

HUKUKA AYKIRI YÖNTEMLERLE ELDE EDİLEN KİŞİSEL VERİ NİTELİĞİNDEKİ İLETİŞİM BİLGİLERİNİN HUKUKA AYKIRILIĞI

Doç. Dr. Murat Volkan Dülger*

Hukuka aykırı yöntemlerle elde edildiği için hukuka aykırı delil niteliğini taşıyan bilgi ve belgelerin muhakeme aşamalarında delil olarak kullanılıp kullanılamayacağına yanı sıra kural olarak kullanılamayacağına kabul edilmesi halinde bunun istisnalarının olup olmayacağı ülkemizde olduğu gibi diğer tüm dünya ülkelerinde tartışmalı bir konudur. Hukuka aykırı delil tartışması, işkence ve kötü muamele gibi yasak yöntemlere başvurulması nedeniyle çok eski yıllardan bu yana bilinen bir olgu olup, bu konu çok tartışılmış, birçok yayına ve bilimsel etkinliğe konu olmuş ve nihayet ulusal ve ulusal üstü çok sayıda hukuki metinde de işlenmiştir. Teknolojinin gelişmesiyle beraber bilişim sistemlerinin sağladığı imkânların, hukuka aykırı yeni yöntemlerin ortaya çıkmasına neden olması ve mevcut yöntemlerin de uygulanmasını kolaylaştırması, hukuka aykırı delil olgusunu günümüzde farklı açılardan ele alınmasını gerekli kılmıştır. Ancak teknoloji sayesinde ya da yardımıyla elde edilen deliller bu kadar yaygın tartışma konusu olmadığı gibi, hukuksal metinlere de henüz beklenen düzeyde girmemiştir.

Öte yandan yine teknolojinin getirdiği yenilikler sonucu hayatımıza giren, özellikle internet siteleri, sosyal medya uygulamaları, biyometrik sistemler veya kamera gibi elektronik uygulamalar bireyleri daha şeffaf ve izlenebilir hale getirmiştir. Böylece bireylerin verilerine kolaylıkla ulaşılabilmekte ve bu veriler meşru bir amaç veya bireyin rızası olmaksızın işleme faaliyetlerine tabi tutulabilmektedir. Bu durum bireylerin verilerinin tehlikede olduğu ve dolayısıyla korunması gerektiği düşüncesinden hareketle kişisel verilerin korunması hakkının doğmasını sağlamıştır. Bugün neredeyse tüm dünya ülkelerinde kişisel verilerin korunması bir hak olarak yasal düzenlemelerle koruma ve güvence altına alınmıştır. Henüz konuya ilişkin özel bir kanunun yürürlüğe girmediği ülkelerde dahi kişisel verilerin korunmasına yönelik çalışmalar devam etmektedir.

Kişisel verilere daha kolay erişilebilen ve bireylerin daha görünür ve izlenebilir olduğu dönemle, bu verilerin hukuka aykırı yollarla elde edilmesinin kolaylaşması ve yaygınlaşması paralellik göstermektedir. Bu nedenle günümüzde kişisel verilerin hukuka aykırı yollarla elde edilmesi ve işlenmesine sıklıkla rastlanmaktadır. Hukuka aykırı yöntemlerle elde edilen kişisel veriler, kolluk güçleri veya yargılama makamları tarafından elde edilerek yargılama aşamasında kullanıldığı gibi, yargılamanın taraflarından biri aracılığıyla da yargılamaya dahil edilebilmektedir.

Kişisel verileri hukuka aykırı olarak elde edilerek aleyhine ispat aracı olarak kullanılan taraf ise, bu durum karşısında kişisel verilerinin korunması hakkının ihlal edildiğini ve bu nitelikteki verilerinin hiçbir şekilde kendisine karşı kullanılamayacağı yönünde itiraz etmektedir. Nitekim

* Akademisyen/Avukat.

bu itirazını hakkında yürütülen dava kapsamında kendisini savunma amaçlı öne sürdüğü gibi ayrı bir dava olarak da iddia edebilmektedir. Bu durum, hukuka aykırı yöntemler kullanılarak elde edilen ve kişisel veri içeren delillerin yargılamada kullanılıp kullanılmayacağı sorununa yeni bir boyut kazandırmış ve hukuka aykırı delillerin kişisel verilerin korunması hakkı bağlamında ele alınmasını gerektirmiştir.

Hukuka aykırı yöntemler kullanılarak elde edilen ve kişisel veri içeren bilgi ve belgelerin yargı makamları nezdinde kullanılmasının yaygınlaşması ve kişisel veri sahibinin buna karşılık olarak haklarının ihlal edildiğini ileri sürmesi, konunun, mahkemeler önüne gelmesine neden olmuş ve mahkemeler aracılığıyla çözüme kavuşturulmasını gerekli kılmıştır. Avrupa İnsan Hakları Mahkemesi (Mahkeme/AİHM) de, bir başvuruçunun, polis tarafından yasadışı yollarla kimliğinin ortaya çıkmasına neden olacak şekilde bilgi toplanıldığından bahisle haklarının ihlal edildiği iddiası üzerine tam da bu konuya ilişkin olarak yaptığı inceleme sonucu yakın tarihte “*Benedik v. Slovenya*”¹ kararını vermiştir.

Hukuka aykırı yöntemlerle elde edilen ve kişisel veri içeren delillerin veri sahibi aleyhine kullanılıp kullanılmayacağı kuralının istisnaları olup olmayacağını anlayabilmek adına ilk olarak, başvurusu konu olayın Mahkeme önüne geliş sürecini anlattıktan sonra hangi gerekçelerle 8. madde kapsamında değerlendirildiğini açıklayacağım. Bundan sonra başvuruçunun hakkına müdahale olup olmadığı; varsa bu müdahalenin meşru olup olmadığını değerlendirerek dava konusu olayın 8. maddeye uygunluğunu tespit etmeye çalışacağım. Bu tespiti yaparken; konuyu, abonelik bilgilerinin elde edilmesinin yasaya uygunluğu, hukuka aykırı yöntemlerle elde ettiği iddia edilen kimlik bilgileri açısından hukuka aykırı delil sorunu ve bilgilerin kişisel veri niteliğinde olması nedeniyle kişisel verilerin korunması olarak üç farklı açıdan ele alacağım. Bu kapsamda Mahkemenin dava konusu olaya ilişkin karar ve gerekçeleri ile benzer konulu kararları ışığında kendi görüşlerimi belirterek kişisel verilerin korunması bağlamında hukuka aykırı delil sorununa ilişkin değerlendirmede bulunacağım.

I. Başvuru Konusu Olay ve Mahkemenin Önüne Geliş Süreci

Dava, Slovenya’nın Kranj şehrinde yaşayan 1977 doğumlu başvuruçusu Igor Benedik’in 2006 yılında Valais Kantonu adli makamlarının “Razorback” ağının kullanıcılarına yönelik yürüttüğü izleme faaliyeti sonucunda pornografik materyallerin teşhir edilmesi, üretilmesi, bulundurulması ve dağıtılması suçunu işlediğinin tespit edilmesi ile ilgilidir. Valais Kantonu adli makamları yürüttükleri izleme faaliyetinde bazı kullanıcıların resim veya video biçimde içerik bulundurduklarını ve bu içerikleri, bağlı bilgisayarlardan her birinin hem kullanıcı hem de sunucu olarak işlev gördüğü p2p (eşler arası) dosya paylaşım ağı aracılığıyla paylaştıklarını tespit etmiştir. Böylece bu ağ üzerindeki her kullanıcı diğer bir kullanıcının paylaşımlarına erişebildiği gibi, ayrıca bu paylaşımları da indirebilecektir.

