan Hakları Mahkemesi de tıbbi verilerin korunmasına özel bir önem vermiştir. Mahkeme'nin bu konuyu ele aldığı davalar içinde en önemlilerinden biri Z v. Finlandiya davasıdır.⁶⁵ Bu davaya konu olan olayda, hem başvuru hem de boşanmış olduğu eşi HIV virüsü taşımaktadır. Başvurucunun eski eşine karşı hem tecavüz suçundan hem de kasıtlı olarak HIV virüsü bulaştırmak suçundan dava açılmıştır. Bu davada, delil olarak kullanmak amacıyla, başvuru kişinin sağlık durumuna ilişkin doktorlarından bilgi istenmiş, hastaneden temin edilen tıbbi kayıtlar soruşturma dosyasına konulmuştur. Temyiz mahkemesinin vermiş olduğu kararda da başvuru kişinin kimliğine ve sağlık durumuna ilişkin bilgilere yer verilmiş, ancak davaya ilişkin dokümanların on yıl geçmeden açıklanması yasaklanmıştır.

Avrupa İnsan Hakları Mahkemesi bu davaya ilişkin vermiş olduğu kararda, öncelikle 108 sayılı Sözleşme ile Avrupa Konseyi Bakanlar Komitesi tarafından 1989 yılında kabul edilmiş olan "*Sağlık Hizmetlerinde ve Sosyal Alanlarda HIV Virüsüne İlişkin Etik Konular Hakkında Tavsiye Kararı*"nda,⁶⁶ Konsey üyesi devletlerden tıbbi verilerin gizliliğine saygı göstermelerinin istendiğini hatırlatmıştır. Mahkemeye göre, bir kişinin HIV virüsü taşıdığına ilişkin verilerin gizliliğinin korunması ise özellikle önem taşımaktadır. Çünkü bu tür bir verinin açıklanması onun özel ve aile yaşamını, iş ve sosyal ilişkilerini ciddi bir şekilde etkileyebilir. Bu bilgilerin açıklanabileceği kaygısını taşıyan bir kişi teşhis ve tedaviden kaçınabilir. Bu da bulaşıcı hastalıkların engellenmesi için toplumun gösterdiği çabalara zarar verebilir. Bu nedenledir ki, müdahalenin izlenen meşru amaçla orantılı olup olmadığına karar verirken, bu tür bilgilerin gizliliğinin korunmasına öncelik verilmelidir. Yapılan müdahale, önemli bir kamu yararı söz konusu olmadığı sürece, Sözleşme'nin 8. maddesine uygun olamaz. Ancak Mahkeme aynı zamanda, suçların soruşturulması ve cezalandırılması ile yargılama-

⁶⁴ Tuğrul Katoğlu, "Türk Hukukunun Bir Parçası Olarak Avrupa Konseyi İnsan Hakları ve Biyotıp Sözleşmesi", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 55, S. 1, 2006, s.177.

⁶⁵ Z v. Finland, 22009/93, 25.02.1997.

⁶⁶ Recommendation N.R. (89) 14 on the Ethical Issues of HIV Infection in the Health Care and Social Settings (24.10.1989).

nın açık olmasının sağlayacağı yararın, bir hastanın ve toplumun tıbbi verilerin korunmasından sağlayacağı yarardan daha fazla olabileceğini kabul etmektedir.

Mahkeme ortaya koyduğu bu görüşler doğrultusunda, başvuru-
cunun doktorlarından bilgi istenmiş olmasının ve başvurucunun tıbbi
kayıtlarının soruşturma dosyasına konulmasının izlenen meşru amaç-
la orantılı olduğunu açıklamış ve bu açılardan Sözleşme'ye bir aykırılık
görmemiştir. Ancak, Helsinki Temyiz Mahkemesi'nin vermiş olduğu
kararda başvurucunun kimliğine ve tıbbi durumuna ilişkin bilgilere
açıkça yer verilmiş olmasının ve dava dosyasında yer alan bilgilerin
10 yıl sonra kamuya açık hale gelmesine izin verilmesinin, başvuru-
cunun özel ve aile yaşamına saygı hakkına yönelik orantısız bir müdahale
oluşturduğunu belirtmiştir.

