



Avrupa İnsan Hakları Mahkemesi Kararları'nın “Kişisel Verilerin Korunması”na Katkısı*

Contribution of European Court of Human Rights Judgements' to “The Protection of Personal Data”

Eren Solmaz¹

Öz

Bu çalışma, Avrupa İnsan Hakları Mahkemesi kararlarının kişisel verilerin korunması hakkına sağladığı katkıları aktarmak amacıyla hazırlanmıştır.

Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasına ilişkin doğrudan bir hüküm olmamasına rağmen AİHM, Sözleşme'nin 8. maddesi kapsamında yaptığı değerlendirmeler sonucunda kişisel verilerin korunmasına bir hukuki değer atfetmiştir.

Nitekim AİHM kararları, kişisel verilerin korunmasının hukuken korunan bir “hak” olarak tanımlanması bakımından Avrupa Birliği Hukukuna ve üye ülkelerin iç hukukundaki yasal düzenlemelere önemli katkılar sunmuştur.

Anahtar Kelimeler

Kişisel Verilerin Korunması • Avrupa İnsan Hakları Mahkemesi • Özel ve Aile Hayatına Saygı Hakkı

Abstract

This study was prepared in order to convey the contribution of the European Court of Human Rights judgements' to the protection of personal data.

Although there is no direct provision in the European Convention on Human Rights for the protection of personal data, the ECHR has cited a legal value for the protection of personal data as a result of its assessments under Article 8 of the Convention.

As a matter of fact, the ECHR judgments have made significant contributions to the European Union Law and to the legal regulations in the internal law of the member states in order to define the protection of personal data as a legally protected “right”.

Keywords

Protection of Personal Data • European Court of Human Rights • Right to Respect for Private and Family Life

* Makale hakem incelemesinden geçirilmiştir.

¹ **Sorumlu Yazar:** Eren Solmaz (Öğretim Görevlisi), İstanbul Üniversitesi, Hukuk Fakültesi Adalet Meslek Yüksek Okulu, İstanbul, Türkiye. E-posta: eren.solmaz@istanbul.edu.tr ORCID: 0000-0002-1956-3482

Atf: Solmaz E, “Avrupa İnsan Hakları Mahkemesi Kararları'nın “Kişisel Verilerin Korunması”na Katkısı” (2019) 18(1) İdare Hukuku ve İlimleri Dergisi 61. <https://doi.org/10.26650/ihid.644402>

GİRİŞ

“Kişisel verilerin korunması” (*protection of personal data*) bir hak olarak, hukuk dünyasında önemli bir yere ve gündeme sahiptir. Ancak kanunlaşması ve kurumlaşması ülkeden ülkeye değişerek, aşamalı bir şekilde gerçekleşmektedir. Ülkelerin iç hukukunda, kişisel verilerin korunmasının, bir hak olarak kanunlaşma süreci her ne kadar birbirinden ayrı ve Türkiye gibi bazı ülkelerde yeni sayılsa da, hakkın varlığı uluslararası hukuk metinlerinde temellendirilmiştir. OECD’nin 1980 tarihli Rehber İlkeleri¹, Avrupa Konseyi 108 Sayılı Kişisel Verilerin Korunması Sözleşmesi² ve BM Evrensel Bildirgesi’nde Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler³, öncül düzenlemeler olarak kabul edilmektedir⁴.

Kişisel verilerin korunması hususu günümüzde, çeşitli nedenlerle daha hassas bir konuma kavuşmuştur. Ekonominin küreselleşmesi, bilim ve teknolojinin gelişmesi⁵, ülkelerin birbiriyle entegre olması, terörizmin artış göstermesi⁶ vb. sebeplerle kişisel verilere daha çok ihtiyaç duyulması aynı zamanda onun korunmasını gerekli kılmıştır. Bu nedenle, kişisel verilerin korunması devlete bir sorumluluk yüklemiştir⁷. Kişisel verilerin işlenmesine⁸ (processing) ilişkin düzenlemelerin kanun koyucu tarafından güvence altına alınması, beraberinde bu görevlerin yerine getirilmesini sağlayacak bir teşkilatı da gerekli kılmaktadır⁹.

Avrupa Birliği’nin 95/46 sayılı Veri Koruma Direktifi¹⁰ ile kişisel verilerin korunması Avrupa Birliği ülkeleri bakımından yasal bir temele kavuşmuştur. Yakın zamanda ihdas edilen 2016/679 sayılı Regülasyon¹¹ ile de kişisel verilerin korunmasına ilişkin ortaya çıkan ihtiyaçları karşılamak üzere daha kapsamlı düzenleme yapılmıştır.

Diğer taraftan, AİHS’te kişisel verilerin korunmasına dair doğrudan bir hüküm bulunmamakla birlikte, AİHM kararlarında konu AİHS’in 8. maddesi kapsamında ele alınmaktadır. AİHM kararları, kişisel verilerin korunması hakkının hukuki alt yapısına

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

² Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981.

³ United Nations, Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly Resolution 45/95 of 14 December 1990.

⁴ Lee A. Bygrave, **Data Privacy Law**, Oxford, Oxford University Press, 2014, s. 31 vd.

⁵ Bygrave, **Data Privacy Law**, s. 9.

⁶ Cemil Kaya, “Avrupa Toplulukları Adalet Divanının PNR Kararının Tahlihi”, **Prof. Dr. Hüseyin Hatemi’ye Armağan**, C. II, İstanbul, Vedat Kitapçılık, 2009, s. 2027-2039, s. 2033.

⁷ Nitekim ülkemizde 2016 yılında, 6698 Sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir.

⁸ 6698 sayılı Kanun’un 3(e) Maddesi, Bkz. “**Kişisel verilerin işlenmesi**: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi, ... ifade eder.”

⁹ Nitekim ülkemizde ve Avrupa ülkelerinde bu amaçla “Kişisel Verileri Koruma Otoriteleri” kurulmuştur.

¹⁰ *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.*

¹¹ *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, Official Journal of the European Union, 04.05.2016, L 119/1-88.

önemli katkı sağlamaktadır. AİHM'in, ilk başlardan itibaren, kişisel verilerin korunmasına ilişkin konularda, geliştirdiği içtihatlar ulusal ve uluslararası hukuki metinlerinin yorumlanmasında dikkate alınmakla birlikte birkaç açıdan önem arz etmektedir¹². Sırf bu açıdan bile kişisel verilere ilişkin AİHM kararlarının önemi ortadadır.

İşte bu çalışma ile AİHM kararlarının kişisel verilerin korunmasına etkisi incelenecektir. Bu amaçla önce AİHM'in kişisel verilerin korunması hususunda geçmişten günümüze önüne gelen davalarda hangi ölçütleri esas alarak karar verdiği ele alınacaktır. Ardından AİHM kararlarının kişisel verilerin korunmasının bir "hak" olarak hukuk âleminde yer edinmesi ve AB üyesi ülkelerin mevzuatına girmesi değerlendirilecektir. Son olarak, AİHM'in esas aldığı ölçütlerin yeterliliği ve isabetli olup olmadığı tartışılarak bu doğrultuda önerilerde bulunulacaktır.

AİHM'İN KİŞİSEL VERİLERİN KORUNMASI KONUSUNDAKİ KARARLARI BAKIMINDAN AİHS MADDE 8'İN ÖNEMİ

Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesi şu şekildedir: "*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*"

AİHS'in 8. Maddesi, özel hayatın ve aile hayatının korunmasını çeşitli yönleri ile ele almakla birlikte kişisel verilerin korunması konusunu da kapsayacak hukuki etkiye sahiptir. Avrupa Birliği'nin 95/46 sayılı Veri Koruma Direktifi ve kişisel verilerin korunmasına ilişkin diğer AB mevzuatına bakıldığında (2016/679 sayılı Regülasyon) AİHS'in 8. maddesini ve AİHM'in yaklaşımını takip ettiği söylenebilir¹³. Her ne kadar Sözleşme'nin kabul edildiği 1950 yılında kişisel verilerin korunmasına ilişkin bir tartışma ortaya çıkmamış ve buna ilişkin bir düzenlemeye ihtiyaç duyulmamışsa da, bu konu hukuki bir sorun haline geldikten sonra, AİHS'in 8. maddesi AİHM'in "özel alan"a ilişkin değerlendirmeleri¹⁴ kapsamında kişisel verilerin ihlali uyumsuzluklarını da kapsayan bir hüküm olarak ele alınmıştır.