İsviçre polisi tarafından yapılan araştırma sonucunda söz konusu ağa bağlandığı tespit edilen IP adreslerinin elde edilmesi üzerine Slovak polisi 7 Ağustos 2006 tarihinde bir internet servis sağlayıcısı şirketi olan ISP şirketinden, elde edilen IP adresinin belirtilen tarih ve saatte tahsis edilen kişiye ait verilerin bildirilmesini talep etmiştir. Polis, bu talebini herhangi bir mahkeme

¹ “*Benedik v. Slovenya*”, B. No: 62357/14, 24.04.2018.

kararına dayandırmamakla birlikte, elektronik haberleşme operatörlerinin ilgili dizinde detaylı bilgileri bulunmayan elektronik iletişim araçlarının kullanıcı veya sahipleri ile ilgili bilgileri polise bildirmeleri gerektiğini öngören Slovenya Ceza Muhakemesi Kanunu'nun (SCMK) ilgili hükmüne dayanmıştır. Bunun üzerine belirtilen IP adresine ilişkin olarak başvurunun babasının adı ve adresi internet hizmetine abone olması nedeniyle ISS tarafından polise bildirilmiştir. Bundan sonra polis, Kranj Bölge Mahkemesi sorgu hakiminden aldığı 14 Aralık 2006 tarihli mahkeme kararına dayanarak ISS'den söz konusu IP adresinin abonesinin kişisel bilgilerini ve trafik bilgilerini talep etmiş ve almıştır. Son olarak alınan arama kararıyla başvurunun babasına ait ev aranarak dört adet bilgisayara el konulmuştur.

Polis tarafından el konulan bilgisayarların sabit diskleri üzerinde yapılan inceleme sonucu çocuk pornografisi içeriklerinin yer aldığı bir dosya tespit edilmiş ayrıca eMule isimli dosya paylaşım programı aracılığıyla indirilen dosyalar arasında çocuk pornografisinin de yer aldığı belirlenmiştir. Başvurucunun söz konusu dosyaların farkında olmadığı ve ISS'nin mahkeme kararı olmadan kişisel verilerini hukuka aykırı bir şekilde polise verdiği yönündeki savunmalarına rağmen, Kranj Bölge Mahkemesi sorgu hakimi tarafından 5 Mart 2008 tarihinde başvuru aleyhine pornografik materyallerin teşhir edilmesi, üretilmesi, bulundurulması ve dağıtılması suçuna yönelik olarak soruşturma başlatılmıştır. Ancak söz konusu IP adresinin kullanıcısının kimlik bilgilerinin ve trafik verilerinin mahkeme kararı olmaksızın verilmemesi gerektiği, aksi halde hukuka aykırı yollarla elde edilen delilin söz konusu olacağı gerekçesiyle soruşturma açma kararına itiraz edilmiştir.

Yapılan yargılama sonucunda başvurunun söz konusu suçu işlediğine hükmedilmiş ve sekiz ay hapis cezasına hükmedilmiştir. Ayrıca hukuka aykırı yollarla elde edildiği iddia edilen verilerin Slovenya Ceza Muhakemesi Kanunu'na uygun olarak elde edildiği dolayısıyla hukuka aykırı delilin söz konusu olmadığı tespit edilmiştir.

Başvurucu ilk derece mahkemesinin vermiş olduğu karara karşılık, hukuka uygun olmayan yollarla elde edilen verilere dayanan tüm delillerin de reddedilmesi gerektiği gerekçesiyle Ljubljana Yüksek Mahkemesi ve ardından Temyiz Mahkemesi nezdinde itirazlarda bulunmuşsa da bu itirazları reddedilmiştir. Bu noktada Temyiz Mahkemesi'nin, Slovakya polisinin, başvurunun elektronik haberleşme trafik verilerini elde etmediği, yalnızca internete erişen belli bir kullanıcının bilgilerine ulaştığı yönündeki görüşü dikkat çekicidir.

Başvurucunun Anayasa Mahkemesi'ne yaptığı bireysel başvuru da Bilgi Komisyonu'nun yürürlükte olan Elektronik İletişim Yasası'nın hükümlerinin trafik veya kimlik verileriyle ilgili olup olmadıklarına bakılmaksızın, elektronik haberleşmeyle ilgili tüm verilerin bir mahkeme kararı gerektirdiğini ve iletişim halinde bulunan kişilerle ilgili verileri almak için polisin sadece yazılı talebini yeterli gören SCMK'nun ilgili hükmünün sorunlu olduğu görüşüne rağmen anayasal haklarının ihlal edilmediği gerekçesiyle reddedilmiştir. Anayasa Mahkemesinin bu kararına karşı Yargıç J. Sovdat tarafından muhalefet şerhi konmuştur:

- Yargıç J. Sovdat ilk olarak uygulanması gereken hükümlerin SCMK'ndan daha yeni tarihli olması nedeniyle Elektronik Haberleşme Yasası'nın ilgili hükümleri olduğunu ve bu hükümler gereğince de abonenin kimlik bilgilerine ulaşmak isteyen polisin mahkeme kararı alması gerektiğini belirtmiştir. Ayrıca Anayasa Mahkemesinin verdiği kararlar

trafik verilerini iletişim içeriğinden ayrı ve bağımsız olarak korumadığını bunun da hukuka uygun olmadığı kanaatine varmıştır. Bundan başka Anayasa Mahkemesinin iddia ettiği gibi başvurunun kendi adıyla kendisini kamuya açık hale getirmesi gibi bir durumun olmadığını ve bu açıklığın yalnızca IP adresleri rakamları üzerinden olduğunu vurgulamıştır.

- Yargıç Jadek Pensa da verdiği muhalefet şerhinde başvurunun internetteki anonimlik beklentisi üzerinde durmuştur. Buna göre başvuru kendi kimliğini ortaya çıkaracak verileri kamuya duyurmamıştır. Dolayısıyla bu verilerinin gizliliğini talep etme hakkına sahiptir. Bu kapsamda her ne kadar polisin talebini dayandığı SCMK hükmü mevcut olsa da; bu hüküm doğrudan elektronik iletişimin gizliliği ve bu gizliliğin korunması ile ilgili değildir ve özel kanun niteliğindeki Elektronik Haberleşme Yasası yürürlüktedir. Bu Yasa gereğince de iletişimin gizliliğine yalnızca yetkili bir makamın kararına dayanılarak müdahale edilebileceği öngörüldüğünden polisin mahkeme kararı alması gerektiği sonucuna ulaşılmıştır.

Böylece bütün iç hukuk yollarını tüketen başvuru Avrupa İnsan Hakları Sözleşmesi'nin gerçek kişilerin Mahkeme'ye başvurusunu düzenleyen "*bireysel başvurular*" başlıklı 34. maddesine dayanarak Slovenya Cumhuriyetine karşı özellikle Sözleşme'nin "*özel ve aile hayatına saygı hakkı*" başlıklı 8. maddesi olmak üzere haklarının ihlal edildiği iddiasıyla Mahkeme'ye başvurmuştur.

II. Kararın AİHS'nin 8. Maddesinin İhlali Açısından Değerlendirilmesi

AİHS'nin 8. maddesi ile herkesin özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkı koruma altına alınmıştır. Bir kamu makamının bu hakkın kullanılmasına 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.

Başvuru, polisin, dinamik IP adresiyle ilişkili abone verilerini elde ettiği ve bunun sonucunda keyfi bir şekilde, mahkeme kararı olmaksızın Sözleşme'nin 8. maddesine aykırı olarak kimliğinin ortaya çıkartıldığı ve dolayısıyla özel hayatının gizliliği hakkının ihlal edildiğini iddia etmiştir. Bu nedenle kararda 8. madde yönünden inceleme yapılmıştır.

