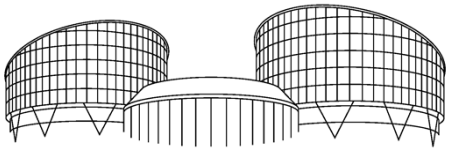

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

AVRUPA İNSAN HAKLARI MAHKEMESİ

DÖRDÜNCÜ DAİRE

BENEDIK / SLOVENYA KARARI

(Başvuru No. 62357/14)

KARAR

STRAZBURG

24 Nisan 2018

İşbu karar Sözleşme'nin 44 § 2 maddesinde belirtilen koşullar çerçevesinde kesinleşecek olup şekli bazı değişikliklere tabi tutulabilir

Benedik / Slovenya Davasında,

Başkan Ganna Yudkivska,
Hakimler ;
Vincent A. De Gaetano,
Faris Vehabović,
Carlo Ranzoni,
Georges Ravarani,
Marko Bošnjak,
Péter Paczolay, ,
ve *Sekreter Yardımcısı* Andrea Tamietti'nin katılımıyla Daire halinde toplanmış olan Avrupa İnsan Hakları Mahkemesi (Dördüncü Daire), 20 Mart 2018 tarihinde gerçekleştirilen kapalı müzakereler sonrasında, aynı tarihte aşağıdaki kararı vermiştir:

USUL

1. Davanın temelinde, Igor Benedik tarafından İnsan Hakları ve Temel Özgürlüklerin Korunmasına ilişkin Sözleşme'nin ("Sözleşme") 34. maddesine göre Slovenya Cumhuriyetine karşı yapılan (no. 62357/14) başvuru bulunmaktadır.

2. Başvurucu, Ljubljana'da bir avukat olan Bay M. Jelenič Novak tarafından Mahkeme önünde temsil edilmiştir. Slovenya Hükumeti ("Hükumet") kamu avukatı olan kendi görevlisi Bayan J. Morela, tarafından temsil edilmiştir.

3. Başvurucu, özellikle, Sözleşme'nin 8. maddesi uyarınca, polisin, yasadışı olarak internet servis sağlayıcısından kimliğinin ortaya çıkmasına neden olacak şekilde bilgi topladığından bahisle haklarının ihlal edildiğini iddia etmiştir.

4. Başvuru, 8 Nisan 2015 tarihinde Hükümet'e bildirilmiştir.

OLAY VE OLGULAR

I. DAVANIN KOŞULLARI

5. Başvurucu 1977 doğumlu olup Kranj' da yaşamaktadır.

A. Soruşturma

6. 2006 yılında Valais Kantonu adli makamları sözde "Razorback" ağının kullanıcılarına yönelik bir izleme faaliyeti yürütmüştür. İsviçre polisi, bazı kullanıcıların resim veya video biçiminde çocuk pornografisi içeriklerini bulundurduklarını ve bunları paylaştıklarını tespit etmiştir. Yasadışı içerik barındıran dosyalar, bağlı bilgisayarlardan her birinin hem kullanıcı hem de sunucu olarak işlev gördüğü "p2p" (eşler arası) dosya paylaşım ağı aracılığıyla paylaşılmıştır. Bu nedenle, her kullanıcı ağdaki diğer kullanıcılar tarafından paylaşılmak üzere sunulan tüm dosyalara erişebilir ve bunları kendi kullanımı için indirebilmektedirler. İsviçre polisi tarafından tespit edilen dinamik İnternet Protokolü ("IP") adresleri arasında, daha sonra başvurucu ile bağlantılı olan bir dinamik IP adresi de tespit edilmiştir.

7. İsviçre polisi tarafından elde edilen verilere dayanarak, 7 Ağustos 2006 tarihinde, Slovak polisi bir mahkeme kararı almadan, bir Slovenya İnternet servis sağlayıcısı şirketi olan S.'den (bundan böyle "İSS" olarak anılacaktır) yukarıda belirtilen IP adresinin 20 Şubat 2006 tarihinde saat 13.28'de tahsis edilen kişiye ait verileri bildirilmesini talep etmiştir. Polis, talebini Slovenya Ceza Muhakemesi Kanunu'nun 149b (3) Maddesindeki hükümlere (bundan sonra "SCMK" olarak anılacaktır, aşağıdaki paragraf 36'ya bakınız) dayandırmıştır. Anılan maddede, elektronik haberleşme ağları operatörlerinin, ilgili dizinde detaylı bilgileri bulunmayan elektronik iletişim araçlarının kullanıcı veya sahipleri ile ilgili bilgileri polise bildirmesi öngörülmektedir. Polisin bu talebi üzerine, 10 Ağustos 2006 tarihinde, İSS, söz konusu IP adresiyle ilgili İnternet hizmetine abone olan başvurucunun babasının adını ve adresini polise vermiştir.

8. Polis, 12 Aralık 2006 tarihinde Kranj Bölgesi Savcılığından, Kranj Bölge Mahkemesi sorgu hakiminden[1] İSS'nin hem söz konusu IP adresi abonesinin kişisel bilgilerini ve bu IP adresine bağlı trafik verilerini bildirmesi hususunda karar vermesi için talepte bulunmasını istemiştir. 14 Aralık 2006 tarihinde, SCMK'nın 149b (1) maddesi uyarınca bu hususstaki mahkeme kararı alınmış ve İSS, polise talep edilen verileri vermiştir.

9. 12 Ocak 2007'de Kranj Bölge Mahkemesi sorgu hakimi, başvurucunun ailesine ait evin aranması hususunda arama kararı vermiştir. Bu hakim kararı şüpheli olmasından dolayı başvurucunun babasına yöneliktir. Ev arama sırasında polis ve Kranj Bölge Mahkemesi sorgu hakimince dört bilgisayara el konulmuş ve daha sonra sabit disklerin kopyası çıkartılmıştır

10. Başvurucunun aile üyeleri ile yapılan diyalog sonrası herhangi bir kayda rastlanılmaması nedeniyle polis suçlamaları başvurucuya yöneltmiştir.

11. Sabit disklerin incelenmesi sonucu polis, çocuklarla ilgili pornografik materyaller bulunan bir dosya tespit etmiştir. Polis, başvurucunun, diğer kullanıcılardan farklı dosyalar indirebildiği ve kendi dosyalarını otomatik olarak sunduğu ve paylaştığı eMule isimli dosya paylaşım programını

[1] Çevirmen Notu: Sorgu Hakimliği müessesesi Türk Hukukunda bulunmamakla birlikte kararda bahsi geçen arama, el koyma, iletişimin denetlenmesi gibi kararlar sulh ceza hakimliği tarafından verilmektedir.

bilgisayarlardan birine kurduğunu tespit etmiştir. Başvurucu tarafından indirilen dosyalar arasında küçük bir oranda çocuk pornografisi yer almıştır.

12. Kranj Bölge savcısı 26 Kasım 2007 tarihinde başvurucu aleyhinde adli soruşturma açılmasını talep etmiştir.

13. Başvurucu, sorgu hakimliğindeki savunmasında, diğer savunmalarının yanı sıra, söz konusu dosyaların içeriğinin farkında olmadığını iddia etmiştir. Ayrıca, İSS'nin hukuksuz bir şekilde, mahkeme kararı olmaksızın, adresini de içeren verileri polise verdiğini öne sürmüştür.

14. 5 Mart 2008 tarihinde Kranj Bölge Mahkemesi sorgu hakimi, başvurucuya karşı, Ceza Kanunun 187 (3). Maddesi kapsamında pornografik materyallerin teşhir edilmesi, üretilmesi, bulundurulması ve dağıtılması suçunu işlediğine dair makul bir şüpheye dayanarak adli soruşturma başlatmıştır. Hakim, diğer şeylerin yanı sıra, başvurucunun babasının belirlenen IP adresinin sahibi olduğunu ve başvurucunun "Benet" adı altında ilgili programa giriş yaptığı iddiasına değinmiştir.

15. 17 Mart 2008 tarihinde başvurucunun avukatı, adli soruşturma açma kararına itiraz etmiştir. Diğerlerinin yanı sıra, ilgili IP adresi kullanıcısının kimliğine ilişkin delillerin yasa dışı bir şekilde elde edildiğini iddia etmiştir. Bu bilgi, trafik verisi ile ilgili olup dolayısıyla mahkeme kararı olmadan elde edilmemelidir.

16. 21 Mart 2008 tarihinde mahkemenin geçici heyeti, avukatın IP adresinin kimliğinin hukuka aykırı şekilde ele geçirilmiş olduğunu iddia etmesine rağmen, bazı belgelerin dosyadan çıkarılmasını talep etmediği gerekçesi ile itirazın reddine karar vermiştir.

B. Yargılama

17. 29 Mayıs 2008 tarihinde, Kranj Bölgesi Eyalet Savcılığı, yukarıda belirtilen suçu isnat ederek başvurucu hakkında bir iddianame düzenlemiştir.

18. 8 Ekim 2008 tarihli duruşmada, başvurucu, mahkeme kararı olmadan elde edilen söz konusu IP adresi kullanıcısı ile ilgili bilgileri içeren ve yasa dışı yollarla elde edilen delillerin dosyadan çıkarılması için yazılı bir talepte bulunmuştur.

19. 5 Aralık 2008 tarihinde, mahkeme, söz konusu IP adresinin kullanıcısına ilişkin verilerin, SCMK'nin 149b (3) maddesine uygun olarak elde edildiği tespiti ile başvurucunu talebini reddetmiştir.

20. 5 Aralık 2008 tarihinde Kranj Bölge Mahkemesi başvurucuyu, isnat edilen suçtan dolayı suçlu bulmuştur. Bir bilgisayar bilimi uzmanının görüşüne dayanarak, Bölge Mahkemesi, başvurucunun çocuklarla ilgili p2p ağları üzerinden indirdiği ve diğer kullanıcılara paylaşıma açtığı 630 pornografik resim ve 199 videodan haberdar olması gerektiğine karar

vermiştir. Başvurucu, sekiz ay hapis cezasına çarptırılmış ve cezası iki yıllık bir deneme süresiyle ertelenmiştir.

C. Ljubljana Yüksek Mahkemesi Önündeki Yargılama

21. Hem başvurucu, hem de bölge savcısı ilk derece mahkemesi kararını temyiz etmiştir. Başvurucu, Bölge Mahkemesi tarafından kabul edilen gerçeklere itiraz etmiştir. Ayrıca, başvurucu, Slovenya polisinin mahkeme kararı olmadan abone bilgilerini elde ettiğini ve dolayısıyla yasa dışı olması nedeniyle delil olarak kabul edilmemesi gerektiğini iddia etmiştir. Sonuç olarak, bu tür yasal olmayan yollarla elde edilen verilere dayanan tüm deliller reddedilmelidir.

22. 4 Kasım 2009 tarihinde Ljubljana Yüksek Mahkemesi, bölge savcısının temyizini kısmen kabul ederek, başvurucunun erteli cezasını altı ay hapis cezasına çevirmiştir. Başvurucunun temyiz başvurusu temelden yoksun olduğu gerekçesi ile reddedilmiştir. Yüksek Mahkeme, ilk derece mahkemesinin davanın esaslarını doğru şekilde tespit ettiğini teyit etmiştir; üstelik bu tür bir amaç için mahkeme kararı gerekmediğini, IP adresini kullanan ile ilgili verilerin yasal olarak elde edildiğine karar vermiştir.

D. Yargıtay Önündeki Yargılama

23. Başvurucu, kullanıcı oturum her açtığında bilgisayara yeni bir IP adresi atanması nedeniyle, bir dinamik IP adresinin bir telefon rehberinde girilmemiş bir telefon numarası ile karşılaştırılamayacağını yineleyerek Yargıtay nezdinde kanun hükmüne ilişkin bir temyiz talebinde bulunmuştur. Buna göre, bu tür veriler, elektronik iletişime bağlı olan ve iletişimin gizliliğinin korunmasını sağlayan koşulları ve durumları oluşturan trafik verileri olarak kabul edilmelidir. Başvurucu, İsviçre polisinin mahkeme kararı olmadan söz konusu dinamik IP adresini alamaması ve Slovenya polisinin de IP adresiyle ilişkili abonenin kimliğine ilişkin verileri böyle bir mahkeme kararı olmadan elde edememesi gerektiğini ileri sürmüştür.

24. Yargıtay, 20 Ocak 2011 tarihinde, web sitelerinin genel erişilebilirliği ve İsviçre polisinin, İnternet trafiğine herhangi bir özel müdahalede bulunmadan basitçe p2p ağındaki veri alışverişini, belirli içerikleri paylaşan kullanıcıları izleyerek kontrol edebildiği, yani internet trafiğine herhangi bir müdahalede bulunmadığı, dolayısıyla böyle bir iletişimin gizli olarak kabul edilemeyeceği ve Anayasa'nın 37. maddesi ile korunmadığı gerekçesi ile başvurucunun temyizini hukuki açıdan reddetmiştir. Buna ek olarak Yargıtay'ın görüşüne göre, Slovak polisi başvurucunun elektronik haberleşmesiyle ilgili trafik verisi elde etmemiş, sadece internete erişilen belirli bir bilgisayarın kullanıcısı ile ilgili verileri elde etmiştir.

E. Anayasa Mahkemesi Önündeki Yargılama

25. Başvurucu, alt mahkemeler nezdinde sunulan şikayetlerini yineleyerek Anayasa Mahkemesi nezdinde bireysel başvuruda bulunmuştur.

26. Anayasa Mahkemesi Bilgi Komiserinden konuyla ilgili görüşün sunmasını istemiştir. Bilgi Komiseri bir elektronik iletişim kullanıcısının kimliğinin tespit edilmesinin nedenin, tam olarak az ya da çok kamuya açık web siteleri aracılığıyla kişilerin iletişim kurması olduğu görüşündedir. Bilgi Komisyonu'nun görüşüne göre, trafik verilerinin abone verilerinden ayrılması imkânsızdır, çünkü trafik verileri tek başına, bu verilerin arkasındaki kişinin kim olduğunun tespit edilememesi halinde bir anlam ifade etmemektedir. - Bu sonraki bilgi, iletişimin gizliliğinin son derece önemli bir unsuru olarak kabul edilmektedir. Bilgi Komiseri, aynı zamanda, yürürlükte olan Elektronik İletişim Yasası'nın hükümlerinin, trafik veya kimlik verileriyle ilgili olup olmadıklarına bakılmaksızın, elektronik haberleşmeyle ilgili tüm veriler hakkında bir mahkeme kararı gerektirdiğini de vurgulamıştır. Bilgi Komiserinin görüşüne göre, iletişim halinde bulunan kişilerle ilgili verileri almak için polisin sadece yazılı talebini yeterli gören SCMK'nın 149b (3) maddesi, anayasal olarak sorunludur.