Mahkeme'nin tıbbi verilerin gizliliği konusunu ele aldığı diğer bir
dava da M.S. v İsveç davasıdır.⁶⁷ Bu davada başvurucu işyerinde ya-
şadığı bir kaza sonucunda çok ağır bel ağrıları olduğu gerekçesiyle
tazminat davası açmıştır. Sosyal Sigortalar Kurumu başvurucunun ted-
davi görmüş olduğu klinikten başvurucunun tıbbi kayıtlarını istemiştir.
Kliniğin gönderdiği raporda, başvurucunun bel ağrılarının kazadan
önce geçirmiş olduğu bir rahatsızlıktan kaynaklandığı ve bu rahatsızlıktan
dolayı kürtaj olmak zorunda kaldığı açıklanmıştır. Başvuru-
cunun, tıbbi kayıtlarının klinik tarafından Sosyal Sigortalar Kurumu'na
gönderilmiş olmasının tıbbi verilerin gizliliğine yönelik bir müdahale
oluşturduğunu ileri sürmüştür.

Mahkeme söz konusu müdahalenin yasaya uygun olarak yapıldığı
ve meşru bir amacının olduğu kanaatine varmıştır. Mahkemeye göre,
tıbbi kayıtların gönderilmesinin nedeni, iş kazası yüzünden tazminat
ödenmesinin koşullarının oluşup oluşmadığı sorununa açıklık
getirmektir. Rahatsızlığın iş kazasından kaynaklandığının saptanması
durumunda kamusal kaynaklar kullanılarak tazminat ödenecektir.
Burada ülkenin ekonomik refahının korunması amacı gözetilmiştir. Bu
kayıtlar olmaksızın Sosyal Sigortalar Kurumu'nun, başvurucunun tazminat
talebinin haklı olup olmadığına karar vermesi çok zor olacaktır.
Kayıtların gönderilmesi için bağlantılı ve yeterli nedenler mevcuttur.

⁶⁷ M. S. v. Sweden, 20837/92, 27.08.1997.

Alınan önlem, izlenen meşru amaç ile orantılıdır. Bu nedenle özel yaşam hakkının ihlali söz konusu değildir.

Mahkeme'nin hem Z v. Finlandiya hem de M.S. v. İsveç kararında kullandığı test, gereklilik ve orantılılık olmak üzere iki kısma ayrılmaktadır. İlk kısımda, verinin açıklanıp açıklanamayacağına ve açıklanması istenen verilerin 8(2). maddedeki istisnalar alanına girip girmediğine karar verilir. İkinci kısım da ise, yalnızca ihtiyaç duyulan verilerin açıklanmasına olanak tanınır. Diğer bir ifadeyle, yalnızca çok az miktardaki verinin açıklanması da yeterli olabilir.⁶⁸

Mahkeme son yıllarda vermiş olduğu I v. Finlandiya kararında da⁶⁹ tıbbi verilerin gizliliği konusunu ele almıştır. Başvurucu bir devlet hastanesinde hemşire olarak çalışmaktadır. Aynı hastanede yaptığı tetkiklerde HIV pozitif olduğu ortaya çıkmıştır. Başvurucu, hastalığına ilişkin tıbbi bilgilerin yer aldığı kayıtlara, ilgili bölümde çalışan personel dışında, hastanede çalışan diğer personelin de rahatlıkla ulaşabildiğinden şikayetçi olmuştur. Bu şikayet üzerine hastane gerekli önlemleri almış, hastanın sahte bir isim ve sosyal güvenlik numarasıyla kaydı yapılmış ayrıca tedaviyi yapan personel dışında diğer personelin bu kayıtlara ulaşması yasaklanmıştır.