A. Mahkeme, başvuru konusu olayı 8. madde kapsamında değerlendirmiştir

Sözleşme'nin 8. maddesi esasen doğrudan yalnızca kişinin özel ve aile hayatına saygı gösterilmesi hakkına yer vermiş olsa da bu hakkın dolaylı olarak diğer birçok hakkı etkilediği ve içerisinde barındırdığı açıktır. "Özel yaşam" ve "yazışmalar" birlikte, kişiler arası iletişimlerini devletin meraklı gözlerinden uzak tutma beklentisi de dahil olmak üzere, bireyin kimliğini bir insan olarak tanımlayan hemen hemen tüm nitelik ve davranışlar için hukuksal koruma sağlar. Mahkeme, çeşitli kararlarında özel hayat kavramının kişinin yalnızca özel alanıyla veya sır niteliğindeki bilgileriyle sınırlı olmadığını belirterek, özel hayatın kapsamının dar tutulmasını engellemek istemiştir.

Mahkeme konuyla ilgili olarak “özel hayat” kavramının kapsamlı bir tanımını yapmanın ne mümkün, ne de bu gayretin gerekli olduğu kanaatindedir. Bununla beraber 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 tutmanın aşırı kısıtlayıcı olacağını belirterek ve özel hayat hakkının belirli bir düzeye kadar başka insanlarla ilişkiler kurmayı ve bu ilişkileri devam ettirmeyi de içermesi gerektiği belirtmiştir. Buna göre AİHM özel yaşamın örneğin “diğer insanlarla ilişki kurmayı ve geliştirme hakkını” içermesi gerektiğini açıkça belirtmektedir².

Bunun yanında kişinin ismi³, etnik kimliği⁴, cinsiyet kimliği/cinsel hayatı⁵, fotoğraf ve görüntüleri⁶, kişisel verileri⁷, parmak izleri ve DNA profilleri⁸ ve tıbbi verileri⁹ de Mahkeme kararlarıyla özel hayat kapsamında ele alınmıştır. Mahkeme, polis talebi üzerine İçişleri Bakanlığı tarafından telefon konuşmalarının dinlenmesi şikayetiyle önüne gelen davada haberleşmeye ilişkin verilerin¹⁰ Sözleşmenin 8. maddesi kapsamında olduğu sonucuna ulaşmış ve özel hayata saygı hakkına müdahale olduğuna kesin kanaat getirmiştir¹¹.

İnceleme konusu kararda polis talebi üzerine bildirilen kişiye ait trafik verileri, haberleşmenin bir elektronik iletişim ağında iletilmesi için işlenmiş herhangi bir veridir ve IP adreslerinin bu trafik verilerine dahil olduğu açıktır. Servis sağlayıcı sadece kendisi ile abonelik sözleşmesi olan bir kişiyi tanımlayan veriyi polise vermiş olsa bile; böyle yaparak aslında kişi ile ilgili elektronik iletişim ağındaki trafik verilerini de vermiş olmaktadır. Böylece kişinin haberleşme verilerinin bildirilmiş olduğu olayın Sözleşme’nin 8. maddesi kapsamında değerlendirilip

² Bu yönde kararlar için bkz: “*Niemietz v. Almanya*”, B. No:13710/88, 16.12.1992; “*CostelloCostella – Roberts v. Birleşik Krallık*”, B. No:13134/87, 25.03.2003.

³ “*Burghartz v. İsviçre*” B. No:16213/90, 22.02.1994; “*Güzel Erdagöz v. Türkiye*” B. No: 37483/02, 21.10.2008.

⁴ “*Aksu v. Türkiye*” B. No: 4149/04 ve 41029/04, 15.03.2012; “*Mihai Ciubotaru v. Moldova*” B. No: 27138/04, 27.04.2010.

⁵ “*Van Kück v. Almanya*” B. No: 35968/97, 12.09.2003.

⁶ “*Van Hannover v. Almanya*” 59320/00, 24.06.2004; “*Reklos v. Yunanistan*” B. No: 1234/05, 15.01.2009.

⁷ “*Rotaru v. Romanya*” B. No: 28341/95, 04.05.2000.

⁸ “*S. ve Marper v. Birleşik Krallık*” Başvuru No. 30562/04 ve 30566/04, 04.12.2008; “*McVeigh, O’Neill ve Evans v. Birleşik Krallık*” B. No: 8022/77, 8025/77, 8027/77, 18.03.1981; “*Murray v. Birleşik Krallık*” B. No: 14310/88, 28.10.1994.

⁹ “*Chave née Jullien v. Fransa*” B. No: 14461/88, 09.07.1991.

¹⁰ “*Malone v. Birleşik Krallık*” B. No: 8691/71, 02.08.1984. Benzer yönde kararlar için bkz: “*P.G. ve J.H. v. Birleşik Krallık*” B. No: 44787/98, 25.09.2001; “*Vetter v. Fransa*” B. No: 59842/00, 31.05.2005.

¹¹ Nitekim Anayasa Mahkemesi kararlarında da haberleşme bilgilerinin özel hayat kapsamında değerlendirildiği görülmektedir. Bireyin elektronik iletişim araçları ile gizli kalacağına güvenerek yaptığı haberleşmelerin rızası dışında elde edilerek ve işlenerek aleyhinde kullanılması, kişinin Anayasa’nın “özel hayatın gizliliği ve korunması” başlıklı 20. maddesi ile “haberleşme hürriyeti” başlıklı 22. maddesi ile güvence altına alınan hakları kapsamında incelemeye tabi tutulmuştur. Uygulamada sıklıkla karşılaşılan çalışanlara ait haberleşme verilerinin elde edilerek çalışanların aleyhinde kullanılması durumu buna örnek gösterilebilir. Çalışanların e-posta hesabı üzerinden yaptığı iletişimin denetlenerek yazışmalarının ve dolayısıyla haberleşme bilgilerinin elde edilmesi durumu Anayasa Mahkemesi kararlarında başvuruçuların özel hayatının gizliliğine ve haberleşme özgürlüğüne olan müdahale sonucu karşılaştıkları yaptırımın orantılılığı ayrıntılı olarak ele alınmıştır. Ayrıca bu durumun AİHS’nin 8. Maddesi kapsamında şikayet konusu olduğu da belirtilmiştir. Bu yönde kararlar için bkz: AYM, *Tevfik Türkmen Başvurusu*, B. No: 2013/9704, 03/03/2016; AYM, *Hüseyin Yelkenci Başvurusu*, B. No: 2013/9706, 10/03/2016; AYM, *Hakan Erdoğan Başvurusu*, B. No: 2013/9481, 24/03/2016.

değerlendirilemeyeceğinin belirlenmesi için haberleşme verileri ile özel hayat ilişkisi belirlenmelidir. Yukarıda bahsedildiği gibi Mahkeme, önceki kararlarında haberleşme verilerini bu kapsamda ele almıştır.

Mahkeme, olaya ilişkin olarak, bir kişinin özel hayatının kendi evi veya özel mülkünün dışında kendisini etkileyecek tedbirler nedeniyle tehlikeye atılıp atılmadığının değerlendirilmesine dair bir dizi unsur olduğunu belirtmiştir. “Özel yaşam” ve “haberleşme” kavramlarının uygulanıp uygulanmayacağını tespit etmek için, bireylerin gizliliklerine saygı duyulması ve korunmasına dair makul bir beklenti içinde olup olmadıkları değerlendirilmelidir. Bu kapsamda somut olayda da söz konusu ağın kamuya açık olarak erişilebilir niteliği göz önünde bulundurulduğunda, başvurunun gizliliğine saygı gösterileceği ve korunacağı konusunda makul bir beklentisi olup olmadığı ele alınmalıdır.

Slovenya Anayasa Mahkemesi başvurunun makul gizlilik beklentisini değerlendirirken Razorback ağına katılmasını önemli bulmuştur. Çevrimiçi etkinliğini ve bağlantılı dinamik IP adresini bilerek hiçbir şekilde gizlememiş olan başvurunun kendisini bilinçli olarak kamuya açık hale getirdiğini ve bu nedenle meşru gizlilik beklentisi içinde olmadığı kanaatine varmıştır. Anayasa Mahkemesi’ne göre bu durumda başvurunun beklentisinin meşruluğundan bahsedilemeyeceği gibi daha da önemlisi bu beklentiden feragat ettiği dahi düşünülebilir.