27. Anayasa Mahkemesi 13 Şubat 2014 tarihinde anayasal haklarının ihlal edilmediğini tespit ederek başvurucunun şikayetini reddetmiştir. Anayasa Mahkemesi'nin kararı ikiye karşı, yedi oyla kabul edilmiştir. Yargıç J. Sovdat ve Yargıç D. Jadek Pensa karara muhalefet şerhi yazmışlardır. Karar başvurucuya 11 Mart 2014 tarihinde tebliğ edilmiştir.

1. Anayasa Mahkemesinin Kararı

28. Anayasa Mahkemesi, en başta, haberleşmenin içeriğine ek olarak, Anayasa'nın 37. maddesinin trafik verisini de koruduğuna, yani bu verinin haberleşmenin bir elektronik iletişim ağında iletilmesi için işlenmiş herhangi bir veri olduğuna işaret etmiştir. Mahkeme, IP adreslerinin bu trafik verilerine dahil olduğunu kabul etmektedir. Ancak Anayasa Mahkemesi, internet üzerinden eriştiği IP adresini hiçbir şekilde gizlememiş olan başvurucunun, kendisini bilinçli olarak kamuya açık hale getirdiği ve meşru gizlilik beklentisi içinde olmadığı sonucuna varmıştır. Sonuç olarak, IP adresi kullanıcısı kimliği ile ilgili veriler, Anayasa'nın 37. Maddesi uyarınca haberleşmenin gizliliği kapsamında korunmamaktadır. Ancak Anayasa'nın 38. Maddesi uyarınca bilgi gizliliği olarak teminat altına alınmıştır ve başvurucunun davasında bunların açıklanması için mahkeme kararına gerek bulunmamaktadır.

29. Anayasa Mahkemesinin kararının ilgili kısımları aşağıdaki gibidir (Anayasa Mahkemesinin web sitesinde İngilizce'ye çevrildiği şekliyle):

"**İsviçre polisi tarafından başvurucunun IP adresine erişilmesi ile ilgili itirazlarının incelenmesi**

11. Haberleşmenin gizliliği hakkına herhangi bir müdahalede bulunmak için bir mahkeme kararı gerektirdiğinden dolayı Anayasanın 37. maddesinin ikinci fıkrası, AİHS'nin 8. maddesinden daha yüksek düzeyde bir koruma sağlamaktadır... Anayasa'nın 37. maddesinin birinci fıkrası ile düzenlenen haberleşmenin gizliliği hakkı, öncelikle iletilen mesajın içeriğini korumaktadır. ... Mesaj içeriğine ek olarak, haberleşme ile ilgili koşullar ve olgular da korunmaktadır. Bu görüş uyarınca Anayasa Mahkemesi, 2 Ekim 2008 tarih ve 106/05 sayılı kararında (Resmi Gazete RS, 100/08 ve OdlUS XVII, 84) Anayasanın 37. maddesi ile sağlanan korumayı mahkeme kararı olmaksızın bu bilgilerin alınamaması için, doğaları gereği haberleşmenin ayrılmaz bir parçası olan telefon görüşmelerine ilişkin verilere de teşmil etmiştir. Bahsedilen Karar, aksi halde telefon iletişimine atıfta bulunur, ancak aynı sonuç, *uyduğu ölçüde* bir şekilde diğer iletişim türlerine de uygulanabilir. Anayasa Mahkemesinin, Anayasa'nın 37. Maddesi kapsamında belirli bir iletişimin korunup korunmadığını incelerken yapılan kritik anayasal inceleme testi, gizlilikle ilgili meşru beklenti testidir.

12. İnternet aracılığıyla gerçekleşen iletişim, ilke olarak, kişiliğin özgürce gelişmesi, ifade özgürlüğü ve fikirlerin ifadesi için ve dolayısıyla özgür ve demokratik bir toplumun gelişmesi için asıl gerekli olan anonim bir formdadır. Anayasanın 37. maddesinin ikinci fıkrası ile belirlenen sıkı şartlar ile teminat altına alınan haberleşmenin gizliliği, bu nedenle teknolojik ilerlemeler ve ilgili izleme olanaklarına bağlı olarak giderek daha da önemli hale gelen çok önemli bir insan hakkıdır. Bu, devletin modern iletişim kanalları aracılığıyla haberleşmede, bireyleri yalnız bırakacağına ve yaptıkları, söyledikleri, yazdıkları veya düşündükleri şeyler için kendilerini savunmak zorunda olmadıklarına dair bireylerin meşru beklentilerini de beraberinde getirir. Suç işlediğine dair bir şüphenin bulunması durumunda, polisin bu iddia ile ilgili belirli bir haberleşmeye katılan bireyleri belirleme yetkisine sahip olması gerekir çünkü faillerin internetteki anonimlik ilkesi nedeniyle izini bulmak daha zordur. Polisin, soruşturma işlemlerini yürütebileceği koşullar ve mahkeme kararına gerek olup olmadığı hususu iletişimin gizliliği hakkına bir müdahale gerektirip gerektirmediğine bağlıdır.

13. Yukarıda belirtildiği gibi, iletişim içeriğine ek olarak, Anayasa'nın 37. maddesi trafik verisini de korumaktadır. Trafik verileri, bir elektronik iletişim ağında iletişimin iletilmesi veya bununla ilgili faturalandırılması için işlenen herhangi bir veriyi ifade etmektedir. Bu, IP adresinin bir trafik verisi olmasına neden olur. Bu nedenle Anayasa Mahkemesi, bu veri hakkında şikayetçinin gizlilikle ilgili meşru bir beklentisinin olup olmadığı sorusunu cevaplamalıdır.

14. Bu inceleme ile ilgili olarak iki faktörün tartılması gerekmektedir: IP adresi ile ilgili gizlilik beklentisi ve ikincisinin, toplumun meşru olarak kabul etmeye istekli olduğu bir doğaya sahip olması gerektiği durumda, bu beklentinin meşruiyeti. Konuyla ilgili davadaki şikayetçi, çocuk pornografisi içerenler de dahil olmak üzere çeşitli dosyaları paylaşmak ve indirmek için eMule uygulamasını kullanarak Razorback ağının diğer kullanıcılarıyla iletişim kurmuştur. İnternet kullanıcılarının genel anonimliğine ve dosyaların içeriğine ilişkin olarak, Anayasa Mahkemesine göre, şikayetçinin iletişiminin mahrem kalacağını ve kimliğinin açıklanmayacağını umduğu tartışmasızdır. Dolayısıyla sorun, gizlilik beklentisinin meşru olup olmadığıdır. Şikayetçi, internete eriştiği IP adresinin herhangi bir şekilde gizlendiğini ve dolayısıyla diğer kullanıcılara görünmeyeceğini ya da Razorback ağına (ve dolayısıyla dosyaların içeriğine) erişimin herhangi bir şekilde kısıtlanmış olduğunu ortaya

koyamamıştır. Aksine, şikayetçinin davasında, bu tür verilerin paylaşılmasıyla ilgilenen herkes söz konusu dosyalara erişebilmektedir ve şikayetçi, IP adresinin bir şekilde, bu ağın diğer kullanıcılarınca görülemez ve erişilemez olduğu hususlarını kanıtlayamamaktadır. Bu durum, dünyanın belirli yerlerinde interneti kullanan ve belirli dosyaları paylaşmaya ilgi gösteren, önceden belirlenmemiş bir yabancılar çemberi ile açık bir iletişim hattı gerektirdiği ve aynı zamanda diğer kullanıcıların IP adreslerine erişimin bu ağın kullanıcıları ile sınırlı olmadığı sonucuna götürür. Bu nedenle, Anayasa Mahkemesi'nin görüşüne göre, şikayetçinin gizlilik beklentisi meşru değildir; Bir ev bilgisayarından ve kendi evinin sığınağından bile olsa, bilerek kamuya açık hale gelen kişi Anayasa'nın 37. Maddesi tarafından sağlanan korumadan yararlanamayacaktır. Yukarıdakiler ışığında, Yargıtay'ın itiraza konu değerlendirmesi anayasa hukuku ile ilgili bir problem oluşturmamaktadır. Davanın tüm koşulları dikkate alındığında bu veriyi elde etmek için mahkeme kararı gerekli olmadığından, şikayetçinin dinamik IP adresi ile ilgili verilerin elde edilmesi, Anayasa'nın 37. maddesinin birinci fıkrası ile belirlenen haberleşmenin gizliliği hakkını ihlalini niteliğinde değildir. Bu şekilde davranarak şikayetçi özel hayatın gizliliği hakkından kendisi feragat etmiştir. Dolayısıyla feragatinin sonucu olarak gizlilikle ilgili meşru bir beklentisi yoktur.

...

IP adresinin kullanıcısına ait verilere erişim ile ilgili itirazların incelenmesi

16. Şikayetçi, ayrıca, SCMK'nın 149b maddesinin üçüncü fıkrası uyarınca hizmet sağlayıcısına yaptığı talebi ile polisin trafik verisi almadığını, ancak yalnızca belirli bir iletişim aracı kullanıcısı ile ilgili verileri aldığı yönündeki Yargıtay'ın görüşüne karşı çıkmaktadır...

17. Söz konusu davada, 7 Haziran 2006 tarihinde, SCMK'nın 149b maddesinin üçüncü fıkrası uyarınca, Polis, 20 Şubat 2006 saat 13.28'de 195.210.223.200 IP adresinin tahsis edildiği kullanıcı ile ilgili verilerin bildirilmesi için servis sağlayıcısından bir talepte bulunmuştur. Polis, bu talebe verilen cevapla iletişimin en yakın saniyeye ayarlandığı zaman zaten bilinmesine rağmen kullanıcının adı, soyadı ve adresi ile ilgili verileri elde edilmiştir. Daha sonra 14 Aralık 2006 tarihinde Polis, sorgu hakimi tarafından SCMK'nın birinci paragraf 149b Maddesi uyarınca verilen bir mahkeme kararını almış ve servis sağlayıcısı da bu karara göre trafik verisini vermiştir. Bu noktada Anayasa Mahkemesinin ana meselesi, belirlenen bir IP adresine ait kullanıcının kimliğine ilişkin verilerin elde edilmesinin, haberleşme gizliliği çerçevesinde olup olmadığı hususudur.

18. Anayasa Mahkemesinin 106/05 sayılı kararındaki tutumu ile uyumlu olarak, Anayasa'nın 37. maddesi, kimin, ne zaman, kiminle ve ne sıklıkla iletişim kurduğuna ilişkin veriler gibi, trafik verisini korumaktadır. İletişimde bulunan kişinin kimliği, iletişimin gizliliğinin önemli unsurlarından biridir, bu nedenle Anayasa'nın 37. maddesinin ikinci fıkrası uyarınca açıklanması için bir mahkeme kararının alınması gerekmektedir. Bu bakış açısına rağmen, Anayasa Mahkemesi, şikayetçinin Anayasa'nın 37. maddesinin ihlal edildiğine dair iddiasının konuyla ilgili davada temelsiz olduğuna karar vermiştir. Şikayetçi kendi davranışı ile kendi IP adresini ve iletişiminin içeriğini kamuya açık hale getirerek gizliliğinin korunmasından feragat etmiştir ve bu nedenle kimlik bilgilerinin verilmesi konusunda artık buna dayanamaz. Aynı zamanda gizlilikle ilgili meşru beklentiden de feragat ettiğinden, IP adresi kullanıcısının kimliğine ilişkin veriler artık, haberleşme gizliliği açısından korumadan

yararlanamayacaktır. ancak sadece Anayasa'nın 38. Maddesinde öngörülen bilgi gizliliği korumasından faydalanabilecektir. Bu nedenle, şikayetin iletişime geçtiği dinamik IP adresinin kullanıcısının adı, soyadı ve adresi ile ilgili verilerin elde edilmesi ile polis şikayetçinin haberleşmesinin gizliliğini ihlal etmemiştir ve dolayısıyla kimliğinin tespiti içi mahkeme kararına gerek bulunmamaktadır. Yukarıda belirtilenler ışığında, Yargıtay'ın itiraza konu tutumu Anayasa'nın 37. Maddesi ile tutarsız değildir ve şikayetçinin bu kısımdaki şikayetleri temelsizdir. "

2. Yargıç J. Sovdat'ın Muhalefet Şerhi

30. Yargıç J. Sovdat, Anayasa Mahkemesinin Yargıtay'ın ilgili bilgilerin trafik verisi oluşturmadığı yönündeki görüşünden ayrılmasını memnuniyetle karşılamıştır. Ancak görüşüne göre, abonenin kimliğini almak isteyen polisin mahkeme kararı talep etmesi gerekiyordu. Yargıç J. Sovdat, Anayasa Mahkemesi'nin sonucuna göre, trafik verilerinin gizliliğinin korunmasının her zaman iletişim içeriğinin korunmasına bağlı olduğu zımnen ifade edildiğine işaret etmektedir. Buna göre, belirli bir iletişim ile ilgili trafik verileri, söz konusu iletişimin içeriği korunduğu sürece korunmaktadır. Sonuç olarak, bir birey ayrı ve bağımsız olarak trafik verilerinin korunmasından yararlanamamıştır. Yargıç Sovdat, bu görüşe katılmamakla birlikte, başvurucunun kendi adıyla kamuya açık hale gelmediğini, bunun yalnızca dinamik IP adresinin rakamları üzerinden olduğunu belirtmiştir.

31. Yargıç Sovdat, Bilgi Komiserinin polisin, cihazın sahipliğinde değil, "iletişim kuran ve tam olarak iletişim kurduğu kişinin kimliği" ile ilgilendiği yönündeki görüşüne katılmaktadır. Yargıç Sovdat Komiserin, "iletişim içeriğinin, iletişim kuranların kimliğinin yokluğunda belirli bir değere sahip olmadığı" yönündeki görüşünü teyit etmektedir. Ayrıca, yeni Elektronik Haberleşme Yasasının (EHY) 166. ve 168. maddeleri uyarınca ("EHY -1'in aşağıdaki paragraf 39'a bakınız), internet sağlayıcısının depolanan bilgileri mahkeme kararı olmadan aktarmasına izin verilmediğine de dikkat çekmiştir. SCMK'nın 149b (3) maddesiyle karşılaştırıldığında, Elektronik Haberleşme Kanunu kesinlikle daha yakın tarihlidir ve bu nedenle çoğunluğun kararı, hâlihazırda ulaşılan hakların korunması düzeyine aykırıdır.