Mahkeme, tıbbi verilerin gizliliğine saygı gösterilmesinin Sözleşme'ye taraf devletlerin hukuk sistemlerinde güvence altına alınması gereken temel bir ilke olduğunu belirtmiş ve özellikle de bu ilkenin hastaların HIV pozitif olduklarına ilişkin bilgilerin gizliliğinin korunması açısından geçerli olduğunu açıklamıştır. Söz konusu hastane, fiillerinden devletin sorumlu olduğu bir devlet hastanesidir. Hastane yetkilileri, tıbbi kayıtların gizliliğinin hastane personeline karşı da korunması konusunda gerekli önlemleri ancak yapılan şikayet üzerine almıştır. Bu önlemlerin alınmasında başvurucu açısından geç kalmıştır. Ayrıca iç hukukta, başvurusunun kişisel verilerinin hukuken uygun olmayan bir şekilde açıklanmış olmasından dolayı gördüğü zararın tazminine ilişkin sunulan olanaklar, başvurusunun özel yaşam hakkının korunması açısından yeterli değildir. Bu nedenle, başvurusunun özel yaşam hakkına saygının güvence altına alınabilmesi

⁶⁸ Jose Miola, "Owning Information-Anonymity, Confidentiality and Human Rights", *Clinical Ethics*, Vol. 3, No.3, 2008, s.119.

⁶⁹ I. v. Finland, 20511/03, 17.07.2008.

için Sözleşme'nin 8. maddesinin yüklemiş olduğu pozitif yükümlülüğü devlet yerine getirmemiştir.

Mahkeme'nin I v. Finlandiya kararı kilometre taşı niteliğinde bir karar olarak değerlendirilmektedir. Çünkü yalnızca yasal düzenlemelerin yapılmasını yeterli bulmamış, kişisel verilerin korunmasında, en azından resmi görevlilerin açısından belirsizliğe yer verilmemesi için, alınması gereken güvenlik önlemlerinin altını çizmiştir.⁷⁰ Hastalara ait tıbbi verilerin hastane personeli tarafından dışarıya sızdırıldığına ve hatta satıldığına ilişkin birçok vakanın olduğu⁷¹ dikkate alındığında bu kararın önemi daha da artmaktadır.

Mahkeme I v. Finlandiya kararından kısa bir süre sonra verdiği S. ve Marper v. Birleşik Krallık kararında⁷² ise parmak izi, DNA profilleri ve hücre örneklerinin saklanması sorununu ele almıştır. Başvurucu S. 11 yaşındayken hırsızlığa teşebbüs suçundan yakalanmış ve hakkında yürütülen ceza davasının sonucunda beraat etmiştir. Başvurucu Marper ise partnerini taciz suçundan yakalanmış ancak daha sonra aralarında uzlaşma sağladıkları için dava düşmüştür. Başvurucular, yakalandıkları dönemde kendilerinden alınmış olan parmak izlerinin, hücre örneklerinin ve DNA profillerinin hala ulusal veritabanında saklanıyor olmasından şikayetçi olmuşlar ve bu verilerin silinmesini istemişlerdir. Ancak yürürlükteki yasa bu verilerin saklanmasına izin verdiği için talepleri reddedilmiştir. Mahkeme, bu verilerin 108 sayılı Sözleşme'ye göre kişisel veri olarak kabul edileceğini belirtmiş ve özellikle hücre örnekleri ile DNA profillerinin çok hassas nitelikte veri olduğunu açıklamıştır. Mahkeme'ye göre, beraat eden ya da haklarındaki ceza davası düşen kişilere ait parmak izi, hücre örneği ve DNA profillerinin saklanması durumunda, yarışan kamusal ve özel menfaatler arasında denge bozulur ve devlete tanınmış olan takdir hakkının sınırları aşılır. Söz konusu verilerin saklanması başvuruçuların özel yaşamına saygı hakkına yönelik orantısız bir müdahaledir ve demokratik bir toplumda gerekli bir müdahale olarak değerlendirile-

⁷⁰ Jari Raman, "European Court of Human Rights: Failure to Take Effective Information Security Measures to Protect Sensitive Personal Data Violates Right to Privacy- I. v. Finland, no.20511/03, 17 July 2008", *Computer Law & Security Report* 24, 2008, s.562.

⁷¹ Bkz. Charles J. Sykes, *The End of Privacy*, St. Martin's Press, 1999, s. 106.

⁷² S. and Marper v. the United Kingdom, 30562/04 and 30566/04, 04.12.2008.

mez. Mahkeme bu gerekçelere dayanarak 8. maddenin ihlal edildiğine karar vermiştir.