Bununla birlikte AİHM, Anayasa Mahkemesi ile aynı fikirde olmayıp başvurunun kendi dinamik IP adresini gizlememiş olmasının, söz konusu beklentisinin makul olup olmadığının objektif olarak değerlendirilmesinde ölçü alınmaması gerektiğini düşünmektedir. Mahkeme esas alınması gerekenin başvurunun dinamik IP adresine ilişkin olan beklentisinin değil; kimliği hususundaki beklentisi olduğu kanaatindedir. Bu yönde yapılan incelemede başvurunun söz konusu çevrimiçi etkinliğinde kimliğini açıklamış olduğu ya da örneğin web sitesi sağlayıcısı tarafından bir hesap veya iletişim verileri aracılığıyla tanımlanabilir hususlarına ilişkin herhangi bir iddia mevcut olmadığından başvurunun aktivitesinin anonimlikle bağlantılı olduğu ve dolayısıyla kimliğini kamuya açık hale getirmiş olduğu gibi bir durumun olmadığı sonucuna ulaşmıştır.

Haberleşme verilerinin, yerleşik olduğu üzere, özel hayat kapsamında değerlendirilmekte olması ve haberleşme verileri rızası dışında alınan başvurunun bu verileri kamuya açık hale getirerek alenileştirmemiş olması dolayısıyla makul bir gizlilik beklentisi olabileceğinin anlaşılması nedenleriyle somut olayın Sözleşme’nin 8. maddesinin ihlali kapsamında değerlendirilmesi hukuka uygundur.

B. Başvuru konusu olayın 8. maddeye uygunluğunun değerlendirilmesi

Mahkeme, önüne gelen somut olayın özel hayat kapsamına dahil olduğu kanaatine vararak Sözleşme’nin 8. maddesinin uygunluğu açısından değerlendirmede bulunmuştur. Ben de, yukarıda detaylı olarak açıkladığım üzere başvurunun hukuka aykırı elde edilen haberleşme verilerinin, kimliğini ortaya çıkarması suretiyle gerçekleşen olaya 8. maddenin uygulanması gerektiğini düşünüyorum. Bundan sonra yapılması gereken başvurunun ilgili hakkının ihlal edildiği iddiasının incelenmesidir. Sözleşme’nin 8. maddesi kapsamında ele alınan somut

olayda, Hükümet'in iddia ettiği gibi bu maddeye uygun olarak mı hareket edilmiştir; yoksa başvurucunun özel hayatına saygı hakkı ihlal mi edilmiştir?

1. Başvurucunun hakkına müdahale olup olmadığı

Dava konusu olayın Sözleşme'ye uygun olup olmadığının incelenmesinin yapılabilmesi için ilk aşama başvurucunun ilgili hakkına müdahale olup olmadığının değerlendirilmesidir. Burada ilk olarak başvurucunun kimliğinin ortaya çıkarılmasının gerçekten özel ve aile hayatına saygı hakkına bir müdahale teşkil edip etmediği tespit edilmelidir.

Olayda polisin internet servis sağlayıcısı şirketi olan ISS'ye yaptığı talep üzerine edindiği ve başvurucunun kimliği ortaya çıkaran abonelik bilgilerinin kullanılması söz konusu olmuştur. Üstelik bu talep herhangi bir mahkeme kararı olmaksızın yerine getirilmiştir. Ancak özellikle iletişim araçları kullanılarak yapılan haberleşmelerde bireyler, bu verilerin gizliliklerine saygı duyulması ve korunmasına dair makul beklenti içerisinde olduklarıdır. Somut olayda da her ne kadar söz konusu ağ kamuya açık olarak erişilebilir nitelikte ise de başvurucunun kimliğinin ortaya çıkarılması konusunda herhangi bir rızası veya feragati olmadığı açıktır. Başvurucunun gizliliğine saygı gösterileceği ve korunacağı hususundaki makul bir beklentisinin olmasına karşılık; bu beklenti konusu veriler rızası dışında elde edilerek aleyhine kullanılmıştır. Bu kapsamda Mahkeme ile aynı yönde olarak başvurucunun Sözleşme'nin 8. maddesi ile korunan özel hayatın gizliliği, özel hayatın korunması, özel hayata saygı gibi kavramlardan faydalanamadığı ve belirtilen haklarına bir müdahalenin söz konusu olduğunu düşünmekteyim.

2. Başvurucunun hakkına yönelik olarak gerçekleştirilen müdahalenin meşruluğu

Başvurucunun abonelik bilgilerinin polise verilerek kimliğinin ortaya çıkartılması suretiyle gerçekleştirilen fiilin Sözleşme'nin 8. maddesine müdahale niteliğinde olduğu açıktır. Bununla birlikte temel hak ve özgürlüklere yapılan müdahaleler olayın oluş özelliklerine göre meşru kabul edilebilmektedir. Dolayısıyla her müdahalenin hukuka aykırı olduğu söylenemez ve bu hukuka aykırılığın varlığı ayrıca ele alınmalıdır. Gerçekleştirilen müdahalenin meşru olup olmadığının tespit edilebilmesi Sözleşmenin 8. maddesinin 2. fıkrasındaki gereksinimler doğrultusunda şu şekilde bir inceleme yapılmalıdır¹²:

- *Kanunla öngörülme*: Bu kavram, öncelikle uygulanan tedbirin iç hukukta yasal bir temeli olması gerektiğini ifade etmekle birlikte, yasanın içeriği ile de ilgilidir. Bu tedbirin ayrıca ilgili kişi tarafından ulaşılabilir nitelikte olması, kendi açısından doğacak sonuçların öngörülebilir olması ve hukukun üstünlüğü ilkesine uygun olması gerekir. Sözleşme ve AİHM içtihadı esas alındığında, Sözleşme'nin 8. maddesi kapsamında yapılacak bir müdahalenin meşruluğu, öncelikle söz konusu müdahalenin yasa uyarınca gerçekleştirilmesine bağlı olduğu görülmektedir. Müdahalenin, yasal olma şartını taşımadığının tespiti halinde ise Sözleşmenin 8. maddesinin (2) numaralı fıkrasında yer alan diğer ölçütlere bakılmaksızın, müdahalenin ilgili maddeye aykırı olduğu sonucuna ulaşılmaktadır¹³.

¹² "Özpinar v. Türkiye", B. No: 20999/04, 19.10.2010; "Yeşilgöz v. Türkiye", B. No: 45454/99, 20.09.2005.

¹³ "Bykov v. Rusya" B. No: 4378/02, 10.03.2009.

- *Meşru amaç:* Müdahalenin 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 halinde fiilin amacının meşruluğundan bahsedilecektir. Müdahalenin meşru kabul edilmesi için meşru bir amacı hedef alması zorunludur.
- *Demokratik bir toplumda gereklilik:* Son olarak incelenmesi gereken husus, yukarıda anılan meşru amaca ulaşmak için yapılan müdahalenin demokratik bir toplumda gerekli olup olmadığıdır. Demokratik bir toplumda gereklilik ölçütü ise müdahalenin “acil bir sosyal ihtiyaca cevap verip vermediği” ile “izlenen meşru amaçla orantılı olup olmadığı” yönünden inceleme yapılarak tespit edilir. Bu noktada dikkat edilmesi gereken gereklilik ölçütünün kime göre ele alınacağıdır. AİHM, gerekçelerin yeterli ve etkili olup olmadığı konusunda takdir hakkının kendisine ait olduğunu altını çizse de, müdahalenin gerekli ve ilgili olup olmadığı konusunda öncelikle değerlendirme yetkisinin ulusal mercilere ait olduğunu kabul etmektedir. Sözleşmeciler, bu bağlamda yargılamaya konu olan faaliyetin niteliği ve sınırlamanın amacına göre değişen bir takdir hakkından yararlanmaktadırlar¹⁴.

a. Abone bilgilerinin elde ediliş yöntemi bakımından yasaya uygunluk

Dava konusu olayda polis tarafından söz konusu dinamik IP adresi ile ilişkili abone bilgilerinin talep edilmesi SCMK’ya dayandırılmıştır. Buna göre ilgili hükümde sayılan şartların varlığı halinde polis, suçu ortaya çıkarmak için elektronik haberleşme ağının operatöründen bilginin ilgilisi olan kişinin rızası olmasa da bunları kendisine verilmesini yazılı olarak isteyebilecektir. Dolayısıyla mevcut olayda gerçekleştirilen müdahalenin iç hukukta bir temeli olduğu söylenebilir.