3. Yargıç D. Jadek Pensa'nın Muhalefet Şerhi

32. Yargıç D. Jadek Pensa, Anayasa'nın 37. Maddesinde belirtilen anayasal güvencelerin, bu yaşam alanında gizlilik beklentisini güçlendirmeyi ve idarenin orantısız müdahalelerini ve gücünü kötüye kullanmasını önlemeyi amaçladığını ileri sürmüştür.

33. Başvurucunun İnternetteki anonimlik beklentisi ile ilgili olarak, Yargıç Jadek Pensa, şikayetçinin kamuya açıkladığı verilerin hiçbirinin onun kimliğini ortaya çıkartmadığını ifade etmiştir. Yargıç Pensa'ya göre, anonimlik, polisin belirli bir kişiyle belirli bir iletişimi ilişkilendirmesini engelleyen şeydir. Yani bir dinamik IP adresi ile bir bireyi kendi adı ve

adresi ile ilişkilendirilme durumundan korumasıdır. Ayrıca, Yargıç, başvurucunun iletişim şeklinin gizlilik beklentisinin nesnel olarak haklı kıldığına dair sonuca yol açıp açmayabileceği sorusunun, ilgili zamanda yürürlükte olan yasa da dahil olmak üzere tüm şartlar dikkate alınarak ele alınması gerektiğini ileri sürmüştür. Elektronik Haberleşme Yasasının (EHY) (Madde 103 (1 (2)), 104 (1) ve 107 - aşağıdaki paragraf 37'ye bakınız), mesajların aktarımı için artık gerekli olmadığında İnternet sağlayıcılarınca trafik verilerinin silinmesini öngördüğünü ortaya koymuştur. Ayrıca, Elektronik Haberleşme Yasası'nın 107. maddesine göre, iletişimin gizliliğine yalnızca yetkili bir makamın kararına dayanarak müdahale edilebilecektir. Polisten internet sağlayıcısına gönderilen bir talep kanunen gerekli görülen bir karar olarak addedilemez. Böylece, SCMK'nın 149b (3) maddesi, bir internet abonesi hakkında polisin bilgi talep etmesine izin verilebileceği şeklinde yorumlanabilse bile, "elektronik iletişimin gizliliği ve gizliliğin korunması" ile açıkça ilgili olan Elektronik Haberleşme Yasası tarafından düzenlenen durumlarda bu uygulanmamalıdır. Aksi halde, mevzuat çelişkili olabilecektir. Yargıç, uygulanabilir yasal çerçevenin, makul ve yeterli düzeyde bilgilendirilmiş bir birey olarak, başvurucunun gizlilik beklentisine sahip olamayacağı sonucuna yol açmamalıdır. Yani, anonimliğinin korunacağını beklememiş olacaktı.

34. Judge Jadek Pensa, belirli bir dinamik IP adresi kullanıcısı hakkındaki veriler gibi trafik verilerinin tarafsızlığı hakkında ayrıntılı bilgi vermektedir:

> "9. Trafik verisi - belirli bir anda rastgele atanan dinamik IP adresi - anladığım kadarıyla, bir bilgisayarın belirli bir bağlantıya ayrılmaz şekilde eklendiği için bilgisayarın internette nasıl kullanıldığını açıklamaktadır... Bunun nedeni, sadece iki verinin, interneti anonimleştirilmemiş bir şekilde nasıl kullandığı, yani tanımlanmış bir kişi ile bağlantılı internet kullanımına ilişkin olarak, ortaklaşa iletişim kurmasıdır. Benim görüşüme göre bu temel durum , polisin servis sağlayıcılardan almaya çalıştığı belirli bir (bilinen) dinamik IP adresi için bir kullanıcıya ait verilerinin tarafsızlığı kavramını yani, belirli bir kişinin adı ve adresinden (hizmet sağlayıcıyla abonelik sözleşmesi olan) daha fazla bir şey iletme yeteneğini reddeden koşullarda verilerin tarafsızlığı kavramını çürütmektedir; Bu veri ayrılmaz bir şekilde belirli bir iletişim ile bağlantılı olduğu için, trafik verisi tam olarak iletişimin gizliliği kapsamında korunan alana girer.
>
> 10. Servis sağlayıcısı, 'sadece' sağlayıcı ile abonelik sözleşmesi olan bir kişiyi tanımlayan veriyi polise vermiş olsa bile, anladığım kadarıyla, böyle yaparak servis sağlayıcı aslında (yalnızca basitçe açıklarsak) bu kişi ile ilgili elektronik iletişim ağındaki trafik verisini vermiş olmaktadır. Polis, daha önce de açıkladığım gibi, abonelik sözleşmesi imzalamış olan belirli bir kişinin adından ve soyadından daha fazlasını belirlemek istemektedir. Anladığım kadarıyla, belirli bir kişiyle ilgili trafik verilerini talep ettikleri için SCMK'nın 149b maddesinin birinci fıkrası uyarınca soruşturmayı yürütmek ve sorgu yargıcından bir karar almak zorunda kalacaklardır. "

II. İLGİLİ İÇ HUKUK KURALLARI VE UYGULAMASI

A. Anayasa

35. Haberleşme ve diğer iletişim araçlarının gizliliği ve kişisel verilerin korunmasını teminat altına alan Anayasanın 37 ve 38. maddeleri aşağıdaki gibidir:

Madde 37

"Haberleşme ve diğer iletişim araçlarının gizliliği teminat altına alınmıştır.

Haberleşmenin ve diğer iletişim araçlarının gizliliğinin korunması ve özel hayatın dokunulmazlığı, bir ceza soruşturmasında ve ulusal güvenlik sebebiyle gerekli olan durumlarda, belirli bir süre için mahkeme kararına dayanmak kaydıyla ancak kanunla askıya alınabilir.."

Madde 38

"Kişisel veriler teminat altına alınmıştır. Kişisel verilerin toplanma amacına aykırı kullanılması yasaktır.

Kişisel verilerin gizliliğinin toplanması, işlenmesi, tayini, denetlenmesi ve korunması kanunla düzenlenecektir.

Herkes, kendisiyle ilgili toplanan kişisel verilere ve bu tür verilerin kötüye kullanılması durumunda hukuksal koruma için erişim hakkına sahiptir."

B. Ceza Muhakemesi Kanunu

36. Ceza Muhakemesi Kanunu'nun (Resmi Gazete no. 8/06) soruşturma aşamasında polis tarafından alınan tedbirleri düzenleyen 149b maddesi şu şekildedir:

"(1) Bir failin re'sen soruşturulmasına neden olan bir suçun işlendiği, işlenmekte olduğu, suça ilişkin hazırlık hareketlerinin yapıldığı veya organize olunduğu, ve bu suçu yada suçluyu açığa çıkarmak için elektronik haberleşme ağları kullanan iletişim bilgilerinin elde edinilmesi gerektiği hususlarında şüphe duymak için gerekçeler varsa, sorgu hakimi, savcının talebinde öne sürdüğü makul gerekçeler üzerine, elektronik haberleşme ağının operatöründen elektronik haberleşme hizmetlerinin kullanıcılarının sayısı veya elektronik iletişim servisindeki aramanın türü, tarihi, zamanı ve süresi veya diğer bir şeklini; iletilen veri miktarı; elektronik haberleşme servisinin kullanıldığı yer gibi kullanıcılar ve elektronik iletişimin koşulları ve durumları hakkında bilgi vermesini isteyebilir.

(2) Talep ve mahkeme kararı yazılı olmalı ve elektronik iletişim araçlarının tanımlanmasına, makul gerekçelere dair bir belirtiye, bilginin gerekli olduğu süreye ve tedbirin kullanımını gerektiren diğer önemli koşullara ilişkin bilgileri içermelidir.

(3) Şayet failin re'sen soruşturulmasına neden olan bir suçun işlendiği veya hazırlandığından şüphelenmek için gerekçeler varsa ve ayrıntıları, iletişim araçlarının kullanımda olduğu ya da kullanımda olduğu zamanla ilgili bilgilerin yanı sıra ilgili dizinde bulunmayan belirli bir elektronik iletişim aracının sahibi veya kullanıcısı hakkında bilgi varsa, bu suç veya suçu ortaya çıkarmak için polis, elektronik haberleşme ağının operatöründen bilginin ilgilisi olan kişinin rızası olmasa da bunları kendilerine vermesini yazılı olarak isteyebilir.

(4) Elektronik iletişim ağları operatörü, müşterisine veya üçüncü bir kişiye sorgu hakimine (bu maddenin birinci paragrafı) veya polise (önceki paragraf) bilgi verdiğini yada verme niyetinde olduğunu açıklayamaz. ."

C. Elektronik Haberleşme Yasası

37. Söz konusu verilerin elde edildiği tarihte (Ağustos 2006), Elektronik Haberleşme Yasası ("EHY", Resmi Gazete no. 43/04 ve 86/04) yürürlüktedir. Bu Kanunda, diğer hususların yanı sıra 2002/58 / EC sayılı Direktif tatbik edilmiştir. (bkz. Aşağıdaki 56. paragraf). Aşağıdaki hükümler bu hususla ilgilidir:

Madde 1

Yasanın Kapsamı

"Bu Kanun, elektronik haberleşme ağlarının sağlanması ve elektronik haberleşme hizmetlerinin sağlanması için şartları düzenlemektedir... kullanıcıların haklarını düzenler... elektronik iletişimin gizliliğinin ve gizliliğinin korunmasını düzenler ve elektronik iletişim ile ilgili diğer hususları düzenler."

Madde 3

Kullanılan Terimler

"Yasada kullanılan terimler aşağıdaki anlamda kullanılmıştır;

...

25. Trafik verileri, bir elektronik iletişim ağı üzerinde iletişimin sağlanması veya bunların faturalandırılması amacıyla işleme tabi tutulan herhangi bir veridir.

..."

Madde 103

İletişimin Gizliliği

"(1) İletişimin Gizliliği:

1. İletişimin içeriğini ;

2. Yukarıdaki (1) 1 numaralı maddede bahsedilen iletişime bağlı trafik verileri ve konum verileri;

3. Başarısız bağlantı girişimleri ile ilgili durum ve koşullar.

İfade etmektedir.

(2) Bir operatör ve faaliyetlerinin sağlanmasında ve yerine getirilmesinde yer alan herhangi bir kişi, gizliliği korumakla yükümlü olduğu faaliyetini durdurduktan sonra iletişimin gizliliğini korumayı sürdürmelidir.

(3) Yukarıdaki (2). Fıkrada sorumlu olan kuruluşlar, yalnızca kamuya açık belirli bir iletişim hizmetlerinin sağlanması için gereken yukarıda fıkra (1)'de belirtilen haberleşmeler hakkında bilgi edinebilir ve bu bilgiyi, hizmetleri sağlamak için yalnızca kullanabilir veya diğerlerine aktarabilir [posreduje].

(4) İşletmecilerin iletişimin içeriği hakkında bilgileri toplaması veya kaydetmesi veya haberleşmeleri ve yukarıdaki (3). Fıkradaki trafik verilerinin saklaması durumunda, İşletmeciler, abonelik sözleşmesi imzalandığında veya kamuya açıklığın başlamasının ardından kullanıcıya bu hususu bildirmekle yükümlü olup teknik olarak mümkün olan en kısa zamanda ve kamuya açık özel iletişim hizmetinin sağlanması için gerekli olan bilgiye artık ihtiyaç bulunmadığında iletişimin veya iletişimin içeriğine ilişkin bilgileri silmekle yükümlüdür.

(5) Yukarıdaki (1) numaralı fıkrada belirtilen iletişimin dinlenmesi, kaydedilmesi, saklanması ve aktarılması [*posredovanje*] gibi her türlü izleme ve dinleme, bu Kanunun 107. maddesinin (4). fıkrası kapsamında izin verilmediği müddetçe veya mesajların gönderilmesi için bu izleme veya dinleme gerekli olmadıkça, (örneğin, faks mesajları, elektronik posta, elektronik posta kutuları, sesli mesaj ve SMS hizmetleri) yasaklanmıştır.

..."

Madde 104

Trafik verileri

"(1) Aboneler ve kullanıcılar ile ilgili, operatör tarafından işleme tabi tutulan ve saklanan trafik verileri, mesajların aktarımı için artık gerekli olmadıkça silinmeli veya anonim hale getirilmelidir.

(2) Yukarıda (1) numaralı fıkra hükmü saklı kalmak kaydıyla, operatör, bir hizmet için yapılacak ödemenin tamamlanmasına kadar, ancak sınırlama süresini geçmemek üzere hesaplama ve ödeme amaçları için gerekli olan trafik verisini saklayabilir ve işleyebilir.

(3) Elektronik haberleşme hizmetlerinin pazarlanması ya da katma değerli hizmetlerin sağlanması amacıyla, kamuya açık bir elektronik iletişim servisi sağlayıcısı, yukarıdaki (1) numaralı fıkrada sözü edilen verileri bunların hizmet vermesi veya pazarlanması için gerekli olan süre boyunca ancak sadece, verilerin ilgili olduğu abone ya da kullanıcı önceden onay vermişse işleyebilir. Abonelerin veya kullanıcıların, izin vermeden önce, işlenen trafik verilerinin türü ve bu tür işlemlerin süreleri konusunda bilgilendirilmesi gerekir. Bir kullanıcı veya abone, istediği zaman onayını geri çekme hakkına sahiptir.

(4) Yukarıdaki (2) numaralı fıkrada belirtilen amaçlar için, hizmet sağlayıcı, trafik verilerinin tutulacağı ve işleneceği genel şartlar ve koşullar ile bunların süresini belirlemelidir ve veri koruma yasalarına uygun olarak hareket edeceğini beyan etmelidir.

(5) Trafik verileri, sadece işletmecinin yetkisi altında hareket eden ve fatura veya trafik yönetimini ele alan, müşteri taleplerine cevap veren, dolandırıcılığı saptayan elektronik haberleşme hizmetlerini pazarlayan veya katma değer sağlayan kişiler tarafından yukarıdaki (1) - (4) fıkrası kapsamında işleme tabi tutulabilir. Ve bu işlem, bu tür faaliyetlerin amaçları için gerekli olanlarla sınırlı olmalıdır.