Mahkeme'nin vermiş olduğu bu karar oldukça önemli bir karardır. Çünkü Avrupa Konseyi üyesi 47 ülke arasında Birleşik Krallık, be-
raat eden ya da haklarındaki ceza davası düşen kişilere ait DNA profillerinin ve hücre örneklerinin sistematik ve süresiz bir şekilde tutulmasına izin veren tek ülkedir. Bu ülkede 5 milyondan fazla kişinin DNA profili saklanmaktadır. Bunun yaklaşık 1 milyonu herhangi bir suçtan dolayı mahkum olmamış kişilere aittir. Yarım milyonu ise yetişkin olmayan kişilere aittir.⁷³ Yaşları 10 ile 17 arasında değişen yaklaşık 300 çocuğa ait DNA profilleri her gün Birleşik Krallık ulusal veritabanına eklenmektedir.⁷⁴ Bu rakamlar göz önüne alındığında Avrupa İnsan Hakları Mahkemesi'nin vermiş olduğu kararın önemi daha iyi anlaşılmaktadır.

V. SONUÇ

Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme, kişisel verilerin korunması alanında Avrupa'da atılan ilk adımdır. 1980 yılında Ekonomik İşbirliği ve Kalkınma Örgütü tarafından yayınlanan "*Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler*" kişisel verilerin korunması konusunda dünya genelinde hazırlanan ilk belge olmakla beraber, bu belge tavsiye niteliğinde olan ve bağlayıcı özelliği olmayan bir belgedir. 108 sayılı Avrupa Konseyi Sözleşmesi bu alanda kabul edilmiş olan ilk bağlayıcı belge olması açısından da önem taşımaktadır.

108 sayılı Sözleşme kişisel verilerin korunması açısından önemli güvenceler içermektedir. Kişisel verilerin dürüstlük kuralına ve hukuka uygun olarak işlenmesi zorunluluğunu getirmesi, kişisel verilerin ancak belli ve meşru amaçlar için kaydedilmesine izin vermesi ve bu amaçlarla bağdaşmayan bir şekilde kullanılmasını yasaklaması, verilerin Sözleşme'deki güvencelere aykırı bir şekilde işlenmesi durumunda

⁷³ George J. Annas, "Protecting Privacy and the Public-Limits on Police Use of Bio-identifiers in Europe", *The New England Journal of Medicine*, July 9, 2009, s.199.

⁷⁴ James Slack, "300 Children a Day Added to DNA Database: 400.000 under-15s on Big Brother Roll", *The Daily Mail*, 12 Ağustos 2009.

verileri düzeltebilme, sildirebilme ya da hukuksal yollara başvurabilme hakkını veri sahibine tanımış olması Sözleşme'nin sağladığı önemli güvencelerdir.

108 sayılı Sözleşme sağlamış olduğu bu güvencelerle önemli bir belge olma özelliği taşımaktadır. Ancak içerdiği bazı eksiklikler kişisel verilerin korunması konusunda Sözleşme'nin etkili olmasını engellemektedir. Yalnızca otomatik yollarla işlenen kişisel veriler açısından güvenceler sağlaması Sözleşme'nin uygulama alanını daraltmaktadır.

Sözleşme'deki ilkelerin uygulanmasını denetleyecek bir denetim organının oluşturulmaması da önemli bir eksikliktir. 2004 yılında yürürlüğe giren Ek Protokol, Sözleşme'ye taraf olan devletlerin kendi iç hukuklarında bir kontrol makamı oluşturmalarını öngörmektedir. Her taraf devletin kendi iç hukukunda kontrol makamı oluşturması önemli olmakla beraber, Sözleşme'nin uygulanmasını izlemekle görevli bir Sözleşme organının oluşturulması Sözleşme hükümlerinin uygulanması açısından önemli bir güvence sağlayacaktır.

Kişisel verilerin korunması açısından Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesindeki düzenleme ile Avrupa İnsan Hakları Mahkemesi'nin vermiş olduğu kararlar da kişisel verilerin korunması açısından önem taşımaktadır. Mahkeme'nin bu alandaki içtihadı çok yavaş gelişmiş olmakla beraber, kişisel verilerin korunmasına büyük ölçüde katkıda bulunacak çok önemli kararlar vermiştir.