Buna karşın kanunla öngörülme ölçütünün varlığından bahsedebilmek için müdahale konusu fiilin kanun hükümleriyle belirtilmiş olması yeterli değildir. Kanunla öngörülmüş olma, müdahalenin iç hukuktaki kanun hükümleriyle öngörülmüş olmasının yanı sıra bu kanunun erişilebilir ve öngörülebilir olmasını ve ayrıca hukukun üstünlüğü ile uyumlu olmasını kapsar¹⁵. Öte yandan AİHM, bu iç hukukun uygulanma biçiminin Sözleşme’nin prensipleri ile uyumlu sonuçlar doğurup doğurmayacağı açısından da inceleme yapmak zorundadır. Dolayısıyla iç hukukta mevcut bir kanun hükmü söz konusu açılardan da ele alınacaktır.

Mahkeme, bir kanunun erişilebilir ve öngörülebilir olduğundan bahsedebilmek için ilgili hükmün bir kimsenin davranışını düzenlemesine imkân tanıyacak yeterli hassasiyetle formüle edilmesi gerektiğini vurgulamaktadır¹⁶. Öyleyse mevcut olayda müdahalenin dayanağını oluşturan hükmün objektif bir bakış açısıyla erişilebilir ve öngörülebilir olduğu söylenebilecektir. Buna karşılık hukukun üstünlüğü ile uyumlu olmak iç hukukun 8. maddeye ilişkin keyfî hak ihlallerine karşı yeterli koruma sağlamasını gerektirir¹⁷. Dolayısıyla

¹⁴ “Dudgeon v. Birleşik Krallık”, B. No: 7525/76, 22 .10.1981.

¹⁵ “Rotaru v. Romanya”, B. No:28341/95, 04.05.2000; “Liberty ve Diğerleri v. Birleşik Krallık”, B. No:58243/00, 1 Temmuz 2008.

¹⁶ Rotaru v. Romanya.

¹⁷ “Amann v. İsviçre” B. No: 27798/95, 16.02.2000.

Mahkeme'nin hukukun üstünlüğü ile uyumlu olduğu kanaatine varabilmesi için iç hukukta müdahaleye karşı yeterli ve gerekli güvencelerin bulunması zorunludur. Bu güvencelerin bulunması ise, uygulamayı haklı kılan gerekçeleri ve bu yetki ya da usulün kapsam ve sınırlarının çizilmesi demektir.

Dava konusu olayda, müdahale SMCK'nın ilgili hükmüne dayandırılmışsa da söz konusu hüküm dinamik IP adresi ile abone bilgisi arasındaki ilişki hakkında kesin kuralları içermemektedir. Ayrıca Slovenya Anayasası iletişim gizliliğine yönelik yapılacak bir müdahalenin ancak mahkeme kararıyla mümkün olabileceğini öngörmektedir. Öte yandan olay sırasında konuya ilişkin özel kanun hükmünde olan Elektronik İletişim Yasası ceza soruşturması için trafik verilerine erişmeye imkân tanıyan herhangi bir hüküm de içermemektedir. Dolayısıyla konuya ilişkin mevzuat bütünlük içerisinde değildir. Bu durumda Mahkeme hangi hükmün uygulanması gerektiğine karar verdiği takdirde ulusal mahkemelerin yerine geçecektir. Oysaki Mahkeme'nin niteliği itibarıyla böyle bir yetkisi bulunmamaktadır. Dolayısıyla bundan ziyade yerel mahkemelerin konuya bakış açısına eğilerek incelemesini yapmalıdır.

AİHM'in yerel mahkemelerin konuya ilişkin verdiği kararları değerlendirirken, Slovenya Anayasasının bu tür bir tedbir için mahkeme kararı gerektiğine dair hükmüne önem vermektedir. Buna göre iletişim halindeki bir kişinin kimliği, iletişimin gizliliğinin önemli yönlerinden biridir ve belirli bir dinamik IP adresi ile ilişkili abone bilgilerinin verilmesi, kural olarak mahkeme kararına tabidir; polisin basit bir yazılı talebi ile elde edilememelidir. Mahkeme ayrıca Anayasa Mahkemesi'nin başvurusunun gizliliğine ilişkin beklentisinden feragat ettiği görüşüne katılmamakta ve bunu gösteren herhangi somut bir delilin bulunmadığının altını çizmektedir. Öyleyse başvurusunun kimlik bilgilerinin gizli kalacağına yönelik makul bir beklentisinin mevcut olduğundan bahsedilebilir. Ayrıca somut olayda polisin, mahkeme kararı almasında elini kolunu bağlayan herhangi bir zorunluluk bulunmadığından, bu bilgilerin elde edilebilmesi için mahkeme kararı alınması şarttı.

Bütün bu açıklamalar ışığında Mahkeme, iç hukukun yersiz ve dahası keyfi müdahalelere karşı hiçbir koruma sağlamadığı kanaatine ulaşmıştır. Zira iç hukuk, internet servis sağlayıcılarının büyük çaptaki verileri polise vermek konusunda mecbur kılmış olmasına rağmen, olay anında polisin bu yetkisini kullanmasını denetleyecek bağımsız bir denetim mekanizması öngörmemiştir. Mahkeme'ye göre itiraza konu müdahalenin yasal dayanağı netlikten yoksundur ve 8. maddeye ilişkin olarak keyfi müdahalelere karşı yeterli koruma sağlanamamıştır. Böylece Mahkeme tarafından iç hukukun, hukukun üstünlüğü ilkesine uymadığı kanaatine ulaşıldığı görülmektedir.

b. Hukuka aykırı yöntemlerle elde edilen verilerin kullanımı sorunu

Hukukun üstünlüğü ilkesine uygun olmayan bir kanun hükmüne dayanarak abone bilgilerinin elde edilmiş olması ve Slovenya Anayasası'nda iletişimin gizliliğine yönelik müdahalelerin mahkeme kararı ile mümkün olabileceğini öngörülmüş olması, mevcut olayda kimlik bilgilerinin elde edilmesi için uygulanan yöntemin hukuka aykırı olduğu sonucunu doğurur. Bu noktada hukuka aykırı delil sorunu gündeme gelmektedir. Dolayısıyla Mahkemenin hukuka

aykırı yöntemlerle elde edilen bilgi ve bulguların yargılamanın herhangi bir aşamasında kullanılıp kullanılamayacağına ilişkin karar ve görüşlerine değinmek gerekir.