(6) Yukarıdaki (1), (2), (3) ve (5) numaralı fıkraların hükümleri saklı kalmak kaydıyla, işletmeci, ihtilafların, özellikle de arabağlantı veya faturalandırma uyuşmazlıklarının çözülmesi amacıyla kurulmuş yetkili bir organın yazılı talebi üzerine ve yürürlükteki mevzuata uygun olarak, bu tür bir kuruluşa trafik verilerini gönderir."

Madde 107

İletişimin yasal olarak dinlenilmesi

"... (2) Operatör , kamu iletişim ağının belirlenen bir noktasında, yetkili makam tarafından verilen kararın bir nüshasını alır almaz, iletişimin yasal olarak dinlenilmesine olanak sağlamalıdır.... iletişimin yasal bir şekilde dinlenmesinde bu tedbirin araçları, kapsamı ve süresi ile ilgili diğer verilerin yer alması gereklidir.

38. 28 Kasım 2006 tarihinde kabul edilen, bu davadaki ihtilaflı tedbirler alındıktan sonra EHY de yapılan, (ECA-A) ilave düzenlemeler (Resmi Gazete No. 129/06), *diğerlerinin yanı sıra*, cezai kovuşturma amaçları doğrultusunda trafik verilerinin saklanmasını da düzenlemiştir.

Buna, belirli bir IP adresi tahsis edilen abonenin adı ve adresi, iletişimin hedefinin tespiti ve tarihi belirlemek için gereken veriler gibi, iletişim kaynağının tanımlanması için gerekli olan veriler dahil edilmiştir. (Madde 107.a ve 107.b). Bu konuda statik ve dinamik IP adresi arasında ayrım yapılmamıştır. Buna ek olarak, madde 107.c ile getirilen değişiklikle, yetkili organ tarafından düzenlenen karar metnini aldıktan sonra en geç üç gün içinde operatör saklanan verilere derhal erişme veya aktarmaya izin verme yükümlülüğü altında olduğu öngörülmüştür. Değiştirilen Kanunun 107.e maddesine göre, "belirli verilere erişilmesine karar veren mahkeme, saklanan verilerin verilmesi veya bunlara erişilmesi için verilen mahkeme kararlarına ilişkin verilerin kaydı tutmalıdır." Ayrıca, mahkemeden Adalet Bakanlığına ve daha sonra bakanlıktan Avrupa Komisyonuna kadar, saklanan verilere erişim konusunda raporlama prosedürü öngörülmüştür.

39. 20 Aralık 2012 tarihinde yeni bir Elektronik Haberleşme Yasası ("EHY -1", Resmi Gazete 109/2012) kabul edildi. Yasa'nın 166 ve 168. Maddeleri aşağıdaki gibidir;

Madde 166

Saklanan verilerin yetkili makamlara verilmesi

"(1) Operatör, hemen veya gereksiz bir gecikmeye mahal vermeden, yetkili makamın kararı kendisine ulaşır ulaşmaz erişim kapsamındaki istenen bilgileri vermelidir.

...

(4) Operatör haklarındaki mahkeme kararını bu kişilere ya da üçüncü kişilere ve saklanan verilerin bu maddeye göre yetkili olan organa verildiğini ya da verileceğini açıklayamaz.

...

(7) Bilgi komiseri, diğer yasalara göre başka yetkili organların denetimi altında olmadığı sürece, bu maddedeki sağlayıcıların yükümlülüklerini yerine getirmelerini denetleyecektir."

Madde 168

Erişim kararları ve veri transferleri ile ilgili veriler

"(1) Verilere erişilmesine karar veren bir mahkeme, bu Kanunun 166. maddesine uygun olarak, erişim kararlarının ve veri transferinin kaydını tutmalıdır. Bu kayıt aşağıdakileri içerecektir:

1. Saklanan verilere erişilmesine karar verilen davaların sayısı;

2. Verinin istendiği tarih veya süre, erişim kararını veren yetkili organa ve veri transferi tarihini içeren verilere ait kayıtlar;

3. İnfaz edilemeyen veri erişim kararlarının sayısı;

(2) Yetkili mahkeme, cari yıl için yukarıdaki (1) numaralı fıkrada belirtilen kaydı, bir sonraki yıl en geç 31 Ocak tarihine kadar Adalet Bakanlığına iletir.

(3) Adalet Bakanlığı, tüm mahkemelerden alınan kayıtlara göre, önceki yıl için her yıl en geç 20 Şubat'a kadar saklanan verilere erişim konusunda ortak bir rapor hazırlar. Avrupa Komisyonu'na ve istihbarat ve güvenlik hizmetlerinin denetlenmesinden sorumlu Ulusal Meclis Komitesine geciktirmeksizin iletilmek üzere bakanlığa ulaştırır.

(4) Adalet Bakanlığı, Slovenya Cumhuriyeti Yüksek Mahkemesi Başkanı'nın görüşünü aldıktan sonra, bu maddedeki raporlama formlarını kullanarak yönerge çıkarır. "

D. Kişisel Verilerin Korunması Yasası

40. Slovenya'nın Avrupa Birliğine üye olmasına istinaden, Slovenya Parlamentosu, 15 Temmuz 2004 tarihinde, 95/46/ES sayılı Direktifle (Aşağıdaki paragraf 53'e bakınız) desteklenen yeni bir Kişisel Verilerin Korunması Yasası'nı kabul etmiştir. (86/04 sayılı Resmi Gazete) İlgili olduğu kadarıyla aşağıda belirtilmiştir.

Madde 1

Yasanın Kapsamı

"Bu Kanun, kişisel verilerin işlenmesinde bireyin (bundan sonra: birey olarak anılacaktır) gizlilik ve haysiyetlerine anayasaya aykırı, hukuksuz ve gayrimeşru tecavüzlerin önlenmesi için hakları, sorumlulukları, ilkeleri ve önlemleri düzenlemektedir. "

Madde 6

Terminoloji

"Yasada kullanılan terimler aşağıdaki anlamda kullanılmıştır:

1. Kişisel veri – ifade ediliş tarzına bakılmaksızın kişilerle ilgili her türlü veri

2. Kişi - kişisel verilerin ilişkili olduğu tanımlanmış veya tanımlanabilir gerçek kişidir; tanımlanabilir bir gerçek kişi, tanımlama yöntemi çok fazla zaman, orantısız bir çaba ve önemli maliyete neden olmamak üzere, özellikle bir kimlik numarası ya da fiziksel, fizyolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğine özgü bir ya da daha fazla faktörle doğrudan ya da dolaylı olarak tanımlanabilen kişidir.

...

18. Anonimleştirme - artık, kişi ile ilişkisi kurulamayacak veya bu tür ilişkilendirmenin ancak orantısız çaba, masraf veya zaman harcanarak yapılabilecek olan kişisel verilerin şeklinin değiştirilmesidir.

19. Hassas kişisel veriler - ırksal, ulusal veya etnik köken, siyasi, dini veya felsefi inançlar, sendika üyeliği, sağlık durumu, cinsel yaşam hakkındaki verilerdir..."

41. Kişisel Verilerin Korunması Yasası'nın 2. maddesi, kişisel verilerin yasal ve adilane bir şekilde işlenmesini öngörmüştür. 8. maddesi, kişisel verilerin, yasaların düzenlemesi veya ilgili kişinin rızası temelinde işlenebileceğini öngörmüştür. 12. maddesine göre, bir kişinin yaşamı veya uzvunun korunması için acil olarak gerekli olması halinde kişisel veriler başka bir yasal dayanak olmaksızın işlenebilir.

42. Kişisel Verilerin Korunması Yasası ayrıca, verilerin sadece öngörülmüş ve yasal amaçlar için toplanabileceğini ve bu doğrultuda (madde 16) ve sadece bu amaçların gerçekleştirilmesi için gerekli olduğu hallerde işlenebileceğini (madde 21) düzenlemiştir. Daha sonra silinmeli, imha edilmeli, bloke edilmeli veya anonim hale getirilmelidir (a.g.e). Kanun ayrıca, kişisel verileri güvence altına almak için ve verilerin yetkili olmayanlarca, kasıtlı olarak imha edilmesinin önlenmesi, değiştirilmesini, kaybını veya yetkisiz işlemeyi önlemek için operatörlerin ve sözleşmeli işlemcilerin alması gereken önlemleri ve izlemesi gereken usulü düzenlemiştir (madde 24 ve 25).

E. Ceza Kanunu

43. Ceza Kanununun, 187. maddesinde, pornografik materyalin on dört yaşından küçüklere sunulması ve reşit olmayanları tasvir eden pornografik malzemenin üretilmesi ve dağıtılması yasaklanmıştır. İlgili hüküm aşağıdaki gibidir:

"...

(2) Pornografik resimlerin, görsel-işitsel veya pornografik içeriğin diğer nesnelerini üretmek için reşit olmayan kişileri istismar eden veya pornografik içeriğin

yapılmasında reşit olmayan bir kişiyi kullanan kişi, altı aydan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Küçükleri tasvir eden pornografik veya diğer cinsel materyalleri üreten, dağıtan, satan, ithal eden veya ihraç eden, başka herhangi bir şekilde tedarik eden veya üretme, dağıtma, satma, ithal etme, ihraç etme ya da başka herhangi bir şekilde sunma amacı ile bulunduranlar, yukarıdaki (2). fıkradaki ceza ile cezalandırılırlar..."

F. 2 Ekim 2008 tarih ve Up-106/05/2 sayılı Anayasa Mahkemesi kararı

44. Up-106/05 sayılı karar, mahkeme kararı olmaksızın SIM kartından elde edilen verilere (bir telefon numarası ve metin mesajı) dayanarak, yasa dışı uyuşturucu ticaretinden suçlu bulunan şikayetçi ile ilgili bir içtihattır. Şikayetçi mahkumiyetinin, polisin cep telefonuyla iletişimini mahkeme kararı olmadan izlemesi ile yasaya aykırı olarak elde edilen delillere dayandığından şikayetçi olmuştur. Anayasa Mahkemesi şikayeti kabul etmiş ve alt mahkemelerin kararlarını bozmuştur.

45. Anayasa Mahkemesi, iletişimin gizliliğinin ayrılmaz bir unsuru olan telefonun hafızasında saklanan veriler de dahil olmak üzere, sadece haberleşmenin içeriğinin değil, aynı zamanda iletişime bağlı olan koşulların ve olayların da korunduğuna karar vermiştir. Bu nedenle, son aranan ve son cevapsız çağrılara ilişkin verilerin elde edilmesi, iletişimin içeriğinin ve koşullarının incelenmesini gerektirmektedir ve sonuç olarak bu da Anayasanın 37. maddesinin birinci fıkrasında teminat altına alınan haklara bir müdahale oluşturmaktadır. Mahkeme, bu tür müdahalenin, Anayasa'nın 37 § 2. maddesi uyarınca, aşağıdaki koşulların yerine getirilmesi durumunda kabul edilebilir olduğuna işaret etmiştir: (1) müdahale yasa tarafından öngörülmüş olmalı; (2) mahkeme kararına dayanmalı; (3) müdahale edilen süre kesin olarak belirlenmeli ve (4) ceza yargılaması süreci veya ulusal güvenlik için müdahale gerekli olmalıdır.

III. İLGİLİ ULUSLARARASI HUKUK

A. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

46. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (28 Ocak 1981 tarihinde imzaya açılmıştır. "ETS No. 108", "1981 Sözleşmesi" olarak anılacaktır), bütün Avrupa Konseyi Üye Devletleri tarafından onaylanmış ve 1 Eylül 1994 tarihinde Slovenya'da da yürürlüğe girmiştir. 1. maddede belirtilen Sözleşme'nin amacı; "haklarındaki kişisel verilerin otomatik olarak işleme tabi tutulması ile ilgili olarak, her bir taraf devlet ülkesinde, uyrukları veya

ikametleri ne olursa olsun, her birey için, başta özel hayatın gizliliği olmak üzere kişilerin haklarına ve temel özgürlüklerine saygı duyulmasını güvence altına almaktır ('verilerin koruması')." 1981 Sözleşmesi, diğer şeylerin yanı sıra, bireyleri istismarlara karşı korumaktadır ve yargı ve emniyet birimlerinin veri işlenmesi gibi hem özel, hem de kamu sektörü tarafından yapılan tüm veri işlemlerine uygulanır. 2. maddede "kişisel veriler" kavramını, tanımlanmış veya tanımlanabilir bir bireyle ilgili herhangi bir bilgi olarak tarif edilmiştir. 5. madde ise, otomatik işleme tabi tutulan kişisel verilerin adil ve yasal olarak toplanması ve işleme tabi tutulması öngörülmüştür.

B. Siber Suçlar Sözleşmesi

47. Siber Suçlar Sözleşmesi (23 Kasım 2001 tarihinde imzaya açılmıştır), 1 Temmuz 2004 tarihinde yürürlüğe girmiştir, (bundan böyle "Siber Suçlar Sözleşmesi" olarak anılacaktır ETS No. 185) Slovenya'da 1 Ocak 2005 tarihinde yürürlüğe girmiştir.

48. Siber Suçlar Sözleşmesi, internet üzerinden işlenen suçlarla ilgili ve bütün devletlere açık olan ilk uluslararası anlaşmadır. Ülkelere, diğerlerinin yanı sıra, çocuk pornografisini suç olarak düzenlemelerini şart koşmuştur.

49. 1. maddede, Siber Suçlar Sözleşmesinin amaçları doğrultusunda, "trafik verisi" "iletişimin başlangıç noktasını, istikametini, izlediği yolu, tarihini, boyutlarını, devam süresini ve kullandığı hizmeti belirten, iletişim zincirinde bir parça oluşturan, bir bilgisayar sistemi tarafından üretilen, sisteminin iletişimiyle ilgili herhangi bir bilgisayar verisi" olarak tanımlanmaktadır. Ayrıca Açıklayıcı Raporun ilgili kısım aşağıdaki gibidir (§ 30):

"Kaynak " bir telefon numarasını, İnternet Protokolü (IP) adresi veya bir servis sağlayıcısının hizmet verdiği bir iletişim aracındaki benzer bir tanımını ifade eder. "Hedef", iletişimin ulaştırıldığı iletişim tesisinin karşılaştırılabilir bir göstergesini ifade eder. "Temel hizmetin türü" terimi, dosya aktarımı, elektronik posta veya anında mesajlaşma gibi ağ içinde kullanılan hizmet türünü ifade eder.