AİHS'in 8. maddesi ile devlete, kişisel verilerin korunması açısından iki tür yükümlülük yüklenmektedir¹⁵: Birincisi, devletin negatif yükümlülüğüdür. Yani dev-

¹² Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara, Turhan Kitabevi, 2010, s. 137.

¹³ María Verónica Pérez Asinari, Legal Constraints for The Protection of Privacy and Personal Data in Electronic Evidence Handling, **International Review of Law, Computers & Technology**, 18:2, 2004, s. 231-250, s. 241, <http://www.tandfonline.com/doi/pdf/10.1080/1360086042000223526>.

¹⁴ Küzeci, s. 138.

¹⁵ Feyyaz Gölcüklü / A. Şeref Gözübüyük, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, 9.b., Ankara, Turhan Kitabevi, 2011, s. 330 vd.

letin, kişilerin kişisel verilerinin korunması amacıyla belirli eylemleri yapmaktan kaçınması, AİHS'e aykırı olarak kişisel verilerin işlenmesine müdahale etmekten kaçınmasıdır. İkincisi ise devletin pozitif yükümlülüğüdür. Kişisel verilerin korunması hakkının ihlal edilmemesi için gerekli ve yeterli önlemlerin alınması, kişisel verilerin gizliliğinin korunması için ilke ve kurallar koyulması, tedbirler alınması ve gerekli güvencelerin sağlanmasıdır.

AİHS'in 8. maddesinin ilk fıkrası özel hayata ilişkin temel hakkı düzenlemektedir. Ancak maddede korunan hakların tanımı yapılmamaktadır. Keza kişisel verilerin korunması AİHS'te bağımsız bir temel hak ve özgürlük olarak yer almamaktadır¹⁶. Ancak AİHM özellikle 1980'li yılların ortalarından beri ve gittikçe artan bir yoğunlukta, kişisel verilerin korunmasını, AİHS'in sağladığı güvenceler kapsamında değerlendirmiştir¹⁷. Nitekim AİHM kişisel verilerin korunmasını AİHS'in 8. maddesi kapsamında görmüştür¹⁸. Aynı zamanda AİHM, bu madde sayesinde, kişisel verilerin ihlali iddiasıyla önüne gelen somut uyuşmazlıklarda nasıl bir metod izleyeceğini ve hangi ölçütleri esas alacağını belirlemiştir. Fakat aşağıda görüleceği üzere, dikkate değer husus ise, gerek Avrupa Birliği'nin 95/46 sayılı Veri Koruma Direktifinin yürürlüğe girmesinden sonra gerekse 2016/679 sayılı Regülasyon'un düzenlenmesinden sonra dahi AİHM'in, kişisel verilerin korunması hakkına ilişkin davalarda AİHS'in 8. maddesi kapsamında yargılama yaparak karar verdiğidir.

AİHM, AİHS'in 8. maddesi çerçevesinde kişisel verilerin korunmasına ilişkin uyuşmazlıkları iki açıdan değerlendirmektedir. Birincisi, 8. maddenin ilk fıkrasından yola çıkarak ortaya koyduğu “özel alan” yaklaşımıdır. Bu kapsamda başvuru konusu olayı “özel yaşam”, “aile yaşamı”, “konut” veya “haberleşme” alanlarına yapılan müdahaleler doğrultusunda değerlendirmektedir¹⁹. İkincisi ise, 8. maddenin ikinci fıkrası kapsamında birinci fıkrada belirlenen alana yapılan müdahaledir. Başka bir ifadeyle ikinci fıkra birinci fıkrada düzenlenen özel yaşama saygı hakkının sınırlarını belirlemektedir²⁰. AİHM de buradan yola çıkarak, öncelikle yapılan müdahalenin meşruluk kazanıp kazanmadığına bakmaktadır²¹.

Bu bağlamda, yapılan müdahale maddede belirtilen “ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın

¹⁶ Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul, Beta Basım, 2008, s. 37; Saadet Yüksel, *Özel Yaşamın Bir parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale*, İstanbul, Beta Basım, 2012, s. 101.

¹⁷ Lee A. Bygrave, Where have all the judges gone? Reflections on judicial involvement in developing data protection law”, *Privacy Law and Policy Reporter*, Y. 2000, C. 7, s. 4, http://folk.uio.no/lee/oldpage/articles/Judges_role.pdf.

¹⁸ *Klass ve diğerleri v. Almanya Davası*, 5029/71, T. 06.09.1978 AİHM'in kişisel verilerin korunması konusunda vermiş olduğu ilk önemli karardır. Bu kararda her ne kadar Almanya devletinin davranışlarının AİHS'in 8. maddesini ihlal etmediğine ve iç hukukun yeterli güvenceyi sağladığına karar verilmiş olsa da, konunun AİHM'in inceleme alanına alınması önem arz etmektedir.

¹⁹ Kütüceci, s. 139.

²⁰ Kütüceci, s. 142.

²¹ B. No: 9063/80 T. 24.11.1986, *Gillow v. Birleşik Krallık*, para. 53, 54.

veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması" amaçlarına yönelik olması, "gerekli olan ölçüde" ve "yasayla öngörülmüş" olması halinde meşru kabul edilmektedir. Nihayetinde AİHM, AİHS'in 8. maddesinin içeriğinden hareketle bir ölçüt oluşturmak suretiyle kişisel verilerin korunması hakkına yapılan müdahalelerde hukuka aykırılık olup olmadığını tespit etmektedir. Dolayısıyla çalışmanın devamında, buradan hareketle, bu ölçütler kapsamında bir inceleme yapılmaya çalışılacaktır.

AİHS 8/1 MADDESİ ÇERÇEVESİNDE "ÖZEL ALAN" ÖLÇÜTÜNÜN KİŞİSEL VERİLERİN KORUNMASINA KATKISI

AİHM öncelikle önüne gelen somut olayda ihlal edildiği öne sürülen hakkın AİHS'in 8. maddesinde sayılan hususlardan birine girip girmediğini tespit etmektedir. Bu hususlar yukarıda da ifade edildiği gibi özel yaşam, aile yaşamı, konut ve haberleşmedir. Nitekim AİHM bireysel özerkliği (personal autonomy) ve bilgilerin akibetini belirleme hakkını 8. madde ile getirilen güvencelerin yorumlanmasında önemli bir temel ilke olarak görmüştür²². AİHM bu alanlara yapılan müdahalelere ilişkin birçok inceleme yapmış ve içtihat geliştirmiştir.

AİHM'e göre, özel hayat kavramının kapsamlı bir tanımını yapmanın ne mümkün ne de gerekli olduğu düşünülmektedir. Ancak bu kavramı bireyin kendi özel hayatını istediği gibi yaşayabileceği bir iç alan ile kısıtlamak ve bu alandan söz konusu alanın içinde olmayan dış dünyayı olduğu gibi hariç tutmak aşırı kısıtlayıcı sayılmaktadır²³. Nitekim AİHM, özel yaşamı kişinin mahrem alanı ile sınırlı görmemekte ve bu bağlamda kişinin ev telefonunun yanında iş telefonunun dinlenmesini de 8. maddenin güvencesi kapsamında kabul etmektedir²⁴. AİHM, kişilerin iş hayatlarını özel hayat kapsamında gördüğünü açıkça ifade etmektedir²⁵. Ayrıca kişilerin internet aracılığıyla kurdukları iletişimin ve e-postalarının izlenmesi ya da içeriklerinin saptanması da bu kapsamda değerlendirilmektedir²⁶. Diğer taraftan AİHM'e göre, kamusal alanların kişilerin görüntülerini alan araçlarla izlenmesi ve bu görüntülerin kayıt edilmesi durumunda özel hayata müdahale söz konusu olmamaktadır. Ancak verilerin kaydedilmesi ve bu kaydın sistemli ya da kalıcı olarak yapılması durumunda aynı şeyi söylemek mümkün değildir²⁷.

Yukarıda da bahsedildiği üzere AİHM kişisel verilerin korunmasına ilişkin ilk ve önemli kararını *Klass v. Almanya* başvurusunda vermiştir. AİHM bu başvuruda, bir kimsenin telefonunun gizli dinlemeye konu olmasını özel yaşam kapsamında ele almıştır. Böylece AİHM, sonraki zamanlarda, çeşitli nedenlerle önüne gelen

²² B. No: 2346/02, T. 29.07.2002, *Pretty v. Birleşik Krallık*, para. 61.