Mahkeme, bir delilin hukuka aykırı olması nedeniyle kabul edilebilirliğine ilişkin kendi görüşlerinin, ulusal mahkemelerin bu doğrultudaki görüşlerinin yerini alamayacağını ifade etmektedir. Buradan hareketle hukuka aykırı delil yasaklarına ilişkin tüm taraf devletlerin uyması zorunlu kural ve ilkeler ortaya koymaktan kaçınmıştır. Kendi değerlendirmesini ise yargılamanın adil olup olmadığı üzerinden yapmaktadır. Adil yargılanma hakkı Sözleşme'nin 6. maddesiyle güvence altına alınmış olmasına karşılık bu madde delillerin kabul edilebilirliğine ilişkin herhangi bir kural içermez. Bu nedenle bu sorunun çözümü ilk olarak ulusal mahkemelere bırakılmıştır. Ulusal mahkemelerin konuyla ilgili takdiri ise Mahkeme tarafından delil yasakları özelinde değil; davanın bütünü kapsamında genel bir değerlendirmeye tabi tutulmaktadır. Bunun tek istisnasını ulusal mahkemelerin kendilerine sunulan olgulara rağmen keyfi ya da ağır adaletsiz karar vermeleri hali oluşturur. Bununla birlikte Mahkeme her ne kadar konuya ilişkin takdir yetkisini ulusal mahkemelere bırakmışsa da; verdiği kararlarla iç hukuk düzeni ve mahkemeler için bağlayıcı veya en azından yol gösterici nitelikte olacağı kaçınılmazdır.

Mahkeme, hukuka aykırı delillerin başvuru aleyhinde kullanıldığı iddiasıyla önüne gelen olaylarda, delillerin sınıflandırılması veya belli delillerin hükme esas alınmaması gibi özel konularla ilgilenmeyip; başvuru hakkının adil yargılanma hakkının ihlal edilip edilmediğini yargılamaya bir bütün olarak bakarak tespit etmeye çalışmaktadır. Dolayısıyla Mahkeme'nin esas çıkış noktası yargılama sürecinin bir bütün olarak adil olup olmadığı noktasındadır¹⁸.

Mevcut olayda başvuru hakkının abonelik bilgileri, polis tarafından internet servis sağlayıcısı aracılığıyla hukuka aykırı bir şekilde elde edilmiş ve sonrasında başvuru hakkının bilgisayarlarına el konulmak suretiyle ulaşılan deliller hukuka aykırı bir şekilde elde edilen bu bilgiler ışığında söz konusu olabilmektedir. Polis, hukuka aykırı yöntemlerle elde ettiği bilgiler sayesinde yargılamaya esas oluşturan delillere ulaşmıştır.

Bu kapsamda dava konusu olayın Mahkeme tarafından hukuka aykırı delil kuramı açısından da incelenmesi gerekirdi. Ancak Mahkeme'nin hukuka aykırı delil ve adil yargılanma hakkı bakımından herhangi bir inceleme yaptığı görülmemektedir. Bunu bir eksiklik olarak görmekle beraber¹⁹ somut olayda bu açıdan bir inceleme yapmamasının nedenini polisin talebini bir

¹⁸ “Göfgen v. Almanya”, B. No: 22978/05, 01.06.2010; “Schenk v. İsviçre”, B. No: 10862/84, 12.07.1988; Bykov v. Rusya.

¹⁹ Nitekim AİHM'nin hukuka aykırı delil kuramına genel bakış açısını eleştirmekte ve bu konuda eksik kaldığını düşünmekteyim. Konuyla ilgili oldukça kapsamlı ve önemli somut olayları incelemiş olmasına rağmen hukuka aykırı delillerin kabul edilebilirliği değerlendirmesini yapmamış olması veya yapmakla birlikte kesin sonuçlara varmamış olması büyük bir eksikliktir. Her ne kadar Mahkeme'nin ulusal mahkemelerin yerine geçme gibi bir fonksiyonu olmadığı ve zaten olmaması da gerektiği konusunda Mahkeme ile aynı fikirde olsam da; Sözleşme'ye taraf devletlerin Mahkeme'nin içtihatları ile bağlı olduğu bir gerçektir. En azından taraf devletlerin kendi içinde yaptığı ulusal yargılamalarda Mahkeme içtihatlarının önemli bir yol gösterici olduğu açıktır. Oldukça tartışmalı bir konuyu oluşturan hukuka aykırı deliller sorununun çözümüne yardımcı olabilecek açık ve kesin kurallar koymak yerine kendi yetkisi olmadığı gerekçesiyle konuya ilişkin değerlendirme yapmaktan kaçınmasını ve yalnızca hukuka aykırı delillerin yargılamanın bir bütününe adil olmaktan çıkardığı zaman devreye girmesini doğru bir yaklaşım olarak değerlendirmiyorum. Mahkeme'nin

kanun hükmüne dayandırabilmiş olmasına bağlıyorum. Polisin internet servis sağlayıcısından abone bilgilerini talep etmesi ve internet servis sağlayıcısının bu bilgileri ilginin rızası olmaksızın polise bildirmesi gerçekten de yasal bir temelden yoksun değildir. Nitekim mevcut olaydaki sorun, adli makamların yasayla yasaklanan bir fiili veya yöntemi gerçekleştirmesi değildir. Polisin delil elde etmesini sağlayan bilgilerin elde edilişi ulusal kanun ile yasaklanmamıştır. Bununla birlikte temel alınan yasa konuya ilişkin yeterli açıklıkta olmadığı gibi; polisin yetkisinin kapsam ve sınırlarını da belirleyememiştir.

Ayrıca elde edilen abone bilgileri iletişimin gizliliği ve korunması hakkı kapsamında ele alınmaktadır. Slovenya Anayasa'sında bu hakka yönelik müdahalelerin mutlak surette bir mahkeme kararına dayanması gerektiğine yönelik hüküm bulunmamaktadır. İletişim halindeki kişinin kimlik bilgileri ise bu hakkın sağlanabilmesi için korunması gerekli en önemli unsurlardan biridir. Dolayısıyla iletişim halindeki bir kişinin kimlik bilgilerine yönelik müdahalenin de mahkeme kararı ile gerçekleştirilmesi gerekirdi.

Bu açıklamalar ışığında, mevcut olayda, esas sorunun temel alınan yasanın belirsiz olması ve hangi yasanın üstün gelerek uygulanması gerektiğinin tespit edilememiş olmasıdır. Bu nedenle Mahkeme, ulusal mahkemelerin vardığı kararlarda sunduğu gerekçeler ve konuya olan bakış açısı temelinde inceleme yapmayı uygun görmüştür. Buna karşılık, kanaatim yine de Mahkeme'nin hukuka aykırı yöntemlerle elde edilen bilgiler aracılığıyla ulaşılan deliller bakımından da inceleme yapması gerektiği yönündedir.

c. Kişisel verilerin korunmasına ilişkin mevzuat bakımından hukuka aykırılık

Başvurucunun şikayet konusu ettiği bilgilerinin haberleşme verilerini içerdiği ve bu verilerin kişisel veri niteliğinde olup; kişisel verilerin de Sözleşme'nin 8. maddesinde belirtilen özel hayat kavramı altında incelendiğini yukarıda detaylı bir şekilde açıkladım. Nitekim madde metninde geçen “yazışma” ibaresi iletişim bilgilerinin de bu noktada korunduğuna işaret etmektedir. Mevcut olayda ilgilinin rızası olmaksızın elde edilen bilgilerin başvurucunun özel hayatına ilişkin bilgiler olduğu noktasında tartışma bulunmamakla birlikte, bu bilgilerin özelde kişisel verisi niteliğinde olması; müdahalenin kişisel verilerin korunması bağlamında hukuka uygunluğunun da tespit edilmesini gerektirir.