50. Siber Suç Konvansiyonu uyarınca, burada belirtilen suçlarla mücadele etmek için aşağıdaki önlemler yetkili makamlar için mevcut olmalıdır:

Madde 18 – Üretim Talimatı

1. Taraflardan her biri, yetkili makamlarını, talimat verme konusunda salahiyete haiz olabilmeleri için gerekli yasama işlemlerini ve diğer tedbirleri kabul edecektir:

....

b. Söz konusu tarafın ulusal sınırları içinde hizmet veren bir servis sağlayıcının yedinde ve kontrolünde bulunan hizmetler ile ilgili, tarafa abone bilgisini vermesi yönünde,

2. Bu maddede bahsi geçen yetki ve usuller Madde 14 ve Madde 15'e tabidir.

3. Bu maddenin amacına yönelik olarak, "Abone Bilgisi" terimi, tahsis edildiği, trafik veya içerik verisinden ziyade, servislerle ilgili abonelere ilişkin, bilgisayar verisi veya başka bir şekilde bulunan bilgi anlamına gelmektedir

Madde 20 – Trafik Verisinin Gerçek Zamanlı olarak Toplanması

1. Taraflardan her biri, yetkili merciin;

a. Söz konusu tarafın alanında, teknik araçların uygulanmasıyla toplaması ve kayıt yapabilmesi, ve

b. Mevcut teknik kapasitesi içinde, bir servis sağlayıcıyı

i. Söz konusu tarafın alanında, teknik araçların uygulanmasıyla toplama ve kayıt yapabilme; veya

ii. Bir bilgisayar sistemi vasıtasıyla kendi alanından geçirilen iletişimle ilgili, gerçek zamanlı trafik verisinin kaydı ve toplanması işleminde, yetkili otoriteleriyle işbirliği yapmasına, yardım etmesine

mecbur kılabilmesini gerektiren, yetki ve diğer önlemleri kabul edecektir.

4. Bu maddede bahsi geçen yetki ve usul, Madde 14 ve Madde 15'e tabidir.

Madde 21 – İçerik Verisine Müdahale Edilmesi

1. Taraflardan her biri, bir dizi ciddi suçla ilgili kendi iç kanunları tarafından belirlenecek yetkili mercilerinin yetkili kılınması için yasama işlemlerini yapacak ve diğer tedbirleri alacaktır:

Bir bilgisayar sistemi vasıtasıyla kendi alanından geçirilen belirlenmiş bir iletişimle ilgili, gerçek zamanlı içerik verisinin kaydı ve toplanması işleminde,

a. Trafik bilgilerinin ilgili tarafın ulusal sınırları içinde bulunan teknik araçların kullanılması suretiyle toplaması ve kaydedilmesi, ve

b. Herhangi bir servis sağlayıcının mevcut teknik kapasitesi içinde,

i. Trafik bilgilerinin ilgili tarafın ulusal sınırları içinde bulunan teknik araçların kullanılması suretiyle toplaması ve kaydedilmesi, veya

ii. Trafik verisinin kayıt altına alınması ve toplanması işleminde, yetkili otoriteleriyle işbirliği yapması, yardım etmesini temin edilmesini gerektiren, yetki ve diğer önlemleri benimseyecektir.

...

4.Bu maddede bahsi geçen yetki ve usuller, Madde 14 ve Madde 15'e tabidir.

51. Üretim talimatı ilgili olarak, Siber Suçlar Sözleşmesine İlişkin Açıklayıcı Raporda (Budapeşte, 23 Kasım 2001, ETS No. 185), bir ceza soruşturması sırasında, abone bilgisinin, esas olarak iki durumda gerekli olabileceğini belirtilmektedir. İlk olarak, hangi servislerin ve ilgili teknik önlemlerin bir abone tarafından kullanıldığının veya kullanılmakta olduğunun, kullanılan telefon hizmeti tipinin, kullanılan diğer ilgili hizmetlerin türünün (örneğin, çağrı yönlendirme, sesli mesaj) veya telefon numarası veya diğer teknik adresin (örneğin e-mail adresi) tespit edilmesinde gereklidir. İkinci olarak, teknik bir adresin bilinmesi durumunda, ilgili kişinin kimliğinin tespitine yardımcı olmak için abone bilgisi gereklidir. Açıklayıcı rapora göre, üretim talimatı, 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 sağlar. Bu önlemler ağır nitelikteki suçlarla sınırlı olmalıdır.

52. Siber Suçlar Sözleşmesi, 18, 20 ve 21. maddelerde belirtilen yukarıda bahsedilen tedbirlerin Madde 14 ve 15'te belirtilen koşullara tabi olmasını şart koşan ilgili hükümler aşağıdaki gibidir:

Madde 14 – Usul Hükümlerinin Kapsamı

"1. Taraflardan her biri, iş bu kısımdaki yetki ve usullerin esas alınması sureti ile bazı cezai soruşturma ve işlemlerinin yapılabilmesi için gerekli yasama işlemlerini yapacak ve diğer önlemleri alacaktır.

..."

Madde 15 - Koşullar ve Tedbirler

1. Taraflardan her biri iş bu madde çerçevesindeki yetki ve usullerin belirlenmesi, uygulanması ve geçerli kılınması hususlarının, ilgili Tarafın ulusal yasalarındaki şartlara ve önlemlere tabi olmasını temin edecektir. Söz konusu hususlar, İnsan Haklarının Temel Özgürlüklerinin Korunması Hakkında 1950 tarihli Avrupa Konseyi Konvansiyonu çerçevesinde, 1966 tarihli Sivil ve Siyasi Haklar Uluslararası Birleşmiş Milletler Anlaşması çerçevesinde, ayrıca yürürlükte bulunan diğer uluslararası insan hakları belgeleri çerçevesinde, üstlenilen yükümlülüklerden doğan hakların gerekli ölçüde korunmasını temin edecek ve hakkaniyet ilkesinin tesis edilmesini sağlayacaktır.

2. Yukarıda belirtilen şartlar ve önlemler, ilgili yetki yada usulün niteliği göz önüne alındığında uygun olduğu ölçüde, söz konusu yetki yada usulün kapsamı ve süresine ilişkin adli yada başka nitelikli bağımsız gözetim, gerekçelerin haklılığına ilişkin başvuru işlemi yada sınırlama yapılmasını da diğer hususlarla birlikte içerecektir.

IV. İLGİLİ AVRUPA BİRLİĞİ HUKUKU

A. 95/46 / EC sayılı Direktif ve (AB)016/679 sayılı Tüzük

53. Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımı hakkında bireylerin korunmasıyla ilgili olarak 24 Ekim 1995 tarih ve 95/46 / EC sayılı Avrupa Parlamentosu ve Konseyi Direktifinin 2 (1) (a) Maddesinde (OJ 1995 L 281, sayfa 31, bundan böyle "Veri Koruma Direktifi" olarak anılacaktır,) "kişisel veri", "tanımlanmış veya tanımlanabilir gerçek kişi ('veri konusu')" ile ilgili her türlü bilgiyi ifade edecek şekilde düzenlenmiştir. Ayrıca, yukarıda belirtilen hüküm kapsamında, "tanımlanabilir kişi", özellikle, bir kimlik numarasıyla veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel ve sosyal kimliğine özgü bir veya birden fazla faktörle doğrudan veya dolaylı olarak tanımlanabilen kişidir." Veri Koruma Direktifinin polis ve ceza adaleti alanında uygulanma kabiliyeti bulunmamaktadır.

54. Rapor 26'ya göre, bir kişinin tanımlanabilir olup olmadığının belirlenmesinde "söz konusu kişiyi tanımlamak için ... makul bir şekilde kullanılmasının mümkün olduğu tüm kayıtlar alınmalıdır"; Koruma ilkeleri, veri konusu artık tanımlanmayacak şekilde anonim hale getirilen veriler için uygulanmayacaktır.

55. Kişisel bilgilerin işleme tabi tutulması ve bu verilerin serbest dolaşımı ile ilgili olarak gerçek kişilerin korunması hakkındaki 27 Nisan 2016 tarihli Avrupa Parlamentosu ve Konseyinin 2016/679 sayılı Tüzüğü, 27/46 / EC sayılı Direktifin kaldırılması ile ilgili (Genel Veri Koruma Tüzüğü)(OJ 2016 L 119/1, s. 1), 24 Mayıs 2016 tarihinde yürürlüğe girmiştir. Yürürlüğe girdiği zaman (25 Mayıs 2018), Veri Koruma Direktifinin yerini alacaktır. 4. Madde "tanımlanabilir bir gerçek kişi", "özellikle bir isim, kimlik numarası, konum bilgisi, çevrimiçi bir tanımlayıcı... gibi bir tanımlayıcıya atıfta bulunarak doğrudan veya dolaylı olarak tanımlanabilen kişi" olarak tarif edilmektedir. Rapor 26 ya göre, ayrıca, gerçek kişiyi tanımlamak için araçların makul olarak kullanılmasının mümkün olup olmadığının belirlenmesinde, işleme tabi tutma zamanındaki mevcut teknoloji, hesabın tanımlanması için gerekli maliyetler ve süre gibi, tüm nesnel faktörler nazara alınmalıdır." Ayrıca, rapora göre, veri koruma prensipleri, anonim bilgilere, yani tanımlanmış ya da tanımlanabilir gerçek bir kişiyle ilişkilendirilemeyen bilgilere ya da veri konusunun tanımlanamayacağı ya da artık tanımlanmayacağı şekilde anonim hale getirildiği kişisel verilere "uygulanamayacaktır.

B. Direktif 2002/58/EC

56. Ek olarak, elektronik haberleşme alanında, kişisel verilerin işlenmesi ve elektronik haberleşme sektöründeki gizliliğin korunması ile ilgili 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Konsey 2002/58 / EC sayılı Direktifi (Elektronik haberleşme Direktifi - OJ 2002 L 201, s. 37) 12 Temmuz 2002 tarihinde kabul edilmiştir. Bunun kolluk işlemlerinde ve ceza yargılaması alanında uygulama kabiliyeti bulunmamaktadır ancak elektronik iletişim sektöründe kişisel verilerin işlenmesiyle ilgili olarak temel hak ve özgürlüklerin eşit düzeyde korunmasını ve özellikle özel hayatın gizliliği hakkının güvence altına alınmasını temin edilmesi için üye devletlerin iç mevzuatlarını uyumlu hale getirmelerini şart koşmuştur. 2. Maddede, "kullanıcı" "kamuya açık bir elektronik iletişim hizmetini, özel ya da iş amaçlı olarak, bu hizmete abone olmak zorunda olmaksızın kullanan bir gerçek kişi" olarak tanımlanmıştır. Ayrıca "trafik verisini" "bir elektronik iletişim ağı üzerindeki bir iletişimin nakledilmesi veya faturalandırılması amacıyla işlenen herhangi bir veri" olarak, "İletişim"'i ise, "kamuya açık bir elektronik iletişim hizmeti aracılığıyla sınırlı sayıda taraf arasında değiştirilen veya iletilen her türlü bilgi" olarak tarif edilmektedir.

C. Konsey Çerçeve Kararı 2008/977 / JHA ve Direktif (AB) 2016/680

57. Cezai konularda polis ve adli işbirliği çerçevesinde işleme tabi tutulan kişisel verilerin korunması ile ilgili 27 Kasım 2008 tarih ve 2008/977 / JHA sayılı Konsey Çerçeve Kararı (bundan sonra Veri Koruma Çerçeve Kararı olarak anılacaktır- OJ 2008 L 350, s. 60); kişisel bilgilerin, bir suçun önlenmesi, soruşturulması, tespit edilmesi veya yargılanması ya da bir cezanın infaz edilmesi amacıyla işleme tabi tutulması halinde gerçek kişilerin kişisel verilerinin korunmasının temin edilmesini amaç edinmiştir. Veri Koruma Çerçeve Kararı, büyük ölçüde, 1981 Sözleşmesi ve Veri Koruma Direktifinde yer alan ilke ve tanımlara dayanmaktadır.

58. Suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezaların infazı amacıyla yetkili şahıslar tarafından kişisel verilerin işlenme tabi tutulması bu tür verilerin serbest dolaşımı nedeniyle gerçek kişilerin korunması ve 2008/977 / JHA sayılı Konsey Çerçeve Kararının yürürlükten kaldırılması (OJ 2016 L 119, s. 89), konusundaki 27 Nisan 2016 tarihli Avrupa Parlamentosu ve Konsey Direktifi (AB) 2016/680 diğerlerinin yanı sıra, cezai suçların soruşturulması ve kovuşturulması amacıyla polis ve adli makamlar gibi yetkili makamlarca verilerin işlenmesini düzenlemektedir. 3. Maddenin 1. fıkrasında Genel Bilgi Koruma Yönetmeliğinde ve rapor 21'de olduğu gibi tanımlama araçlarına ilişkin aynı tanımlayıcı ifade olan "tanımlanabilir gerçek kişi" tabiri kullanılmıştır. (bkz. Yukarıdaki 55. paragraf). Ayrıca, 4. Maddeye göre, kişisel verilerin, *diğerlerinin yanı sıra*,

yasal ve adil bir şekilde işleme tabi tutulması şart koşulmaktadır. 1. Maddenin (3). fıkrası, üye devletlerin direktifte yer alanlardan daha yüksek güvenceler sağlayabileceğini öngörmektedir.

59. 6 Mayıs 2018 tarihinden geçerli olmak üzere Direktif, 2008/977 / JHA sayılı Çerçeve Kararı'nın yerini almıştır.

D. Avrupa Birliği Adalet Divanı'nın Emsal Kararları

60. Veri Koruma Direktifinin 2 (a) Maddesi kapsamındaki "kişisel veri" kavramı ile ilgili olarak, Avrupa Birliği Adalet Divanı (CJEU), 24 Kasım 2011 tarihli *Scarlet Extended* kararında , (C-70/10, AB: C: 2011: 771, paragraf 51), kullanıcıların IP adreslerinin "bu kullanıcıların tam olarak tespit edilmesine imkan tanıdığı için kişisel verileri olarak korunacağına" karar vermiştir.