²³ B. No: 13710/88, T. 16.12.1992, *Niemietz v. Almanya* para. 29.

²⁴ B. No: 20605/92, T. 25.06.1997, *Halford v. Birleşik Krallık*.

²⁵ B. No: 13710/88, T. 16.12.1992, *Niemietz v. Almanya*.

²⁶ B. No: 62617/00, T. 03.07.2007, *Copland v. Birleşik Krallık*.

²⁷ B. No: 44647/98, T.28.04. 2003, *Peck v. Birleşik Krallık*.

başvuruları kişisel verilerin korunması hakkı çerçevesinde değerlendirerek karar vermiştir. 1987 tarihli *Leander v. İsviçre* başvurusunda²⁸ “*toplanan verilerin toplanma amacı dışında kullanılması*”nı, 1989 tarihli *Gaskin v. Birleşik Krallık* başvurusunda²⁹ “*kişisel verilere erişim hakkı*”nı, 1994 tarihli *Murray v. Birleşik Krallık* başvurusunda³⁰ “*Emniyet güçleri tarafından parmak izi ve fotoğraf alınması*”nı, 1997 tarihli *M.S. v. İsveç* başvurusunda³¹ “*sağlık verilerinin gizliliği*”ni, 2000 tarihli *Rotaru v. Romanya* başvurusunda³² “*bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi*”ni, 2001 tarihli *P.G. ve J.H. v. Birleşik Krallık* başvurusunda³³ “*telefon görüşmelerine ilişkin kayıtları izleme*”yi, 2008 tarihli *S. ve Marper v. Birleşik Krallık* başvurusunda³⁴ “*kişisel verilerin gerektiğinden uzun süre tutulması*”nı kişisel verilerin korunması hakkı kapsamında ele almıştır.

Nitekim AİHM 2017 tarihli *Surikov v. Ukrayna* başvurusunda, başvurusunun *sağlık verilerinin daha önce görev yaptığı askeri birlik tarafından çalıştığı şirkete aktarılması sonucunda şirket tarafından mühendislik kadrosuna terfiinin yapılmaması*”nı AİHS’in 8. maddesi kapsamında ele alarak başvurusunun kişisel verilerinin korunması hakkının ihlal edildiğine karar vermiştir³⁵.

Bu ve benzeri kararlara kronolojik açıdan bakılınca AİHM’in kişisel verilerin güvence altına alınmasını, AİHS’in 8. maddesinden beslenmekle birlikte, korunması gereken müstakil bir hak olarak kabul ettiği ifade edilebilir. Böylece AİHM bu ve benzeri uyuşmazlıklarla önüne gelen başvurular sayesinde kişisel verilerin korunmasına hukuki bir değer atfederek bir hak olarak yasal düzenlemelere konu olmasına önemli derecede katkı yapmıştır.

AİHS 8/2 MADDESİ ÇERÇEVESİNDE “MÜDAHALENİN MEŞRULUĞU”NU SAĞLAYAN HUSUSLAR

AİHS’in 8. maddesi özel hayata saygı hakkını güvence altına almakla birlikte bu hakka müdahaleye izin veren kriterleri de düzenlemektedir³⁶. 8. maddenin birinci fıkrası, özel hayata saygı hakkının varlığını ortaya koyarken ikinci fıkrası bu hakkın çerçevesini çizmekte, bu hakka yapılacak müdahalelerin meşruluk sınırını belirlemektedir³⁷.

²⁸ B. No: 9248/81, T. 26.03.1987, *Leander v. İsviçre*.

²⁹ B. No: 10454/83, T. 07.07.1989, *Gaskin v. Birleşik Krallık*.

³⁰ B. No: 14310/88, T. 28.10.1994, *Murray v. Birleşik Krallık*.

³¹ B. No: 20837/92, T. 27.08.1997, *M.S. v. İsveç*; Aynı yönde bkz: B. No: 22009/93, 25.02.1997, *Z.v. Finlandiya*.

³² B. No: 28341/95, T. 04.05.2000, *Rotaru v. Romanya*; Aynı yönde bkz: B. No: 27798/95, T. 16.02.2000, *Amann v. İsviçre*.

³³ B. No: 44787/98, T. 25.09.2001, *P.G. ve J.H. v. Birleşik Krallık*; Aynı yönde bkz: B. No: 8691/79, T. 02.08.1984, *Malone v. Birleşik Krallık*.

³⁴ B. No: 30562/04, T. 04.12.2008, *S. ve Marper v. Birleşik Krallık*.

³⁵ B. No: 42788/06, T. 26.01.2017, *Surikov v. Ukrayna*.

³⁶ Bygrave, *Data Privacy Law*, s.86.

³⁷ Gölcüklü/Gözübüyük, s. 330.

Buna göre öncelikle, müdahalenin yalnızca bir kamu otoritesi tarafından yapılabilceği ve bu müdahalenin ancak ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması amacıyla yönelik olabileceği ifade edilmektedir. Ayrıca müdahalenin demokratik bir toplumda gerekli olan ölçüde olması ve yasayla öngörülmüş olması koşulları aranmaktadır.

Maddenin lafzının -esasen- ortaya koyduğu şey; idare tarafından yapılan müdahalenin kanuna dayanarak, kamu düzeninin sağlanması ve/veya kamu yararı amacıyla ve ölçülülük ilkesi sınırlarında kalacak şekilde yapılmış olması sonucunda meşruluk zemini kazanacağı ve bir hak ihlaline yol açmayacak olmasıdır.

AİHS'in 8. maddesinde özel hayata saygı hakkına müdahaleyi haklı kılan meşru amaçlar, "ulusal güvenlik", "kamu güvenliği", "ülkenin ekonomik refahı", "düzenin korunması", "suç işlenmesinin önlenmesi", "sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması" hususlarına ilişkin olmakla birlikte oldukça geniş bir alanı kapsamaktadır³⁸. AİHM de önüne gelen başvurularda bu kriterleri esas almakta meşruluk sınırında değerlendirmektedir.

AİHM, AİHS tarafından güvence altına alınan diğer haklara ilişkin davalar dışında kişisel verilerin korunmasına ilişkin bazı kararlarında da "müdahalenin milli güvenlik ve/veya suçluluğun önlenmesi amacı"na yönelik olduğu³⁹, bazı kararlarında müdahalenin "başkalarının haklarının korunması" amacıyla yönelik olduğu⁴⁰, bazı kararlarında ise müdahalenin "demokratik toplum düzeninin gereklerine" yönelik olduğu⁴¹ tespitleriyle kararlar vermiştir. Ayrıca AİHM bu kararlarında, müdahalenin "yasal dayanağının olması"⁴² ve müdahalenin "demokratik bir toplumda gerekli olması" koşullarını da referans almıştır.

ÇEŞİTLİ EVRELER BAKIMINDAN KİŞİSEL VERİLERİN KORUNMASI GEREKLİLİĞİ VE AİHM YAKLAŞIMI

Kişisel verilerin korunmasını sağlamak, bu verilerin işlenmesi bağlamında birçok evreyi kapsamaktadır. Bunlar "kişisel verilere erişim", "kişisel verilerin toplanması", "kişisel verilerin saklanması ve kullanılması", "kişisel verilerin aktarılması", "kişisel verilerin ifşa edilmesi" ve "kişisel verilerin silinmesi/imhası" gibi aşamalıdır. Kişisel verilerin korunması hakkı bu aşamalardan herhangi birinde veya bir kaçında ihlale uğrayabilmektedir. Dolayısıyla bu aşamalara ilişkin bazı ilke ve kurallar konulması gereklilik arz etmektedir.

³⁸ Kütüceci, s. 142.

³⁹ P.G. ve J.H. v. Birleşik Krallık, para. 49; Leander v. İsviçre, para. 49; Murray v. Birleşik Krallık, para. 89.

⁴⁰ Pretty v. Birleşik Krallık, para. 69; Niemietz v. Almanya, para. 36; Z. v. Finlandiya, para. 76.

⁴¹ Klass v. Almanya.

⁴² B. No: 11801/85, T. 24.04.1990, Kruslin v. Fransa, para. 33; Aynı yönde bkz: Malone v. Birleşik Krallık.