İlk olarak Slovenya, 1981 tarihinde imzaya açılan ve bütün Avrupa Konseyi üye devletleri tarafından onaylanan “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*”ne taraf olup; bu Sözleşmeyi 1994 tarihinde yürürlüğe koymuştur. Esas amacı bütün üye ülkelerde gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik bilgi işleme tabi tutulması karşısında haklarını güvence altına almak olan Sözleşmeyle, kişisel verilerin korunması, özel hayatın gizliliğinden

konuya ilişkin olarak detaylı ve kapsamlı bir değerlendirme yapması ve belirli, açık ve kesin kurallar koyması halinde konunun taraf devletler açısından da daha anlaşılabilir hale geleceğini düşünüyorum. Konuyla ilgili detaylı bilgi için bkz: **Murat Volkan Dülger**, Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara, Seçkin Yayıncılık, 2014, s.103-105; **Murat Volkan Dülger**, “Avrupa İnsan Hakları Mahkemesi'nin Gäfgen Kararı Bağlamında Ceza Muhakemesinde İşkence Tehdidi ile Elde Edilen Delillerin Kullanımı Sorunu”, Türkiye Barolar Birliği Dergisi, Y.26, S.111, 2014, s.325-410.

ayrı bir hak olarak değerlendirilmiş ve ülkelere konuyla ilgili düzenleme yapma yükümlülüğü getirilmiştir.

2001 tarihinde imzaya açılan “Avrupa Konseyi Siber Suç Sözleşmesi” de 2005 yılından bu yana Slovenya’da yürürlüktedir. Bu sözleşmenin mevcut olay açısından önemli yanları şu şekildedir:

- Sözleşme’de trafik verisi detaylı olarak tanımlanmış olup; “*bir bilgisayar sistemi aracılığıyla gerçekleşen iletişimle ilgili olan, iletişim zincirinin bir halkasını teşkil eden bilgisayar sistemi tarafından üretilmiş, iletişimin başlangıç noktasını, hedefe varış noktasını, izlediği yolu, saatini, tarihini, boyutunu, süresini veya iletişimde kullanılan temel hizmetin türünü gösteren herhangi bir bilgisayar verisini*” ifade eder. Dolayısıyla dinamik bir IP adresine ilişkin verilerin bu kapsamda trafik verisi olması gerekir. Bu veri ayrılmaz bir şekilde belirli bir iletişim ile bağlantılı olduğu için trafik verisi de iletişim gizliliğinin korumasından yararlanmalıdır.
- Sözleşme ile taraf ülkelere çocuk pornografisinin suç olarak düzenlenmesi yükümlülüğü getirilmiştir.
- Sözleşme, bir ceza soruşturmasında abone bilgilerinin gerekli olabileceğini ve bu hallerde toplanabileceğini kabul etmekle beraber; yasa uygulayıcı makamların, içerik verilerinin alınması ve gerçek zamanlı trafik verilerinin toplanması gibi önlemler yerine uygulayabilecekleri daha az müdahaleci ve daha az zorlu bir önlem almayı sağlamaktadır. Ayrıca belirtilen önlemler ağır nitelikteki suçlarla sınırlandırılmıştır.

Avrupa Birliği’ne üye olan Slovenya, “95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” ile 25 Mayıs 2018 tarihi itibarıyla yürürlükte olan “2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)” ile bağlıdır. Kişisel verilerin korunması alanına ilişkin temel uluslararası mevzuatlara üye olan Slovenya, ulusal hukukunu söz konusu Direktif ve Tüzük’e uygun olarak oluşturmak ve ayrıca ulusal yargılamalarında bunlara uyumlu hareket etmek zorundadır. Dolayısıyla Slovenya’nın Direktif ve Tüzük hükümlerinde öngörülen korumayı kendi iç hukukunda sağlaması gerekir. Bu noktada her iki metnin de, özellikle Tüzük ile getirilen korumanın oldukça geniş kapsamlı olduğunu belirtmek gerekir.

Slovenya’nın ulusal hukukuna baktığımız zaman 95/46/EC sayılı direktifi esas alarak özel bir “Kişisel Verilerin Korunması Yasası”nın 2004 yılından bu yana yürürlükte olduğu görülür. Yasa’da “*ifade ediliş tarzına bakılmaksızın kişilerle ilgili her türlü veri*” olarak tanımlanan kişisel verilerin yasal ve adilane bir biçimde işlenmesi gerektiği Yasa’nın 2. maddesiyle öngörülmektedir. Ayrıca kişisel verilerin, yasaların düzenlemesi veya ilgili kişinin rızası temelinde işlenebileceği hüküm altına alınmıştır. Dolayısıyla bu Yasa uyarınca kişisel veriler yalnızca öngörülmüş yasal amaçlar için toplanabilecek ve bu doğrultuda yalnızca bu amaçların gerçekleştirilmesi için gerekli olduğu hallerde işlenebilecektir.

Slovenya’nın kişisel verilerin korunmasına ilişkin tabi olduğu uluslararası mevzuat ile kendi iç hukukuna bakıldığı zaman kişisel verilerin geniş ve kapsamlı bir korumadan faydalandırıldığı görülmektedir. Mevcut olayda veri sahibinin rızası alınmaksızın polise bildirilen abone bilgilerinin, başvurusunun kişisel verisi niteliğinde olduğu konusunda herhangi bir tereddüt bulunmamaktadır. Öyleyse söz konusu bilgilerin polis tarafından talep edilmesi, internet servis

sağlayıcısının bu bilgileri polise bildirmesi ve polisin bu verileri toplaması ve işlemesi esnasında yukarıda sayılan kişisel verilerin korunması mevzuatına uyumlu olarak hareket edilmek zorundadır. Bununla birlikte olayda, kişisel verilerin söz konusu olduğu bu aşamalardan daha ilk aşamadan bu yana, kişisel verilerin konuya ilişkin mevzuata uygun bir talebe konu olduğu söylenememektedir. Yalnızca yasayla öngörölmüş yasal amaçlar için kişisel verilerin toplanabileceğini öngören Kişisel Verilerin Korunması Yasası esas alındığında buna uygun hareket edilmediği açıktır. Mahkeme'nin de belirttiği gibi polisin kişisel veri elde etme talebi açıkça dayanaktan yoksun olmasa da; açık, belirli ve sınırları çizilmiş bir yasa hükmüne dayanmamaktadır. Dolayısıyla meşru bir kişisel veri işleme faaliyetinden söz edilmesi mümkün değildir. Bu kapsamda başvurunun Slovenya'nın taraf olduğu uluslararası hukuk ile kendi iç hukuku hükümlerine istinaden kişisel verilerin korunması hakkında gerektiği gibi faydalanmadığı ve bu hakkına müdahale edildiği söylenebilir.

Sonuç

Yukarıda incelemiş olduğum karar, kişisel verilerin yoğun bir biçimde hukuka aykırı faaliyetlere konu edildiği günümüzde yapılan değerlendirme ve Mahkeme'nin bakış açısını anlayabilmek açısından oldukça önemlidir. Hukuka aykırı yöntemler kullanılarak elde edilen ve kişisel veri içeren bilgi ve belgelerin yargı makamları nezdinde kullanılmasının yaygınlaşması ve kişisel veri sahibinin buna karşılık haklarının ihlal edildiğini ileri sürmesi, konunun sıklıkla mahkemeler önüne gelmesine neden olmuş ve mahkemeler aracılığıyla çözüme kavuşturulmasını gerekli kılmıştır.