61. Avrupa Birliği Adalet Divanı 19 Ekim 2016 tarihli *Breyer* kararında, (C-582/14, AB: C: 2016: 779, dinamik IP adreslerinin özel mahiyetini incelemiştir. Aşağıdaki hususları not etmektedir:

> "[15] IP adresleri, internet üzerinden iletişimi sağlamak için ağa bağlı bilgisayarlara atanan rakamlar serisidir. Bir web sitesine erişildiğinde, erişmek isteyen bilgisayarın IP adresi, erişilecek web sitesinin depolandığı sunucuya iletilir. Bu bağlantı, erişilen verilerin doğru alıcıya aktarılabilmesi için gereklidir.
>
> [16] Ayrıca, referans sırasına göre ve Mahkeme önündeki belgelere göre İnternet servis sağlayıcılarının, internet kullanıcılarının bilgisayarlarına ya bir 'statik' IP adresi ya da 'dinamik' bir IP adresi, yani İnternete her yeni bir bağlantı yapıldığında değişen bir IP adresi tahsis ettikleri açıktır. Statik IP adreslerinden farklı olarak dinamik IP adresleri, belirli bir bilgisayar ile internet servis sağlayıcısının kullandığı ağa yapılan fiziksel bağlantı arasında halka açık erişilebilir bir dosya aracılığıyla bağlantı kurulmasını sağlamaz. "

62. Avrupa Birliği Adalet Divanı, dinamik bir IP adresinin "belirlenmiş bir gerçek kişi" ile ilgili bilgi oluşturmadığı görüşündedir. Çünkü böyle bir adres, bir web sitesinin erişildiği bilgisayarın kullanıcısı olan gerçek kişinin ya da o bilgisayarı kullanmış olabilecek başka bir kimsenin kimliğini doğrudan ortaya koymamaktadır. (a.g.e § 38) Avrupa Birliği Adalet Divanı, bir İnternet medya hizmeti sağlayıcısı tarafından kaydedilmiş olan bir dinamik IP adresinin, Veri Koruma Direktifinin 2 (a) Maddesi anlamında "tanımlanabilir bir gerçek kişi" ile ilgili veri olarak değerlendirilip değerlendirilemeyeceğine karar vermiştir. Bu amaçla, Avrupa Birliği Adalet Divanı, 26 nolu rapora dayanarak, çevrimiçi medya hizmeti sağlayıcısının elinde bulunan dinamik IP adresini İnternet servis sağlayıcısı tarafından tutulan ek verilerle birleştirme imkanının veri konusunun tanımlanması için makul bir araç olup olmadığını değerlendirmiştir. (§§ 41 ve 45). Avrupa Birliği Adalet Divanı bu noktada aşağıdaki gibi bir sonuca varmıştır.

"[49] Yukarıdaki tüm hususları dikkate alarak, ilk soruya verilen cevap şöyledir; 95/46 sayılı Direktifin 2. Maddesinin (a) fıkrası, kamuya açık hale gelmesine neden olacak şekilde bir kişinin bir web sitesine eriştiğinde, dinamik IP adresinin bir çevrimiçi medya hizmeti sağlayıcısı tarafından kaydedilmesi halinde, internet servis sağlayıcısının bu kişi hakkında sahip olduğu ek verilerle veri konusunun tespit edilmesini sağlayan yasal araçlara sahip olduğu durumlarda, bu hükümler bağlamında kişisel veri oluşturduğu şeklinde yorumlanmalıdır.

V. KARŞILAŞTIRMALI HUKUK

A. Alman Federal Anayasa Mahkemesi

63. Başvurucu, 24 Ocak 2012 tarihli BVerfG, 1 BvR 1299/05 sayılı Alman Federal Anayasa Mahkemesi'nin ("AFAM") kararına atıfta bulunmuştur. Alman Federal Anayasa Mahkemesi, *diğerlerinin yanı sıra*, telekomünikasyon servis sağlayıcıları tarafından saklanan dinamik IP adreslerine ilişkin bilgilerin manuel olarak alınmasıyla ilgili şikayetleri kısmen kabul etmiştir.

64. Telekomünikasyon Yasası'nın ("TY") 113. Maddesine göre, telekomünikasyon hizmet sağlayıcıları, (kolluk birimleri de dahil) yetkili mercilerin talebi üzerine, toplanan bazı verileri *diğerlerinin yanı sıra*, cezai veya idari suçların soruşturulması amacıyla ilgili mercilere vermek zorundadır. İtiraz konusu yasal hüküm, mümkünse tüm telekomünikasyon numaralarını kendi abonelerine (ve en nihayetinde, kullanıcılarına) tahsis edebilmesi için öngörülmüştür. Alman Federal Anayasa Mahkemesi tarafından kabul edildiği gibi, bu hüküm kapsamını daha ayrıntılı olarak tanımlayabilecek herhangi bir spesifik ihlal eşiği öngörmemiştir. Bunun yerine, mezkur görevleri yerine getirmek için gerekliyse, her zaman bireysel bazda bilgilere izin verilmiştir. Alman Federal Anayasa Mahkemesi bunu kendi içinde anayasaya aykırı bulmamıştır. Ancak, aynı zamanda ortaya çıkan sorun, söz konusu hükmün, dinamik bir IP adresinin sahibi ile ilgili bilgileri de içermesidir. Başlangıçta, Alman Federal Anayasa Mahkemesi, abone bilgileri ile kendisine atfedilebilecek önceden mevcut içerik bilgisi arasındaki bağlantıyı ele almıştır. Aşağıdaki şekilde karar vermiştir: (§113, Alman Federal Anayasa Mahkemesi'nin web sitesinde sunulan bir çeviriden alıntı)

"... Telekomünikasyonun gizliliği [Temel Yasanın 10.1 maddesi], hizmet sağlayıcılar tarafından belirli abonelere tahsis edilen telekomünikasyon numaraları gibi telekomünikasyon hizmetlerinin her bir kaydının gizliliğini korumaz. "

65. Alman Federal Anayasa Mahkemesi, statik ve dinamik IP adresleri arasındaki ayrımı aşağıdaki gibi belirtmiştir: (§§ 115 ve 116);

"...Statik bir IP adresinin belirli bir abone ile ilişkilendirilmesi - daha kesin bir ifade ile abonenin ağ arayüzüne bağlanması- kural olarak, söz konusu kişinin telekomünikasyon olayları hakkında da dolaylı bilgi verir, çünkü bu adresler, Statik olsa bile kayıt altına alınmıştır ve tam olarak sadece belirli iletişim olaylarıyla

bağlantılı olan kişiyi tanımlayan özellikleri ortaya koymaktadır. Aynı zamanda, bu bağlamda bilginin iletilmesi münhasıran, abonenin ve numaranın soyut olarak ilişkilendirilmesi ile sınırlıdır.

... Buna karşılık, bu adresler özellikle belirli telekomünikasyon olaylarıyla yakından ilgili olduğundan dinamik IP adresleri tanımlanmış kişilerle ilişkilendirildiğinde durum farklıdır. Bu ilişkilendirme, Temel Yasanın 10.1 maddesinin koruma alanı içerisindedir. Bununla birlikte, bu, bir dinamik IP adresinin ilişkilendirilmesi, her zaman zorunlu olarak, dolaylı olarak bilgi sağlayan belirli bir telekomünikasyon olayı ile ilgili olması durumunda otomatik olarak takip etmez. Bu bağlamda, bilgilerin kendisi sadece bir aboneye soyut olarak atfedilen verilerle ilgilidir. Bu nedenle, statik IP adreslerinin ilişkilendirilmesinden temel bir farkı yoktur. Ancak, Temel Yasanın 10.1 maddesinin uygulanması, telekomünikasyon işletmeleri dinamik bir IP adresini tespit etmesi halinde, müşterilerinin ilgili bağlantı verilerini incelemek zorunda oldukları gerçeğine dayanmaktadır. Yani işletmeler belirli telekomünikasyon olaylarına erişmek zorundadırlar. Servis sağlayıcılar tarafından ayrı ayrı saklanan bu telekomünikasyon bağlantıları, hizmet sağlayıcılar tarafından yasal bir görev kapsamında hazır halde tutulup tutulmadıkları... veya sözleşme temelli olarak saklayıp saklamadıklarına bakılmaksızın, telekomünikasyon gizliliğine tabidirler. Yasama organı, telekomünikasyon işletmelerinin devletin görevlerini yerine getirme konusundaki çıkarları doğrultusunda bu verilere erişme ve bunları değerlendirmeleri için sorumluluk yüklediği ölçüde, bu, Temel Kanunun 10.1 maddesine aykırıdır. Bu durum sadece servis sağlayıcılarının bağlantı verisini kendilerine sağlaması gerektiğinde değil, aynı zamanda verileri bir ön sorun olarak kullanmak zorunda olduklarında da söz konusudur. ”

66. Alman Federal Anayasa Mahkemesi, Telekomünikasyon Yasası’nın 113.1 maddesinin, Dinamik IP adresleri hakkında bilgi temini için temel teşkil ettiği ölçüde, Temel Yasanın 10.1 maddesine aykırı olduğu sonucuna varmıştır.

67. Ayrıca, Alman Federal Anayasa Mahkemesi, statik IP adresi ile ilgili verilerin otomatik olarak alınmasını (Telekomünikasyon Yasası’nın 12 maddesi) anayasaya aykırı olarak bulmamış olsa da, bu tür adreslerin aşağıdaki bağlamda sınırlı kullanımına karşı bir tespitte bulunmuştur (§§ 160 ve 161):

“... Halihazırda uygulamada halka açık bir şekilde erişilebilir durumda olan statik IP adreslerinin tahsisi, esasen kurumlar ve büyük ölçekli kullanıcılar ile sınırlıdır. Bu tür sayıları alma olasılığı, bu koşullarda çok az önem ifade etmektedir.”

Bununla birlikte, Telekomünikasyon Yasasının 112. Maddesi, gelecekte İnternet Protokolü Sürüm 6 temelinde, statik IP adresleri internet iletişiminin temeli olarak daha yaygın bir şekilde kullanıldığında, büyük ölçüde daha fazla zarar getirebilecektir. Bir IP adresinin belirlenmesi ile yapılan müdahalenin ağırlığı sorusu, esas olarak, bir IP adresinin teknik olarak dinamik mi, yoksa statik mi olduğuna bağlı olmayıp, (- somut olayda bir takım temel haklar uygulansa bile) ve ancak bu bağlamda bilgi ile ilgili görevin oluşturulmasının mevcut önemine bağlıdır. Fakat pratikte, statik IP adresleri de özel şahıslara büyük ölçüde tahsis edilirse, bu muhtemelen internet kullanıcılarının kimliğinin geniş çaplı veya en azından büyük ölçüde belirlendiği ve İnternet’teki iletişim olaylarının sadece sınırlı bir süre için değil, kalıcı olarak da çözülmesi (de-anonymization) anlamına gelebilir. İnternette iletişimin böylesine geniş kapsamlı bir şekilde çözülme (de-anonymisation) olasılığı, geleneksel bir telefon numarası kaydı etkisinin ötesine geçmektedir. ...Bir IP adresinin bir aboneye

atfedilmesinden etkilenen kişi için var olan önem, bir telefon numarasının tespit edilmesine eşit olmayabilir, çünkü birincisi, kapsamı ve içeriği oldukça geniş olan bir bilgiye erişmeyi mümkün kılmaktadır. ....Bu artan bilgi potansiyeli göz önünde bulundurulduğunda, IP adreslerinin tespitine dair genel olasılığa, anayasal olarak yalnızca daha dar sınırlara tabi olarak izin verilebilir. ”

B. Kanada Yargıtayı

68. *R v. Spencer* (2014 SCC 43, [2014] 2 SCR 212) davası, çocuk pornografisi içeren çevrimiçi dosya paylaşımına ilişkin olarak polisin elde ettiği dinamik IP hakkında temyiz talebinde bulunanın kız kardeşine ait abone bilgilerinin mahkeme kararı olmaksızın alınmasına ilişkindir. İnternet Servis Sağlayıcısından alınan abone bilgilerine dayanarak, polis, temyize başvuran kişi ile ilgili arama kararı almıştır. İkincisinde, polisin mahkeme kararı olmadan İnternet Servis Sağlayıcısından bu kişinin adresini elde edilmesi Kanada Hak ve Özgürlük Sözleşmesi’ne aykırı bir arama anlamına gelmesi gerekçesiyle bilgisayarında bulunan delillerin dosyadan çıkarılmasını talep etmektedir. 13 Haziran 2014 tarihli Kanada Yargıtay’ının (“KY”) temyiz başvurusunda bulunanın lehine olan kararı, Yargıç Cromwell tarafından yazılmıştır.

69. Konuyla ilgili önceki içtihada atıfta bulunan kararda, gizlilik standardının meşru beklentisinin basit bir şekilde tanımlayıcı olmaktan çok normatif olduğunu, gizliliğin korunması için hükumetin eyleminin uzun vadeli sonuçları hakkında, makul bir şekilde bilgilendirilmiş kişinin bağımsız bakış açısıyla yapılan kaçınılmaz bir "değer yargıları ile yüklü" dür. (§ 18). Kanada Yargıtay’ında davaya bakan hakimin görüşüne aykırı olarak, temyiz eden kişinin sübjektif gizlilik beklentisinin, hassas bilgileri iletmek için ağ bağlantısını kullanan kişi olduğu gerçeği ile meşrulaştırıldığına karar vermiştir. Kararda, temyiz eden kişinin sübjektif gizlilik beklentisinin makul olup olmadığını belirlemek istenmiştir. Bu amaçla, karar iki durumda ele alınmıştır: birincisi, söz konusu gizlilik menfaatinin tehlikede olmasıdır. İkincisi ise İnternet Servis Sağlayıcılarının abone bilgilerini vermelerini düzenleyen yasal ve sözleşmesel çerçevedir. Önceden olduğu gibi, Yargıç Cromwell aşağıdaki sonuçlara ulaşmıştır:

“[31 Dolayısıyla, araştırmanın konusunu nitelendirmede diğer kişisel bilgilerle ilgili çıkarımları desteklemeye yönelik bilgi trendinin dikkate alınması gerektiği açıktır.

[36] ... Analiz, araştırılan alanın ya da aranan şeyin gizliliğine ve araştırmanın hedefine olan etkilerine bağlıdır. Fakat aranan şeyin yasal ya da yasadışı niteliğine bağlı değildir...

[41] İnternet kullanımı bağlamında özellikle önemli olan üçüncü bir, bilgi gizliliği kavramı da bulunmaktadır. Gizliliğin anonimlik olarak anlaşılması budur. Benim

görüşüme göre, 8. Maddede (makul olmayan arama yada el koymaya karşı güvence hakkı) potansiyel olarak korunan gizlilik kavramı bu gizlilik anlayışını içermelidir.

[50] ...Bu davanın koşullarında, polisin belirli bir IP adresini abone bilgisi ile ilişkilendirmeyi talep etmesi, aslında belirli bir kişiyi (veya paylaşılan İnternet hizmetini paylaşan durumunda sınırlı sayıdaki kişiyi) belirli çevrimiçi etkinliklerle ilişkilendirmektir. Bu tür bir talep, şüpheliyi anonim olarak gerçekleştirilen çevrimiçi ve Mahkeme tarafından diğer şartlarda önemli gizlilik menfaatleri ile ilgili olarak tanınan aktivitelerle ilişkilendirmeye çalışarak, bilgisel gizlilik menfaatinin anonimlik yönünü ele alır...