Kaya, “...kişisel veriler; dürüstçe ve hukuka uygun olarak toplanmalı ve işlenmeli; belirli, açık ve meşru amaçlar için toplanmalı ve daha sonra da bu amaçlara aykırı şekilde kullanılmamalı; toplandıkları amaçlar ve daha sonraki işlenmeleri için elverişli, uygun ve aşırıya kaçmayacak şekilde olmalı; doğru, tam olmalı ve gerektiği durumlarda güncellenmeli ve toplandıkları ve işlendikleri amaçlar karşısında yanlış olan ve eksik olan verilerin silinmesi veya düzeltilmesi için gerekli tedbirler alınmalı; toplandıkları ve işlendikleri amaçlar için gereken süreyi aşmayacak bir süre boyunca ilgili kişilerin belirlenmesini sağlayacak bir şekilde muhafaza edilmelidir...” diyerek, esasında kişisel verilerin korunmasının ne kadar netameli ve hassas bir konu olduğunu vurgulamakta ve buna ilişkin ilkeleri belirlemektedir⁴³.

Nitekim AİHM de çeşitli kararlarında bu ve benzeri hususları göz önünde bulundurmak suretiyle, kişisel verilerin korunmasının hukuki rejimini belirlemektedir.

KİŞİSEL VERİLERE ERİŞİM

Kişilerin, haklarındaki kişisel verilere erişme/elde etme ve bu verileri kontrol etme hakkı mevcuttur⁴⁴. Bu, bilgi edinme hakkı çerçevesinde elde edilebilecek bir bilgi kategorisidir⁴⁵. Kişisel verilere erişme/elde etmeye yönelik hukuki metinlerde de, bir kimsenin başka bir kişi veya kurumun elinde bulunan kendisine ait kişisel verilere erişme hakkı kabul edilmiştir. Ancak bu hak, kanunda düzenleme yapılması koşuluyla; kamu güvenliğinin ve ülkenin ekonomik çıkarlarının korunması veya suç işleminin önlenmesi, ilgili kişinin ve başkalarının hak ve özgürlüklerinin korunması amaçlarıyla demokratik bir toplumda gereklilik arz ediyor olması halinde sınırlandırılabilir⁴⁶.

AB mevzuatında bu husus kapsamlı bir şekilde düzenlenmiştir. Avrupa Birliği’nin 95/46 sayılı Veri Koruma Direktifinin 12. maddesinde *ilgili kişinin kişisel verilerinin işlenmesine ilişkin veri denetçisinden bazı temel bilgileri sağlayabileceği* düzenlenmişti. Bu ve kişisel verilere erişime ilişkin diğer hususlar 2016/679 sayılı Regülasyon’un 13, 14 ve 15. maddelerinde daha kapsamlı bir şekilde düzenlenmiştir. Veri Koruma Direktifi’nin 13. maddesinde, kişisel veriye erişimin hangi hallerde sınırlandırılacağına ilişkin düzenlemeye karşılık, kişisel verilerin silinmesi hususu 2016/679 sayılı Regülasyon’un ‘unutulma hakkı’ başlıklı 17. maddesinde ayrıntılı olarak kaleme alınmıştır. AİHM kararlarında da bu hususlara dikkat edildiği görülmektedir. Nitekim AİHM kişinin kendisi hakkındaki bilgilere erişim hakkını, AİHS’in 8. maddesi kapsamında ele almış, Veri Koruma Direktifi ve 2016/679 sayılı Regülasyondaki düzenlemelerle aynı doğrultuda değerlendirmiştir.

⁴³ Cemil Kaya, *İdare Hukukunda Bilgi Edinme Hakkı*, Ankara, Seçkin Yayıncılık, 2005, s. 90-91.

⁴⁴ İlgili kişinin veriye erişme hakkı, makul aralıklarla ve aşırı gecikme veya harcamalara maruz kalmadan belli bilgileri veri işleme sorumlusundan alması olarak ifade edilebilir, Yüksel, s. 118.

⁴⁵ Kaya, *İdare Hukukunda Bilgi Edinme Hakkı*, s. 89.

⁴⁶ 95/46/AT sayılı Veri Koruma Direktifi, m. 13.

AIHM, *Gaskin v. Birleşik Krallık* başvurusunda, “Çocuk bakım hizmetine alınan kişinin reşit olduğu zaman, kişisel sorunlarını çözmek için geçmişini öğrenmek istemesine karşın, gizli bilgi içerdiği gerekçesiyle dosyasına erişmesine izin verilmemesini; AIHS’in 8. maddesinin gerektirdiği özel hayata ve aile hayatına saygı hakkının güvence altına alınmasını sağlayamadığı” gerekçesiyle ihlal kararı vermiştir⁴⁷.

Benzer şekilde, AIHM *Leander v. İsveç* başvurusunda, “Marangoz olan bir kişinin hakkındaki güvenlik soruşturması nedeniyle askeri bir deniz üssü yakınındaki müze-deki işine son verilmesi üzerine kendisine ilişkin güvenlik kayıtlarına erişmesine izin verilmemesini ve kişisel verilerin ulusal güvenlik gerekçesiyle gizli olarak tutulmasını” özel yaşama müdahale kabul ederek ihlal kararı vermiştir⁴⁸.

AIHM başka bir başvuruyu ise kişisel verilere erişim kapsamında değerlendirmiş ancak ihlal kararı vermemiştir. *Odièvre v. Fransa* başvurusunda AIHM, “doğumundan sonra öz annesi tarafından terk edilmiş ve Sağlık ve Sosyal Güvenlik birimine bırakılan kişinin, öz ailesini tespit etmesine imkân sağlayacak ayrıntıları edinememekten şikâyet etmesi ve bu ayrıntılara erişme imkânı olanağı bulamamasının, yaşam öyküsünü yeniden oluşturmasını engellediği ve kendisini oldukça kötü etkilediğini belirtmesi” üzerine; doğumun ve özellikle de bir çocuğun doğduğu koşulların, AIHS’in 8. maddesi ile güvence altına alınan, çocuğun ve yetişkin kişinin özel hayatlarının bir parçasını oluşturduğunu kaydetmiştir. Ancak üçüncü tarafın menfaatlerinin korunması güvence altına alınırken, başvurana annesi ve öz ailesiyle ilgili sınırlı bilgilerin verildiğini ve bu bilgiler aracılığıyla soyunun bir kısmının izini sürmesine imkân sağlandığını belirterek, AIHS’in 8. maddesinin ihlal edilmediğine karar vermiştir⁴⁹.

Segerstedt/Wiberg ve Diğerleri v. İsveç başvurusunda, başvuruçuların “suç işlenmesinin önlenmesi ve ulusal güvenliğin korunması amaçlarını tehlikeye düşürebileceği gerekçesiyle, İsveç Güvenlik Polisi tarafından kendileri hakkında tutulan dosyalara tam erişimlerine izin verilmemesinden” şikâyetçi olmaları üzerine AIHM, güvenlik polisi tarafından kendileri hakkında tutulan bilgilere tam erişim sağlanmasının reddedilmesini bir hak ihlali olarak değerlendirmemiştir⁵⁰.

AIHM, *K.H. ve Diğerleri v. Slovakya* başvurusunda ise “Roman kökenli sekiz Slovakya vatandaşının, iki hastanenin kadın hastalıkları ve doğum bölümünde tedavi görmeleri sonrasında artık çocuk sahibi olamamaları ve bunun söz konusu hastanelerde kaldıkları sırada kısırlaştırılmış olmalarından kaynaklandığından şüphelenmeleri üzerine, talep ettikleri tıbbi kayıtların fotokopilerinin kendilerine verilmemesini” ihlal olarak değerlendirmiştir⁵¹.

⁴⁷ B. No: 10454/83, T. 07.07.1989, *Gaskin v. Birleşik Krallık*.

⁴⁸ B. No: 9248/81, T. 26.03.1987, *Leander v. İsveç*.

⁴⁹ B. No: 42326/98, T. 13.02.2003, *Odièvre v. Fransa*, para. 48-49.

⁵⁰ B. No: 62332/00, T. 06.09.2006, *Segerstedt/Wiberg ve Diğerleri v. İsveç*, para. 104.

⁵¹ B. No: 32881/04, T. 06.11.2009, *K.H. ve Diğerleri v. Slovakya*, para. 58.