AİHM'in de bu kapsamda yakın tarihte vermiş olduğu söz konusu kararı, konunun daha iyi anlaşılmasını mümkün kılacağından geçmiş kararları da dikkate alınarak çalışma konusu edilmiş ve yapılan değerlendirme sonucu şu sonuçlara varılmıştır:

- Başvurucunun adli makamların yürüttüğü izleme faaliyeti sonucunda pornografik materyallerin teşhir edilmesi, üretilmesi, bulundurulması ve dağıtılması suçunu işlediğinin tespit edilmesi ile ilgili olan dava konusu olay; dinamik IP adresi aracılığıyla herhangi bir mahkeme kararı olmaksızın abone bilgilerinin ve dolayısıyla kimliğinin ortaya çıkartılması başvuru tarafından Sözleşme'nin 8. maddesi ve diğer hakları ihlal edildiği iddiasıyla AİHM nezdinde inceleme konusu edilmiştir.
- Mahkeme, haberleşme verilerinin yerleşmiş olduğu üzere özel hayat kapsamında değerlendirilmesi nedeniyle somut olayı özel hayatın ihlali açısından ele almış ve olayın 8. maddeyi ihlal edici nitelikte olup olmadığını incelemiştir.
- Bu inceleme kapsamında ilk olarak başvurunun gizliliğine saygı gösterileceği ve korunacağı hususundaki makul bir beklentisinin olmasına karşılık; bu beklenti konusu veriler rızası dışında elde edilerek aleyhine kullanılmasının ilgili hakkına müdahale sonucunu oluşturduğuna kanaat getirmiştir.
- Mahkemenin özel hayata müdahale incelemesinde “gizliliğe saygı gösterileceği ve korunacağına ilişkin makul beklenti” ölçüsünü esas almasının yanı sıra bu beklentinin hangi hallerde var olup olmadığını belirleyecek ölçütlere yer vermesi önemlidir. Bireyin gizliliğine yönelik beklentisinin olmadığı sonucuna ulaşmak için bu beklentiden açıkça feragat edildiğini görmek istemiştir. Böylece açıkça anlaşılmadığı sürece bireyin

gizliliğine ilişkin makul bir beklentisi olduğu kabul edilerek; keyfi bir biçimde bireyin beklentisi olmadığı sonucuna ulaşılmasını yaratacağı tehlikeler önlenmek istenmiştir. Nitekim Slovenya Anayasa Mahkemesi, başvurunun gizlilik beklentisi olmadığına dair herhangi bir somut hareketi olmamasına rağmen, başvurucuyu kendini kamuya açık hale getirerek bu gizlilikten feragat ettiği düşüncesiyle yargılamaya tabi tutarak keyfi bir uygulamada bulunmuştur. Oysaki kişinin özel hayatına ilişkin değerlendirmede bulunurken dikkatli olunması gerektiği ve açıkça anlaşılmadığı sürece kişinin kimlik bilgilerinin ortaya çıkarılmasına rıza göstermesinin söz konusu olamayacağı açıktır. Mahkemelerin benzer konulu yargılamalarda AİHM'nin bu görüşünden hareket etmesi kişinin gizliliği ve mahremiyetinin sağlanabilmesi açısından faydalı olacaktır.

- AİHM, Sözleşme ile koruma altına alınan haklara yönelik olarak gerçekleştirilen müdahalelerin meşru olup olmadığı incelemesini “*kanunla öngörülme*”, “*meşru amaç*” ve “*demokratik toplumda gereklilik*” ölçütlerini esas alarak gerçekleştirmektedir.
- Kanunla öngörülmüş olma, müdahalenin iç hukuktaki kanun hükümleriyle öngörülmüş olmasının yanı sıra bu kanunun erişilebilir ve öngörülebilir olmasını ve ayrıca hukukun üstünlüğü ile uyumlu olmasını kapsar.
- Bir kanunun erişilebilir ve öngörülebilir olduğundan bahsedebilmek için ilgili hükmün bir kimsenin davranışını düzenlemesine imkân tanıyacak yeterli hassasiyetle formüle edilmesi gerekir.
- Hukukun üstünlüğü ile uyumlu olmak ise iç hukukun 8. maddeye ilişkin keyfi hak ihlallerine karşı yeterli koruma ve güvence sağlamasını gerektirir. Bu güvencelerin bulunması, uygulamayı haklı kılan gerekçeleri ve bu yetki ya da usulün kapsam ve sınırlarının çizilmesi demektir.
- Somut olayda her ne kadar abone bilgilerinin elde edilmesinin dayandığı kanun hükmünde erişilebilir ve öngörülebilir olmak bakımından sorun bulunmamaktaysa da; bu hüküm hukukun üstünlüğü ile uyumlu olma noktasında gerekli koşulları taşımamaktadır. Hüküm, dinamik IP adresi ile abone bilgisi arasındaki ilişki hakkında kesin kuralları içermediği gibi; polise verdiği yetkiyi denetleyebilen bağımsız bir denetleme mekanizması da oluşturamamıştır. Dolayısıyla müdahalenin dayandığı hüküm, Mahkeme'nin aradığı nitelikte bir hüküm değildir. Bu nedenle de hukukun üstünlüğü ilkesi ile uyuşmayan bir hükme dayanarak gerçekleştirilen müdahalenin meşruluğundan bahsedilemez.
- Hukukun üstünlüğü ilkesine uygun olmayan bir yasa hükmüne dayanarak abone bilgilerinin elde edilmiş olması ve Slovenya Anayasası'nda iletişimin gizliliğine yönelik müdahalelerin mahkeme kararı ile mümkün olabileceğinin öngörülmüş olması, mevcut olayda kimlik bilgilerinin elde edilmesi için uygulanan yöntemin hukuka aykırı olduğu sonucunu doğurur. Olay, bu açıdan hukuka aykırı delil kuramı bakımından önem arz etmesine rağmen; Mahkeme bu açıdan bir değerlendirme yapmayarak önceki kararlarında belirttiği görüşlerini sürdürmüş ve delil yasaklarını tartışmaktan kaçınmıştır. Ancak bana göre bu durum, AİHM gibi bağlayıcı ve yol gösterici bir yargı makamının eksikliğini oluşturur.
- Başvurucunun şikâyet konusu ettiği bilgilerinin haberleşme verilerini içermesi ve bu verilerin kişisel veri niteliğinde olması nedeniyle, inceleme konusu karar, özel hayat

kavramının yanında zamanla daha fazla önem kazanan ve tek başına bir hak olma özelliğini kazanan kişisel verilerin korunması hakkı açısından da önemlidir. Mahkeme'nin bu bilinçle, kişisel veriler özelinde ayrıca bir inceleme yapmasa da, kişisel verilere ilişkin mevzuata yer vererek haberleşme verilerinin niteliğinden bahsetmesi ve kişisel verilerin önemine değinmesi faydalı olmuştur.

Günümüzde özellikle teknolojinin getirdiği yenilikler sonucu hayatımıza giren elektronik uygulamalar nedeniyle kişisel verilerin daha çok ortada olduğu ve bireylerin daha şeffaf hale geldiği bir dönemde yaşıyoruz. Öyle ki çoğu zaman kişisel verilerimizi bizzat kendi elimizle sunuyoruz. Böylece özel hayatın gizliliği ve korunması hakkı gün geçtikçe ve hiç olmadığı kadar tehlike altına girmekte ve korunmaya ihtiyaç duymaktadır. Bu ihtiyaç, her ne kadar neredeyse tüm ülkeler tarafından fark edilerek uluslararası ve ulusal birçok yasal düzenlemeyle giderilmeye çalışılsa da, bireylerin tam bir güvenceye sahip olduğundan bahsedebilmek için uygulamada da yargı makamları tarafından bireylerin verilerinin gereken korumadan yararlandırılarak karar verilmesi zorunludur. İnceleme konusu karar da tam bu açıdan önem arz eden ve yol gösterici nitelikte bir karardır.

Elektronik iletişim araçlarının gündelik faaliyetlerden mesleki faaliyetlere kadar yaşamın her alanında aktif olarak kullanıldığı günümüzde, bu araçlar kullanılarak söz konusu olan kişisel veriler de etkin bir korumaya sahip olmalıdır. Bireylerin iletişim ve haberleşme gizliliğine yönelik hangi hallerde müdahalenin söz konusu olabileceğinin yanı sıra bu müdahalenin nasıl ve ne şekilde yapılacağı ile sınırlarının ne olacağı açıkça belirlenmelidir. Ayrıca müdahale yetkisine sahip organın, bağımsız bir organ tarafından denetlenerek bu yetkinin belirlendiği gibi kullanılıp kullanılmadığı tespit edilmelidir. İletişim verileri açısından, bireylerin özel hayat, haberleşmenin gizliliği ve kişisel verilerin korunması hakları ancak bu şekilde tam bir korumaya sahip olabilir.