[51] Dolayısıyla, polisin özel olarak gözlemlenmiş, anonim İnternet etkinliğine karşılık gelen abone bilgilerini almak için Shaw'a [İnternet Servis Sağlayıcı] başvurmasının yüksek düzeyde bir bilgi gizliliği ile ilgili olduğu sonucuna varıyorum. Bu noktada Caldwell J.A.'nın vardığı sonuca katılıyorum:

...Gizliliğin korunması ile ilgili akılcı ve bilgilendirilmiş bir kişi, birinin kendi evinde kendi bilgisayarını kullanarak gerçekleştireceği faaliyetlerin kişiye özel olacağı beklentisi içinde olacaktır. . .Benim kararımda, Açıklanmış Bilgilerin kişisel özelliklerinin Bay Spencer'ın kız kardeşi ile ilgili olması önemli değildir, çünkü Bay Spencer somut olayda polisin işleminin sonuçlarına şahsen ve doğrudan maruz kalmıştır... Bu itibarla, polisin işlemi, *ilk bakışta*, Bay Spencer'ın kişisel özel hayatın gizliliği hakkıyla ilgilidir ve bu bağlamda, açıklanmış bilgilerin gizliliği konusundaki menfaati doğrudan ve kişiseldir....”

70. Karar, ayrıca, savcılık makamlarının, çevrimiçi anonimlik hakkının tanınmasının suç dostu bir internet ortamının ortaya çıkmasına neden olacağı yönündeki kaygılarına da cevap vermektedir. Bu kaygının hafife alınamayacağını kabul ederken, Yargıç Cromwell bir çıkarın tanınmasının anonimlik hakkına eşit olamayacağını ve mevcut davada örneğin polisin abone bilgilerini almak için kolayca bir üretim talimatı alabileceğinin açık olduğunu ifade etmiştir.

71. İlgili sözleşme ve yasal hükümler karşısında gizlilik beklentisinin makul olup olmadığı sorusuyla ilgili olarak, Söz Konusu kararda, internet servis sağlayıcısının abonelerinin kişisel bilgilerinin toplaması, kullanması ve açıklaması, Ticari faaliyette bulunan kuruluşlar tarafından tutulan kişisel bilgilerin, ilgili olduğu kimsenin bilgisi veya rızası olmaksızın bilginin açıklanmasını engellemeyi teminat altına alan Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası'na (“PIPEDA”) tabi olduğuna karar verilmiştir. Kararda aşağıdaki tespitler yapılmıştır:

“[62] 7. Bölümün (3) (c.1) (ii) maddesi, söz konusu kurumun bilgileri elde etmek için yasal merciini belirlediği bir devlet kurumuna rıza bulunmaksızın bilgileri vermesine izin verir. Ancak mesele, bu tür yasal bir otorite olup olmadığıdır. Bu durum, kısmen, abone bilgilerine ilişkin makul bir gizlilik beklentisi olup olmadığına bağlıdır. Bu nedenle Bilgi Koruma ve Elektronik Belgeler Yasası makul bir gizlilik beklentisinin varlığına karşı bir faktör olarak kullanılamaz... Bilgi Koruma ve Elektronik Belgeler Yasası'nın amacı, diğer şeylerin yanı sıra, “kişisel bilgileri ile ilgili bireylerin özel hayatın gizliliği hakkını tanıyacak şekilde kişisel bilgilerin açıklanmasını” (s.3) düzenleyen kuralları belirlemektir. Polis tarafından yapılan basit bir talebin, kişisel bilgilerin, ilgilinin rızası hilafına açıklanması konusundaki Bilgi Koruma ve Elektronik Belgeler Yasasındaki yasağı delmeyeceği veya kişisel

bilgilerin açıklanması hususundaki sorumlulukları ortadan kaldırmayacağı beklentisi internet kullanıcıları için makul olabilir."

72. Kararda, polis talebinin hiçbir yasal yetkiye sahip olmadığını ve bu nedenle bu bilgilerin anayasaya aykırı olarak elde edildiği tespit edilmiştir. Mahkeme, bir suç mağduruyla yapılan görüşme gibi diğer polis rutin sorgularıyla paralel doğrultuda karar vermeyi reddetmiştir. *R. v. Duarte*, [1990] 1 S.C.R. 30, kararına atıfta bulunarak aşağıdaki tespitleri yapmıştır:

"[67] ...*Duarte* kararında Mahkeme, bir şüpheliyle yapılan görüşmeyi tekrarlayan bir kişi ile aynı görüşmenin ses kaydını tutan polis arasında ayrım yapmıştır. Mahkeme, tehlikenin "birisinin sözlerimizi tekrarlama riski değil, kendi özgür iradesinde, devletin sözlerimizi kayıt altına almasında ve iletmesine izin vermesindeki içsel sinsi bir tehlike" olduğuna hükmetmiştir.... Benzer şekilde, bu davada, polisin İnternet servis sağlayıcısından abone bilgisini vermesini talep etmesi, aslında Bay Spencer'ı polisin izlemesine konusu olan çevrimiçi aktiviteyle ilişkilendirilmeye yönelik bir taleptir ve böylece soruşturma sırasında polisin sorduğu basit bir sorudan daha önemli gizlilik menfaati ile alakalıdır."

HUKUKİ DEĞERLENDİRME

I. SÖZLEŞMENİN 8. MADDESİNİN İHLAL EDİLDİĞİ İDDİASI

73. Başvurucu, (i) İnternet hizmet sağlayıcısı (bundan böyle "İSS" olarak anılacaktır), söz konusu şahsi verileri yasadışı bir şekilde sakladığı ve (ii) 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 hayatın gizliliği hakkının ihlal edildiğinden bahisle şikayetçi olmuştur, Bunlar aşağıdaki gibidir:

"1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."

A. Kabuledilebilirlik

1. İnternet servis sağlayıcısı (İSS) tarafından kişisel verilerin yasadışı olarak saklandığı iddiasıyla ilgili olarak

74. Hükümet, başvurucunun, İSS tarafından kişisel verilerin yasadışı olarak saklanması hususunu yerel mahkemelerde şikayet konusu

yapmadığını ileri sürmüştür. Bu nedenle yerel mahkemeler ihtilafa konu kararlarında bu meseleyi ele almamışlardır. Ayrıca, İSS'nin özel bir kuruluş olması nedeniyle başvurucunun hukuk mahkemelerinde tazminat davası açabileceğini iddia etmiştir. Öyle yada böyle, hükümetin görüşüne göre başvurunun bu kısmı, iç hukuk yollarının tüketilmemesi nedeniyle kabuledilemez bulunmalıdır.

75. Buna ek olarak, Hükümet, başvurucunun kişisel verilerin saklanmasıyla ilgili 8. Maddenin ihlal edildiği iddiası konusunda mağdurluk sıfatının bulunmadığını, çünkü söz konusu verilerin başvurucu ile ilgili olmadığını, İnternet hizmeti abonesi olan babası ile ilgili olduğunu iddia etmiştir.

76. Başvurucu, İSS'nin kişisel verilerini, bu tür işlemler için açık bir yasal dayanak olmaksızın ve dolayısıyla Sözleşme'nin 8. maddesini ihlal ederek, yaklaşık altı ay sakladığını öne sürmüştür. Hükümet başvurucunun 15 Ekim 2015 tarihinde sunduğu görüşünde, İSS'nin kişisel verilerini gizli tutamadığı için veya yasal limitleri aşmasından dolayı değil devletin davaya konu verileri, hakkındaki bir ceza yargılamasında elde ettiği ve kullandığı için Mahkeme'ye başvuru yaptığını iddia etmiştir. Başvurucu ceza yargılaması boyunca, mahkemelerin yasadışı olarak elde edilen delillere dayandığını ileri sürmüştür.

77. Mahkeme, Hükümet'in başvuru ile ilgili mağdurluk statüsüne itiraz ettiğini hatırlatmaktadır. Ancak, başvurunun bu kısmı aşağıdaki nedenlerle kabul edilemez olduğu için bu itirazı ele almayı gerekli görmemektedir.

78. AİHM, AİHS'nin 35/1 maddesinin amacının, Sözleşmeci Devletlere aleyhlerindeki iddialar AİHM önünde sunulmadan önce bu iddiaları önleme ya da düzeltme fırsatını sağlamak olduğunu gözlemlemektedir. Sözleşme'nin oluşturduğu koruma mekanizması ilkesinin önemli bir yönü olan bu kural insan haklarına koruma sağlayan ulusal sistemlere ikincil niteliktedir.

Nitekim Mahkeme'ye sonradan yapılması öngörülen şikâyet, öncelikle, en azından özünde, iç hukukta belirlenen resmi şartlara ve zaman sınırlarına uygun olarak yetkili merci nezdinde yapılmış olmalıdır. (Bakınız diğerleri arasından, *Sejdovic v. Italy* [GC], no. 56581/00, §§ 43-44, ECHR 2006-II).

79. Mevcut davada, başvurucu, mahkemeye yaptığı başvurusunda kendi kişisel verileri olduğunu iddia ettiği verinin İSS tarafından saklanmasından şikayetçi olmuştur. Ancak bu konuda iç hukukta en azından özü itibariyle bir şikayette bulunmadığından dolayı iç hukuk yollarını tüketmemiştir.

80. Sonuç olarak, başvurunun bu kısmı Sözleşme'nin 35 §§ 1 ve 4. maddeleri kapsamında kabul edilmez bulunmuştur.

2. Abone bilgilerinin verilmesi ile ilgili olarak

81. Hükümet, İSS'nin polise verdiği abone bilgileri, babasına ait olduğu için başvurucunun mağdur olduğunu iddia edemeyeceğini ileri sürmüştür.

82. Başvurucu bu görüşe itiraz etmiştir. İhlal edilen gizliliğin aboneninki olmadığını, kendi gizliliğinin ihlal edildiğini ve söz konusu sorunun sahiplik olmayıp özel hayatın gizliliği hakkı olduğunu ifade etmiştir.

83. Mahkeme, bu konunun şikâyetin esasıyla yakından ilgili olduğunu ve bu nedenle Hükümetin esasa ilişkin itirazlarıyla birleştirilmesini işaret etmiştir.

84. Mahkeme bu şikâyetin, Sözleşme'nin 35 § 3 (a) Maddesi anlamında açıkça temelsiz olmadığını değerlendirmektedir. Ayrıca, kabul edilemez bulunması için başka bir neden de bulunmamaktadır. Bu nedenle başvuru kabuledilebilir bulunmuştur.

B. Esas Hakkında

1. Tarafların beyanları

(a) Başvurucu

85. Başvurucu, 1981 Sözleşmesi'ndeki kişisel verilerin tanımına atıfta bulunarak (bkz. Yukarıdaki paragraf 46) mahkeme kararı olmaksızın verilerin elde edilmesinin (yukarıdaki paragraf 7'ye bakınız) kimliğinin tespit edilmesine yol açtığını öne sürmüştür.

86. Ayrıca, iletişiminin içeriğini belirsiz bir kamuya açıklamasına rağmen, trafik (metraj) verileriyle ilgili, yani bu veriler internet kullanımının süresi ve zamanı, İnternet'i kimin kullandığı ve bu kullanım sırasında hangi siteye eriştiği ile ilgili verilerdir, gizlilik hakkından feragat etmediğini öne sürmüştür. Başvurucuya göre bu veriler bilgi ve iletişimin gizliliği de dahil özel hayat kavramı kapsamında ayrı bir korumadan yararlanırlar.

87. Bununla bağlantılı olarak, statik ve dinamik IP adresleri arasındaki önemli farkın kabul edilmesi gerektiğini belirtmiştir. Bilgisayar ve telefon numarasına sabit olarak atanan bir statik IP adresi arasında bir kıyas yapılması mümkün ise de; dinamik IP adresi İnternete her girildiğinde atanmaktadır. Alman Federal Anayasa Mahkemesinin 24 Ocak 2012 tarihli kararına atıfta bulunarak (bkz. Yukarıdaki 63. paragraf) başvurucu, internete girmek için kullanılan bilgisayarı ve dolayısıyla aboneyi tespit etmek için ekstra veri gerektirdiğinden, dinamik bir IP adresini seçerek (somut olayda abonenin sahip olduğu gibi), kişilerin kimliğini gizlemeyi tercih ettiklerini iddia etmiştir. Başvurucunun görüşüne göre, dinamik IP adresi, 149b (1) Maddesinin uygulandığı trafik verileri (ölçüm) kapsamına girmektedir.

88. Başvurucu ayrıca, Slovenya makamlarının katılımı olmadan iletişim içeriği hakkındaki verilerin elde edildiğine dikkat çekmiştir. Slovenya makamları, bu tür verilerin elde edilmesi için bir mahkeme kararına ihtiyaç

duyacaklardı. Ancak SCMK'nın 149b (3) maddesi temelinde abone bilgisini talep ederek gerekli olan usulü izlemekten kaçınmışlardır. İkincisine ilişkin olarak, başvurucu, Slovak polisinin kimliği ile ilişkili IP adresini elde ettiği tarihte, bu tür verilere erişimi düzenleyen kanunun açık olmadığı (*lex certa – belirlilik ilkesi*) ve dolayısıyla 8. maddenin ikinci fıkrasının gerektirdiği hukukilik şartının karşılanmadığını iddia etmiştir. Özellikle, müdahale tarihi itibariyle (Ağustos 2006), bu konuyla ilgili iç hukuk hükümleri çelişkilidir. Anayasanın 37. maddesinin ikinci fıkrasına göre iletişimin gizliliği hakkına müdahale ancak bir mahkeme kararı ile olabilir. Elektronik iletişim yasası, trafik verilerinin gizli tutulmasını ve bu iletişimin sadece yetkili bir makam tarafından verilen bir karar temelinde dinlenebileceğini öngörmüştür. Bu kararlar iç hukuk sisteminde sadece mahkeme kararı veya teorik olarak bir kovuşturma kararı olabilir. Her halükarda, 107. Maddesine göre saklanan belirli verileri devretmek değil sadece verileri saklamak mümkündür. Üstelik 104 Maddesine göre, servis sağlayıcılar, faturalandırma amacı için artık gerekli olmadığı zaman sakladıkları bu bilgileri silme yükümlülüğü altındadırlar. Diğer taraftan, SCMK'nın 149b (1) ve (3) maddeleri, verilere erişmek için farklı koşullar öngörmüştür ve uygulamada bu ikisi arasındaki ayrımın ne olduğu açık değildir. İç mevzuattaki bu belirsizliğin bir sonucu olarak, özel hayatın gizliliği hakkına kamu otoriteleri tarafından yapılacak keyfi bir müdahaleye karşı yasal korumanın yeterli olduğu söylenemez..