Haralambie v. Romanya başvurusunda ise, başvuruçunun “*bilhassa, komünist rejim dönemindeki eski gizli servisi tarafından kendisi hakkında oluşturulmuş olan kişisel dosyaya erişme hakkının engellenmesinden*” şikâyetçi olması üzerine AİHM, başvurunun komünist rejim altında gizli servis tarafından kendisi hakkında oluşturulmuş kişisel dosyaya erişiminin engellenmesinin bir hak ihlali olduğuna karar vermiştir⁵².

Birçok Avrupa ülkesinde ve değişik konularda ortaya çıkmış uyuşmazlıklar hakkında AİHM’in “kişisel verilere erişimi” AİHS’in 8. maddesi kapsamında mütalaa ettiği görülmektedir. Ayrıca doktrinde ve mevzuatta bir hak olarak kabul edilen *kişinin kendisi hakkındaki bilgilere erişebilmesi* gerekliliğini, aynı minvalde (istisnai halleriyle birlikte) değerlendirmekte ve aynı kriterlere göre karar verdiği anlaşılmaktadır.

KİŞİSEL VERİLERİN TOPLANMASI

Kişisel verilerin korunması bakımından önemli bir diğer aşama, “kişisel verilerin toplanması”dır. Kişisel verilerin “belirli, açık ve meşru amaçlar için toplanması” bir ilke olarak ifade edilmektedir. Nitekim bir kişisel veri ancak “meşru” bir amaç doğrultusunda toplanmalıdır⁵³. Kişisel verilerin toplanma amacı mümkün olduğunca “açık”⁵⁴ ve “belirli”⁵⁵ olmalıdır. Ayrıca belli bir amaç için toplanan bir veri başka bir amaç için kullanılmamalıdır⁵⁶. Keza verilerin toplanma amacı ile işleme amacı birbiriyle uyumlu olmalıdır⁵⁷. Kişisel verilerin toplanmasına ilişkin bir başka husus ise verinin toplanma amacı açısından yeterli olması, aşırı olmaması ve amaçla ilgili olmasıdır⁵⁸. Bir kişisel veri “ileride bir gün kullanılmak üzere” toplanmamalıdır⁵⁹. Böyle bir durum kişilerin özgürlüklerini kısıtlar⁶⁰ ve hukuk devleti ilkesine aykırılık teşkil eder.

İletişim teknolojisinin gelişmesi ile birlikte kişisel verilerin toplanması hususunda çok sayıda uyuşmazlık gündeme gelmektedir. AİHM de çeşitli konulara ilişkin önüne gelen başvurularda kişisel verilerin toplanması aşamasında hak ihlali tespiti yapmaktadır.

L.H. v. Letonya başvurusunda, “bir devlet kurumu (Tıbbi Bakım ve İşe Uygunluk Bakımından Kalite Kontrol Teftiş Kurumu) tarafından, ilgilinin rızası olmaksızın kişisel tıbbi verilerinin alınmasını” özel hayata saygı hakkının ihlali olarak değerlendiren AİHM, “kişilerin özel yaşama saygı hakkını kullanması konusunda tıbbi

⁵² B. No: 21737/03, T. 27.01.2010, *Haralambie v. Romanya*, para. 96.

⁵³ Peter Carey, *Data Protection*, 2. ed., Oxford, Oxford University Press, 2004, s. 54; Bygrave, *Data Privacy Law*, s.153.

⁵⁴ Bygrave, *Data Privacy Law*, s.155.

⁵⁵ Carey, s. 54.

⁵⁶ Carey, s. 51-67; Christopher Kuner, *European Data Protection Law*, 2. ed., Oxford, Oxford University Press, 2007, s. 100; Bygrave, *Data Privacy Law*, s.155.

⁵⁷ Carey, s. 54; Bygrave, *Data Privacy Law*, s.155.

⁵⁸ Carey, s. 55.

⁵⁹ Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Seçkin Yayınları, Ankara 2009, s. 142.

⁶⁰ Küzeci, s. 198.

verilerin korunmasının önemini vurgulayarak, *geçerli mevzuatın* yetkili makamlara ve yetki kullanma şekillerine tanınan *takdir payı kapsamını yeterli açıklıkla göstermediği*" gerekçesiyle, ihlal kararı vermiştir⁶¹. Bu karardan anlaşılacağı üzere AİHM kişisel verilerin toplanabilmesi için meşruluk zemini aramaktadır. Ayrıca kararda, toplama amacının belirli ve açık olması gerektiğini vurgulanmaktadır.

Tersi yönde bir kararda ise AİHM, "Solcu radikal bir hareket tarafından gerçekleştirilen bombalı saldırılara karıştığından şüphelenilen başvuranın GPS ile izlenmesinin ve bu yolla elde edilmiş olan verilerin hakkında yürütülen ceza yargılamalarında kullanılmasının kendisinin özel hayata saygı hakkını ihlal ettiği" iddiası üzerine ulusal güvenliğin korunması, kamu güvenliğinin korunması, mağdurların haklarının korunması ve suç işlenmesinin önlenmesi gibi amaçlarla 8. maddenin ihlal edilmediğine karar vermiştir⁶².

AİHM, *Taylor v. Sabori v. Birleşik Krallık* başvurusunda, "başvuranın çağrı cihazına gönderilen mesajların polis tarafından gizli bir izleme operasyonu kapsamında tespit edilmesi" üzerine özel hayata saygı hakkının ihlaline karar vermiştir⁶³.

Benzer şekilde, *Dragojević v. Hırvatistan* başvurusunda AİHM, "uyuşturucu kaçakçılığı yaptığı şüphesi bulunan bir kişinin telefon görüşmelerinin gizlice dinlenmesini, sorgu hâkiminin gizli dinleme tedbirinin kullanılmasının başvuranın davasında gerekli olup olmadığını ve haklı gerekçelerinin bulunup bulunmadığını etkili bir şekilde değerlendirmeye yönelik olarak Hırvatistan yasalarında öngörülen usule uyulmadığı iddiası" üzerine, ihlal kararı vermiştir⁶⁴.

AİHM'in, elbette bu konuya ilişkin inceleyemediğimiz başkaca kararları olmakla birlikte, yalnızca yukarıda verilen kararlardan edinilen kanaatle; AİHM'in de kişisel verilerin toplanması hususunda aynı kriterleri esas alarak karar verdiğini ifade edebiliriz. Her bir uyuşmazlıkta somut olay ve iç hukuktaki mevzuatı göz önünde bulundurmakla birlikte kararları kişisel verilerin toplanmasına ilişkin ilkeler eksenine oturtmaktadır. Kamu düzeni ve ulusal güvenliği özel hayatın korunması hakkı karşısında üstün kabul ederken, gizli dinlemenin yasalara uygun yapılmamış olmasının özel hayata saygı hakkının ihlali olarak değerlendirmiştir.

KİŞİSEL VERİLERİN KULLANILMASI

Kişisel veriler, belli bazı amaçlarla işlenmekte, kaydedilmekte ve ihtiyaç duyuldukça kullanılması mümkün olabilmektedir. Bu doğrultuda hukuki metinlerde, *kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi ilkesinin* benimsendiği

⁶¹ B. No: 52019/07, T. 29.04.2014, L.H. v. Letonya, para. 59-60.

⁶² B. No: 35623/05, T. 02.12.2010, Uzun v. Almanya, para. 80-81.

⁶³ B. No: 47114/99, T. 22.01.2003, Taylor-Sabori v. Birleşik Krallık, para. 18-19.

⁶⁴ B. No: 68955/11, T. 15.04.2015, Dragojević v. Hırvatistan, para. 101-102.

görülmektedir⁶⁵. Bu minvalde, işlenecek kişisel verinin doğru olması, işlenmesinin gereklilik arz etmesi ve güncel olarak tutulması hususlarına riayet etmek gerekmektedir⁶⁶. Aynı zamanda, kişisel verilerin işlenmesinde hukuk devleti ilkesinin bir gereği olarak ölçülülük ilkesi de dikkate alınmalıdır⁶⁷. Ayrıca özel olarak korunması gereken *hassas verilerin* işlenmesi kural olarak yasaklanmakta ancak yasal bir temel ve ilgili kişinin rızası ile işlenebilmektedir⁶⁸.

Kişisel veriler toplanma amacına uygun bir şekilde işlenmeli ve kullanılmalı⁶⁹ ve gerektiğinden fazla süre kayıt altında tutulmamalıdır⁷⁰. Ayrıca kişisel verilerin hangi amaçla kullanılacağına ilgili kişi tarafından da bilinmesi gereklilik arz etmekte ve bunun önleyici bir koruma sağlayacağı düşünülmektedir⁷¹. Nitekim kişisel verilerin işlenmesi ve kullanılması sürecinde bu hususlara dikkat edilmelidir. Aksi takdirde kişisel verilerin korunması hakkı ihlal edilmektedir. AİHM de çok sayıda başvuruya bu çerçeveden bakarak kararlar tesis etmiştir.

AİHM *S. ve Marper v. Birleşik Krallık* başvurusunda, “ilgili kişilerden alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin, bu kişiler hakkında beraat kararı verilmesine ve haklarındaki ceza davasının sona ermesine rağmen, bir veri tabanında belirsiz bir süre boyunca saklanmasını” ölçülü olmayan bir müdahale olarak nitelendirmiş ve demokratik bir toplumda gerekli olduğunun değerlendirilemeyeceğini kaydederek, AİHS’in 8. maddesinin ihlal edildiğine karar vermiştir⁷².

Diğer taraftan, *Garde v. Fransa*⁷³ başvurusunda ise, “Yetkili bir konumda iken 15 yaşındaki çocuklara tecavüz suçundan mahkûm edilen kimselerin, özellikle, cinsel suçluların bilgilerinin tutulduğu ulusal veri tabanına kaydedilmelerinden şikâyetçi olmaları üzerine AİHM, “cinsel suçluların ulusal veri tabanına kaydedilmelerine ilişkin sistemin söz konusu çatışan kişisel çıkarlar ile kamu menfaati arasında adil bir denge tesis etmiş olduğunu” ifade ederek AİHS’in 8. maddesinin ihlal edilmediğine karar vermiştir.

L.L. v. Fransa başvurusunda ise “boşanma davası bağlamında, kendisinin ve tıbbi uzmanın rızası olmadan bu çerçevede düzenlenen kendisine ait tıbbi kayıtlarla ilgili belgelerin mahkemeler tarafından sunulması ve kullanılması üzerine” hak ihlali

⁶⁵ Örneğin bkz. OECD Rehber İlkeleri m. 7, m. 8, m. 9, m. 10, m. 11, m. 12, m. 13, m. 14; APEC Çerçeve Belge; BM Rehber İlkeleri m. 12; 108 Sayılı AK Sözleşmesi m. 5(a); AB 95/46 sayılı Veri Koruma Direktifi m. 6/1.

⁶⁶ Carey, s. 57.

⁶⁷ Şimşek, s. 98.

⁶⁸ Cemil Kaya, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 69, S. 1-2, 2011, s. 317-334, s. 323.

⁶⁹ “...verilerin daha sonra işleme amaçlarının toplanma amacı ile uyumlu olması, ilke ile hedeflenen hukuksal yararın gerçekleşebilmesi için de bir zorunluluktur. Kişisel verilerin sonraki kullanımlarının toplanma amacı ile bağdaşmaması durumunda ilgili kişinin kişisel verileri üzerindeki denetimi kaybedeceği açıktır.” Kütüceci, s. 201.

⁷⁰ Kişisel verilerin gerektiğinden fazla süre tutulmaması gerekliliği aynı zamanda “unutulma hakkı” olarak değerlendirilmektedir. Ayrıntılı bilgi için bkz., Eren Sözüer, **Unutulma Hakkı**, İstanbul, On İki Levha Yayıncılık, 2017.

⁷¹ Kütüceci, s. 202.

⁷² B. No: 30562/04, T. 04.12.2008, S. ve Marper v. Birleşik Krallık, para. 125-126.

⁷³ B. No: 16428/05, T. 17.03.2010, Gardel v. Fransa, para. 71.

iddiasına karşın AİHM “başvurucunun özel hayatına yapılan müdahalenin kişisel verilerin korunmasının temel önemi açısından gerekçelendirilmediğini” belirterek, AİHS’ın 8. maddesinin ihlal edildiğine karar vermiştir⁷⁴.

Shimovolos v. Rusya başvurusunda ise AİHM, “bir insan hakları aktivistinin gizli bir güvenlik izleme veri tabanına kaydedilmesi, bu yolla Rusya içerisinde tren ya da havayolu ile yaptığı seyahatlerin takip edilmesi ve bununla ilgili olarak tutuklanması” üzerine yapılan başvuruyu hak ihlali olarak görmüştür⁷⁵.

Khelili v. İsviçre başvurusunda ise 1993 yılında Cenevre’de gerçekleştirilen bir polis kontrolü sırasında başvurucunun, üzerinde “İyi, güzel bir kadın, otuzlarının sonunda, birlikte bir şeyler içmek ya da arada sırada dışarı çıkmak için bir erkek arıyor. Tel. no. ...” yazan kartvizitler taşıdığı tespit edilmiştir. Polisin, bu kartları bulması sonrasında, başvurucu, adının bilgisayar veri tabanına “fahişe” olarak kaydedildiğini iddia etmiş ve bu mesleği yapmadığını sürekli olarak yinelemiştir. “Özel hayatına ilişkin olarak yanlış olduğunu iddia ettiği bu verilerin kaydedilmesini, özel hayatına saygı hakkını ihlal ettiği iddiası ile yapmış olduğu başvuruda AİHM, “başvuranın özel hayatına ilişkin yanlış olduğu iddia edilen verilerin polis kayıtlarında tutulmasının başvuranın özel hayata saygı hakkını ihlal ettiğine ve ‘fahişe’ kelimesinin yıllar boyunca kayıtlarda muhafaza edilmesinin haklı gerekçelere dayanmadığına ve demokratik bir toplumda gerekli olmadığına” kanaat getirerek ihlal kararı vermiştir⁷⁶.

AİHM’in, kişisel verilerin işlenmesi ve kullanılmasına ilişkin farklı konularda önüne gelen uyuşmazlıklarda, bir kriter belirlemeye çalıştığı söylenebilir. AİHM, öncelikle, verilerin meşruluk ve hukuka uygunluk zemininde işlenmesi ve kullanılması gerektiğini ifade etmektedir. Diğer taraftan, verilerin saklanması ve kullanılmasında korunan hukuki değerler bakımından bir orantılılık olması gerektiğine işaret ederek ölçülülük ilkesinin gerekliliğine vurgu yapmaktadır. Keza geçmişte, belli bir dönemde gerçekleşmiş fiiller kapsamında saklanan verilerin, belli bir süreden sonra gereklilik arz etmemesi üzerine kullanılmaması gerektiğini ifade etmektedir. Bunlarla birlikte kamu düzeni ve güvenliği gibi hususlara ilişkin işlenen verilerin, korunan hukuki değer bakımından kişisel verilerin korunmasından daha üstün bir yarar taşıdığına hükmetmektedir.

KİŞİSEL VERİLERİN AKTARILMASI VE İFŞA EDİLMESİ

Kişisel verilerin aktarılması veya ifşa edilmemesi/yayılmaması, verilerin korunması kapsamında yer almaktadır. Kişiyi bir şekilde etkileyebilen her bilgi kişisel veri olarak nitelendirilebilmektedir⁷⁷. Nitekim bu verilerin başka kişi veya kurumlara

⁷⁴ B. No: 7508/02, T. 12.02.2007, L.L. v. Fransa, para. 47-48.

⁷⁵ B. No: 30194/09, T. 28.11.2011, Shimovolos v. Rusya, para. 70-71.

⁷⁶ B. No: 16188/07, T. 08.03.2012, Khelili v. İsviçre, para. 70-71.

⁷⁷ Karen McCullagh, “Protecting ‘privacy’ through control of ‘personal’ data processing: A flawed approach”, *International Review of Law, Computers & Technology*, Vol. 23, Nos. 1–2, March – July 2009, s. 13-24, s. 15.

hukuka aykırı olarak aktarılması veya belli şekillerde kamuya açık bir şekilde ifşa edilmesi veya yayılması kişisel verilerin korunması hakkının ihlaline yol açmaktadır. Bu ihlaller aynı zamanda ceza hukuku bakımından da suç teşkil etmekte ve mevzuatta da münferit düzenlemelere tabi tutulmaktadır⁷⁸.

Kişisel verilerin korunmasında “*veri güvenliği ilkesi*” büyük önem arz etmektedir. Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemelerin neredeyse tamamında bu ilkeye yer verilmektedir. Bu ilke veri denetçilerinin kişisel verilerin ortadan kaldırılmasını, bunlara yetkisiz erişimi, değiştirilmesini, silinmesini ve yayınlanmasını engelleyecek önlemleri almasını gerektirir⁷⁹. Dolayısıyla kişisel verilerin ilgili kişinin rızası⁸⁰ dışında, hukuka aykırı bir şekilde bir başkasına aktarılması veya yayılması *veri güvenliği ilkesi* ile güvence altına alınmaktadır. AİHM de kişisel verilerin hukuka aykırı şekilde aktarılmasını, ifşa edilmesini veya yayılmasını hakkın korunmasının ihlali olarak AİHS’in 8. maddesi kapsamında ele almaktadır.

AİHM, *M.S. v. İsveç* başvurusunda, başvurusunun geçirdiği kürtaj hakkında bilgi içeren tıbbi kayıtların bir klinik tarafından sosyal güvenlik kurumuna iletilmesi üzerine, “*başvurucunun tıbbi kayıtlarının söz konusu klinik tarafından sosyal güvenlik kurumuna iletilmesi için uygun ve yeterli gerekçelerin mevcut olduğu ve uygulanan tedbirin, ülkenin refahının korunması yönündeki meşru amaçla orantılı olduğu*” gerekçesiyle ilgili kişinin kişisel verilerine yönelik hukuka aykırı bir müdahale olmadığına hükmetmiştir⁸¹.

Z. v. Finlandiya başvurusunda, HIV hastası olan başvurusunun hakkındaki tıbbi bilgilerin eşi aleyhindeki bir dava sırasında ifşa edilmesi üzerine AİHM, “*başvurucunun kimliğinin ve HIV hastası olduğuna ilişkin bilgilerin Temyiz Mahkemesinin basının erişimine açık olan karar metninde ifşa edilmesinin hiçbir haklı gerekçesinin bulunmadığını ve dolayısıyla ilgili bilgilerin yayımlanmasının başvuranın özel hayata ve aile hayatına saygı duyma hakkına ilişkin bir ihlale neden olduğunu*” ifade ederek ihlal kararı vermiştir⁸².

Peck v. Birleşik Krallık başvurusunda ise başvurusunun “bir sokağa yerleştirilen kapalı devre kameranın kaydettiği ve içinde kendisinin bileğini kestiğini gösteren kamera görüntülerin medyaya verilmesi” üzerine AİHM, “*görüntülerin Belediye Meclisi tarafından medyaya verildiği sırada yeterli güvencelerin sağlanmadığından bahisle*” başvurusunun özel hayatına orantısız ve haksız bir müdahalede bulunulduğuna karar vermiştir⁸³.

⁷⁸ 5327 Sayılı Türk Ceza Kanunu’nun; “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” başlıklı Dokuzuncu Bölümü’nün altında “*Haberleşmenin gizliliğini ihlal*” başlıklı 132. maddesi, “*Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması başlıklı*” 133. maddesi, “*Özel hayatın gizliliğini ihlal*” başlıklı 134. maddesi, “*Kişisel verilerin kaydedilmesi*” başlıklı 135. maddesi, “*Verileri hukuka aykırı olarak verme veya ele geçirme*” başlıklı 136. maddesi ve “*Verileri yok etme*” başlıklı 138. maddesi bu hususta düzenlemeler içermektedir.

⁷⁹ Bygrave, *Data Privacy Law*, s.164.

⁸⁰ Küzeci, s. 220 vd.; Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması*, Ankara, Yetkin Yayınları, 2004, s. 39 vd.; Yüksel, s. 113.

⁸¹ B. No: 20837/92, T. 27.08.1997, M.S. v. İsveç, para. 44.

⁸² B. No: 22009/93, T. 25.02.1997, Z. v. Finlandiya, para. 113.

⁸³ B. No: 44647/98, T.28.04. 2003, Peck v. Birleşik Krallık, para. 86-87.

AİHM, *Doorson v. Hollanda* başvurusunda, *polis dosyasında bulunan davacıya ait fotoğrafın üçüncü kişilere gösterilmesinin AİHS'in 8. maddesinin ihlali olup olmadığını değerlendirirken; fotoğrafların sadece soruşturma amacıyla kullanılması, genel olarak kamu erişimine açık olmaması ve daha önce gerçekleşen bir tutuklama sırasında kanunlara uygun olarak çekilmesini dikkate alarak suçu önlemeye yönelik olan bu eylemi kişisel verilerin korunması hakkının ihlal edilmediği şeklinde nitelendirmiştir*⁸⁴.

Panteleyenکو v. Ukrayna başvurusunda, başvuru "zihinsel durumuna ve psikiyatrik tedavisine ilişkin gizli bilgilerin bir duruşma sırasında açıklanması" üzerine AİHM'e müracaat etmiş ve AİHM "*başvuranın ruhsal sağlığına ve ilgili tedaviye ilişkin gizli bilgilerin ruh ve sinir hastalıkları hastanesinden elde edilmesinin ve kamuya açık bir duruşmada açıklanmasının başvuranın özel hayatına saygı duyma hakkına dair bir müdahale oluşturduğuna*" karar vermiştir⁸⁵.

AİHM, Monaco Prensesi Coroline'in, *ata binerken ya da alışveriş yaparken çekilmiş fotoğraflarını yayınlayan* ünlü Bunte ve Neue Post dergilerine karşı (oldukça ses getiren) başvurusunda; "*mevcut davada kamunun bir menfaati bulunsa dahi aynı zamanda söz konusu fotoğraf ve makalelerin yayınlanmasında dergilerin de ticari bir menfaati bulunduğundan, bu menfaatlerden başvuruçunun özel hayatının etkin şekilde korunması hakkı diğeri karşısında üstün gelmektedir*" diyerek AİHS'in 8. maddesi kapsamında özel yaşamın ihlaline karar vermiştir⁸⁶.

AİHM yukarıda verilen örneklerden anlaşılacağı üzere somut olaylardaki kendine özgü hususları göz önünde bulundurmak suretiyle ölçülülük ilkesi kapsamında değerlendirme yapmaktadır. Kişisel verilerin aktarılmasına veya yayılmasına üçüncü kişilerin katkısı ve beklentisi veya kurumların ihmali davranışı bir hak ihlali oluşup oluşmadığı noktasında belirleyici olabilmektedir. Bazen de ilgilinin kendi davranışı kişisel verinin aktarılmasını veya yayılmasını hukuka uygun hale getirmektedir.

KİŞİSEL VERİLERİN SİLİNMESİ/İMHASI

Kişisel verilerin işlenmesi, saklanması/kaydedilmesi, kullanılması ve yayılması nasıl ki belli ölçütlere bağlı kılınmışsa bu verilerin silinmesi, ortadan kaldırılması da bir gereklilik arz etmektedir. Çünkü kişisel verilerin tutulması (her zaman olmamakla birlikte) kendi başına potansiyel bir risk taşımaktadır⁸⁷. Dolayısıyla kişisel verilere duyulan ihtiyaç ortadan kalktığında, ya o veriler ortadan kaldırılmalı ya

⁸⁴ B. No: 20524/92, T.26.03.1996, *Doorson v. Hollanda*, para. 48-70.

⁸⁵ B. No: 11901/02, T. 12.02.2007, *Panteleyenکو v. Ukrayna*, para. 81.

⁸⁶ B. No: 59320/00, T. 24.06.2004, *Von Hannover v. Almanya*, para. 74.

⁸⁷ Kütüceci, s. 210.

da anonimleştirilmelidir⁸⁸. Kişisel verilerin gerektiğinden fazla saklanmamasının bir başka önemi ise; haklı gerekçelerle de olsa, bir kez kişisel verileri işlenen bir kimşenin ömür boyunca bu bilginin bir yerlerde kayıt altında tutulmayı sürdüreceğini ve her daim kullanılabilceğini düşünmesidir. Böyle bir durumda, bireyin maddi ve manevi bütünlüğü, bireysel özerklik ve özel yaşamın gizliliği gibi hukuken korunan değerleri ihlal edilmiş olacaktır⁸⁹. Nihayetinde bir kişinin, kendisi hakkında işlenen bir kişisel verinin silinmesini isteme hakkı, kişisel verilerin korunması hakkının bir gereğidir.

Dolayısıyla kişisel verilerin işlenme amacı ortadan kalktığında, bir başka deyişle, kişisel veri ile işlenme amacı arasındaki nedensellik bağı sona erdiğinde bir daha erişilemeyecek şekilde tamamen ortadan kaldırılmalıdır. Nitekim kişisel verilerin tamamen ortadan kaldırılmamasından kaynaklanan birçok uyumsuzluğun çözümü için AİHM'e başvurulmaktadır.

Rotaru v. Romanya başvurusunda, başvuru komünist rejimi eleştirmiş olması sebebiyle 1948 yılında bir yıl hapis cezasına mahkûm edilmiştir. AİHM, Romanya İstihbarat Servisi tarafından başvuru özel hayatına mahsus olan bilgilerin tutulması ve kullanılmasının kanunlara uygun olmadığını değerlendirerek, AİHS'in 8. maddesinin ihlal edildiğine hükmetmiştir.

AİHM, özellikle, bilgilerin makamlarca sistematik bir şekilde toplanması ve dosyalarda saklanması halinde, özel hayat kapsamına girebileceğini gözlemlemiş ve "*iç hukukta tutulan bilgilerin ne kadar bir süreyi kapsayacağına ya da ne kadar uzun süreyle bilgi tutulabileceğine dair sınırlar konmamasını, Romanya hukukunun kamu makamlarına tanınan ilgili takdir yetkisinin kapsamını ve kullanılma biçimini makul bir açıklıkla belirtmediği*" gerekçesiyle ihlal kararı vermiştir⁹⁰. Dolayısıyla AİHM, kişisel verilerin hiç kullanılmasa dahi belli bir veri tabanında kayıtlı tutulmasını hak ihlali olarak değerlendirmiştir.

AİHM başvuru hakkında, "*fahişe*" kelimesinin yıllar boyunca kayıtlarda muhafaza edilmesinin haklı gerekçelere dayanmadığına ve demokratik bir toplumda gerekli olmadığına kanaat getirmiş ve başvuru "*fahişe*" kelimesinin polis kayıtlarından silinmesini istemedi kayda değer ölçüde menfaati bulunduğuna" karar vermiştir⁹¹. AİHM bu kararında, esasen, bir kişinin; kendisi hakkında işlenen bir kişisel verinin artık geçerli ve gerekli bir bilgi olmadığını ileri sürerek, o verilerin silinmesini isteme hakkına sahip olduğunu belirtmiştir. Şüphesiz o verinin veri tabanında varlığı sürdürmesi, o kişinin hayatını olumsuz yönde etkilemeye devam edebilecektir.

⁸⁸ Carey, s. 58.

⁸⁹ Kütüceci, s. 210.

⁹⁰ B. No: 28341/95, T. 04.05.2000, *Rotaru-Romanya*, para. 62.

⁹¹ B. No: 16188/07, T. 08.03.2012, *Khelili v. İsviçre*, para. 70-71.

SONUÇ

Çok uzun bir geçmişi olmayan kişisel verilerin korunması hakkı yakın bir zamanda ortaya çıkmış ve gelişme göstermiştir. Hal böyle olunca da bu alana ilişkin yasal temel, somut olayların dava konusu olması üzerine verilen yargı kararlarıyla belli bir hukuki zemine oturmuştur. Günümüzde "Kişisel verilerin korunması" üzerine hem uluslararası hem de ulusal ölçekte düzenlemeler bulunmaktadır. Özellikle Avrupa Birliği ülkeleri başta olmak üzere birçok ülke, farklı yönleri olmakla birlikte, kişisel verileri koruma kanunları ve alt düzenlemeleri ile birlikte kişisel verileri koruma kurumları oluşturmuştur. Nitekim yasal düzenlemeler ve kurumlar kişisel verilerin korunması hakkının varlığına ve saygınlığına önemli katkı sunmaktadır.

AİHM kararlarının da kişisel verilerin korunması hakkına katkısı çoktur. Nitekim Avrupa Birliği'nin 95/46 sayılı Veri Koruma Direktifi ve 2016/679 sayılı Regülasyonu henüz yürürlüğe dahi girmeden AİHM, kişisel verilerin korunması hakkı konusunda birçok karar vermiştir. Bu kararların, Avrupa Birliği'nin 95/46 sayılı Veri Koruma Direktifi ve 2016/679 sayılı Regülasyonu başta olmak üzere diğer hukuki metinlerin düzenlenmesinde, kaynak niteliğinde olduğu ifade edilebilir.

AİHM, kişisel verilerin korunması hakkında yapılan başvuruları AİHS'de münhasır bir düzenleme bulunmadığı için AİHS'in 8. maddesi kapsamında ele almıştır. Yukarıda da aktarıldığı üzere, AİHM konuya ilişkin kararlarında, AİHS'in 8. maddesinin birinci ve ikinci fıkralarını referans almaktadır. AİHM bu iki fıkra arasındaki hukuka uygunluk sınırını somut olaylar özelinde değerlendirmek suretiyle tespit etmektedir. AİHM davaları her ne kadar AİHS'in 8. maddesi kapsamında incelemiş olsa da kişisel verilerin korunmasına ilişkin kararlarında, kronolojik olarak, bir gelişme kaydetmiştir. AİHM'in bir sonraki kararları önceki kararlarına göre daha gelişmiş değerlendirmeleri içermektedir. Ancak çalışmada değinilen kararlarından anlaşılacağı üzere AİHM'in, kişisel verilerin korunması hakkında kendine özgü ve yeni ölçütler ortaya koyamamış AİHS'in 8. maddesine bağımlı kalmıştır.

En nihayetinde, AİHS'nin 8. maddesi ve AİHM kararları, kişisel verilerin korunması hakkı bakımından temel bir yapı taşı olarak varlığını sürdürmektedir. AİHS'nin 8. maddesi ve AİHM kararları, bu hakkın omurgasını oluşturan hukuk yolu olarak önemli bir konuma sahiptir.

KAYNAKÇA

Asinari, M. Verónica Pérez : Legal Constraints for the Protection of Privacy and Personal Data in Electronic Evidence Handling, **International Review of Law, Computers & Technology**, 18:2, 2004.

Başalp, Nilgün : **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yayınları, 2004.

Bygrave, Lee A. : **Data Privacy Law**, Oxford, Oxford University Press, 2014.

- Bygrave, Lee : “Where have all the judges gone? Reflections on judicial involvement in developing data protection law”, **Privacy Law and Policy Reporter**, Y. 2000, C. 7, s. 11-14, 33-36.
- Carey, Peter : **Data Protection**, 2. ed., Oxford, Oxford University Press, 2004.
- Gölcüklü, Feyyaz/ : **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Gözübüyük, A. Şeref, 9.b., Ankara, Turhan Kitabevi, 2011.
- Kaya, Cemil : **İdare Hukukunda Bilgi Edinme Hakkı**, Ankara, Seçkin Yayıncılık, 2005.
- Kaya, Cemil : “Avrupa Toplulukları Adalet Divanının PNR Kararının Tahlili”, **Prof. Dr. Hüseyin Hatemi’ye Armağan**, C. II, Vedat Kitapçılık, İstanbul, 2009, s. 2027-2039.
- Kaya, Cemil : Avrupa Birliği veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. 69, S. 1-2, 2011, s. 317-334.
- Kuner, Christopher : **European Data Protection Law**, 2. ed., Oxford, Oxford University Press, 2007.
- Küzeci, Elif : **Kişisel Verilerin Korunması**, Ankara, Turhan Kitabevi, 2010.
- McCullagh, Karen : “Protecting ‘privacy’ through control of ‘personal’ data processing: A flawed approach”, **International Review of Law, Computers & Technology**, Vol. 23, Nos. 1-2, March-July 2009, s. 13-24.
- Özdemir, Hayrunnisa : **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara 2009.
- Sözüer, Eren : **Unutulma Hakkı**, İstanbul, On iki levha Yayıncılık, 2017.
- Şimşek, Oğuz : **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta Basım, 2008.
- Yüksel, Saadet : **Özel Yaşamın Bir parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, İstanbul, Beta Basım, 2012.