89. Başvurucuya göre, Elektronik Haberleşme Yasası SCMK'ya göre daha üst hüküm (lex specialis) niteliğindedir ve kişisel verilerin polise verilmesine olanak tanımamıştır. Yasadaki bu tür bir boşluk durumunda, Anayasa doğrudan uygulanmalı ve Anayasa, açıkça bu verilerin verilmesi için bir mahkeme kararını şart koşmaktadır.

(b) Hükümet

90. Hükümet IP adreslerinin kişisel veriler olduğunu ve benzer şekilde dinamik IP adreslerinin de kişisel veriler olduğunu ancak bunların trafik verisini oluşturmadığını ifade etmiştir. Bu ikisi arasındaki tek fark, statik IP adresi, İSS değiştirilmediği sürece abone ile kaldığı halde, Dinamik IP'de abone internete her bağlandığında yeni bir dinamik IP adresi tahsis edilmektedir. Her ikisiyle ilgili olarak, belirli bir IP adresinin kullanım zamanına ilişkin verileri İSS kayıt altında tutmaktadır.

91. Hükümet, yalnızca bilgisayarlara el konulması ve incelenmesi sonrasında ve başvurucunun adresinde yaşayanların sorgulanmasından sonra soruşturmada başvurucuya odaklanıldığını iddia etmiştir. Böylece, başvurucu ile abone arasındaki bağlantı, geçerli bir mahkeme kararına göre icra edilen ev aramasından sonra ortaya çıkmıştır.

92. IP adresinin, bir şahsın kimliğinin tespit edilmesine olanak tanıdığı için kişisel verilerin bir öğesi olduğu hususunu kabul ederken, Hükümet

kişisel verilerin ve / veya belirsiz ve sınırsız bireyler topluluğuna, iletişimin içeriğinin açıklanmasına yol açan bir web sitesine girilmesinin her kullanıcının kendi tercihi olduğuna işaret etmiştir. Hükümet, başvurucunun, dosya paylaşım programına erişim için kullandığı IP adresini gizlediğini iddia etmediğini öne sürmüştür. IP adresinin açıklanması yada verilmesi, abone bilgilerinin açıklanması anlamına geldiği için, başvurucunun kimliğini özel ve gizli tutmak niyetinde olmadığını ve bu nedenle özel hayatın gizliliği hakkı mevcut davada uygulanamayacaktır.

93. Hükümet, başvurucunun, dinamik IP adresi ile ilgili abone bilgilerinin polisten gizlenmiş olmasını bekleyemeyeceğini iddia etmiştir. Onların görüşüne göre, itiraza konu tedbirler, özellikle savunmasız bireyler olarak, Sözleşme kapsamında özel korumadan yararlanan çocukların bütünlüğünü koruma amacı içinde hukuki ve orantılı olmuştur.

94. Hükümet, sürüş sırasında kapalı devre televizyon kamerasına bir şüphelinin yakalandığı durumla paralellik kurmaktadır. Böyle bir durumda, şüphelinin fotoğrafı ve plaka numarası onu teşhis etmek için yeterli olacaktır. Benzer şekilde, mevcut davada, polisin dinamik IP adresi ve kullanımının zaman çizelgesine sahip olduğu anda, kullanıcının bu verilerle tespit edilebileceği varsayılmalıdır. Hükümet, bu nedenle, yerel mahkemelerin, bir iletişim cihazının sahibi veya kullanıcısı ile ilgili veriler için değil de ilgili trafik verileri hakkında 149b (1) yerine, 149b (3) Maddesini doğru bir şekilde uyguladıklarını ileri sürmüştür.

2. Mahkemenin Değerlendirmesi

(a) İlk gözlemler ve Mahkeme'nin değerlendirmesinin kapsamı

95. Mahkeme, başlangıçta, dinamik bir IP adresiyle ilişkili abone bilgilerinin açıklanmasıyla ilgili mevcut davaya özgü bir muhtevanın olduğunu gözlemlemektedir. Mahkeme, Avrupa Birliği içinde kişisel verilerin korunması ve elektronik haberleşmenin gizliliğine ilişkin kapsamlı mevzuat ve içtihatlara dikkat çekmekte ve somut olaya uygulanabilecek olan bazı teknik hususların değerlendirilmesinde bunlara ve diğer ilgili karşılaştırmalı hukuk esaslarına dayanmaktadır. Aynı zamanda uygun olduğu kadar, bu konudaki mevcut hukuki doktrinler de dikkate alınacaktır.

96. Bir ön sorun olarak, ayrıca Mahkeme, IP adresinin, bir ağdaki her bir cihaza atanan, cihazların birbirleriyle iletişim kurmasını sağlayan, benzersiz bir numara olduğunu kaydetmektedir. Bir aygıtın belirli bir ağ arabirimine sabit olarak tahsis edilen statik IP adresinden farklı olarak, dinamik IP adresi cihazın Internet'e her bağlandığında geçici olarak İSS tarafından tahsis edilir.(bkz. yukarıdaki paragraf 61, 87 ve 90). Yalnızca IP adresi, kullanıcının bağlı olduğu İSS ve daha büyük bir fiziksel konum, büyük olasılıkla İSS'nin yeri gibi belirli detayların belirlenmesine olanak sağlamaktadır. Çoğu dinamik IP adresi, belirli bir bilgisayara değil, İSS'ye kadar takip edilebilir. Dinamik IP adresi kullanarak abonenin adını ve

adresini elde etmek için, İSS'nin normal olarak bu bilgiye bakması ve bu amaçla abonelerinin ilgili bağlantı verilerini incelemesi gerekir (bkz. Yukarıdaki paragraflar 61 ve 65).

97. Mevcut davada, dinamik IP adresi ve tahsis edildiği süre hakkındaki bilgiler, çocuk pornografisi materyalini içeren belirli İnternet ağının kullanıcılarına yönelik izleme faaliyeti yürüten İsviçre polisi tarafından toplanmıştır. Mevzubahis olan dinamik IP adresiyle ilişkili abonenin yani başvurucunun babasını adı ve adresini (yukarıda paragraf 6 ve 7'ye bakınız). İSS'den alan İsviçre polisi bu bilgileri Slovenya polisine aktarmıştır.

98. Hükümet, AİHS'nin 8. maddesinin başvurucunun itiraza konu tedbirden doğrudan etkilenmediği ve etkilenmiş olsa bile söz konusu olan dosyaları kamuya açık olarak paylaşmak suretiyle özel hayatın gizliliği hakkından feragat ettiği için bu davaya uygulanmayacağını öne sürmektedir (yukarıdaki paragraf 92 ve 93'e bakınız). Bu sorulara cevap verebilmek için, Mahkeme, başvurucunun veya İnternet kullanan herhangi bir başka kişinin, diğer kamuya açık çevrimiçi faaliyetlerinin anonim kalmaya devam edeceğine dair makul bir beklentisi olup olmadığını dikkate almalıdır (bkz. yukarıdaki paragraf 115 ila 118).

99. Mahkeme, bu bağlamda, cinsel istismarın mağdurlara karşı zayıflatıcı etkileri olan, tartışmasız nefret uyandıran bir suç olduğunu yinelemektedir. Çocuklar ve diğer savunmasız bireyler, özel hayatlarının temel unsurlarına yapılan bu türden çok ciddi müdahalelerden caydırıcı bir biçimde Devlet tarafından korunmalarını hak etmektedirler ve bu koruma suçluların tespitini ve yargı önüne çıkartılmalarını da kapsar. (bkz. *KU / Finlandiya*, no. 2872/02, § 46, AİHM 2008-V). Bununla birlikte, Hükumet'in 8. maddenin uygulanabilirliğine ilişkin olarak sorduğu sorular, söz konusu faaliyetin hukuki veya yasadışı niteliğinden bağımsız olarak cevaplanmalı ve Sözleşme koşullarına halel getirmeksizin savunmasız bireylerin korunması diğerlerinin yanı sıra, *KU v. Finlandiya* kararında işaret edildiği gibi, üye devletler tarafından teminat altına alınmalıdır (anılan).

(b) 8. Maddenin Uygulanabilirliği

(i) İlgili ilkelerin özetlenmesi

100. Mahkeme, özel hayatın, bir tanımla söylenip bitirilemeyecek kadar geniş bir terim olduğunu yinelemektedir. 8. Madde, diğerlerinin yanı sıra, kişilik ve kişisel gelişim hakkını ve diğer insanlarla ve dış dünyayla ilişkiler kurma ve geliştirme hakkını teminat altına almaktadır. Bu nedenle, kamusal anlamda bile "özel hayat" kapsamına girebilecek, kişilerin etkileşim alanı

mevcuttur (bkz. *Uzun v. Almanya*, no. 35623/05, § 43, AİHM 2010). -VI (özet).

101. Bir kişinin özel hayatının kendi evi veya özel mülkünün dışında kendisini etkileyecek tedbirler nedeniyle tehlikeye atılıp atılmadığının değerlendirilmesine dair bir dizi unsur vardır. "Özel yaşam" ve "haberleşme" kavramlarının uygulanıp uygulanmayacağını tespit etmek için, Mahkeme, birçok durumda bireylerin gizliliklerine saygı duyulması ve korunmasına dair makul bir beklenti içinde olup olmadıklarını ele almıştır. (bkz. *Bărbulescu / Romanya* [GC], no 61496/08, § 73, AİHM 2017 ve *Copland / Birleşik Krallık*, no. 62617/00, §§ 41-42, AİHM 2007-I). Bu bağlamda, Mahkeme, gizliliğe ilişkin makul bir beklentinin, olmazsa olmaz kesin bir etken niteliğinde olmasa da, kayda değer olduğunu ifade etmektedir (bkz. Yukarıda atıf yapılan *Bărbulescu*, § 73).

102. Kişisel veriler bağlamında, Mahkeme, "özel yaşam" teriminin dar bir şekilde yorumlanmaması gerektiğine dikkat çekmektedir. Geniş yorumun, 1981 Sözleşmesi'ndeki yorum ile örtüştüğünü, sözleşmedeki amacın "haklarındaki kişisel verilerin otomatik olarak işleme tabi tutulması ile ilgili olarak, her bir taraf devlet ülkesinde, ... her birey için, başta özel hayatın gizliliği olmak üzere kişilerin haklarına ve temel özgürlüklerine saygı duyulmasını güvence altına almak" (Madde 1) olduğu tespitinde bulunmuştur. Bu tür kişisel veriler "tanımlanmış veya tanımlanabilir bir bireyle ilgili herhangi bir bilgi" olarak tarif edilmiştir.(Madde 2) (bkz. *Amann - İsviçre* [GC], no. 27798/95, § 65, AİHM 2000 II; ayrıca bkz. Paragraf 46).

103. Ayrıca, Mahkeme, belirli bir kişi hakkında bir veri toplandığı durumlarda, kişisel verilerin işleme tabi tutulması veya kullanılması ya da söz konusu materyalin normal olarak öngörülebilir olanın ötesinde bir şekilde yayınlanmasının, ortaya çıktığına dair oturmuş içtihatlar ile uyuşmaktadır. (bkz. *Satakunnan Markkinapörssi Oy ve Satamedia Oy / Finlandiya* [GC], no 931/13, § 136, AİHM 2017 (özetler)). Bu nedenle Sözleşme'nin 8. maddesi, bireylerin, 8 maddedeki hakları ile bağlantılı bir biçimde ve tarzda tarafsız da olsa, kolektif olarak toplanan, işlenen ve yayılan, verilerle ilgili gizlilik haklarına dayanmalarına olanak sağlayarak, bir bilgi formunda kendi kaderini tayin etme hakkını düzenlemektedir. (a.g.e § 137).

104. Mahkeme, daha önce, aranan telefon numaralarını (bkz. *Malone / Birleşik Krallık,* 2 Ağustos 1984, § 84, Seri A no. 82), telefonla, e-postayla ve İnternet kullanımıyla ilgili kişisel bilgiler (bkz. *Copland*, yukarıda anılan §§ 41 ve 43), başvurucunun iş ilişkilerine ait soruşturma mercileri tarafından bir karta saklanan bilgiler (bkz. yukarıda anılan *Amann*, § 66), başvurucunun kamuya açık uzak geçmişiyle ilgili yetkililer tarafından saklanan bilgiler (bkz. *Rotaru / Romanya* [BD], 28341/95, §§ 43 ve 44, AİHM 2000 V) gibi ölçme verilerini 8. madde kapsamında ele almıştır.

105. Üstelik Mahkeme daha önce *Delfi AS / Estonya* kararında çevrimiçi anonimliğin önemini kabul etmiştir ([GC] No. 64569/09, § 147, AİHM 2015) ve bunun uzun süredir misilleme veya istenmeyen dikkatlerden kaçınmanın bir aracı olduğunu belirtmiştir. Böylelikle, özellikle internette fikir ve bilgi akışını önemli bir şekilde teşvik edebilir. Aynı zamanda, Mahkeme, geleneksel medya ile karşılaştırıldığında yasadışı konuşmanın internet üzerindeki etkilerini ciddi ölçüde ağırlaştırabilecek olan, internette bilginin yayılmasının kolaylığını, kapsamını ve hızını ve bir kez açıklandıktan sonra bilginin kalıcılığını göz ardı etmemektedir (a.g.e).

106. Yukarıda bahsi geçen davada Mahkeme ayrıca, çevrimiçi faaliyette bulunan farklı anonimlik derecelerine de değinerek aşağıdaki gibi tespitlerde bulunmuştur. (a.g.e. § 148):

> "Mahkeme, internette farklı anonimlik derecelerinin mümkün olduğunu kaydetmiştir. Bir internet kullanıcısı kamunun büyük çoğunluğuna anonim olabilirken, aynı zamanda ya doğrulanmamış ya da onaya tabi tutulabilen –sınırlı doğrulamadan (örneğin, bir hesabın e-mail adresi ya da sosyal ağ hesabı üzerinden aktif hale getirilmesi) kişinin çok daha güvenli kimliğe sahip olmasına olanak sağlayan ulusal elektronik kimlik kartları ya da online bankacılık kimlik denetimi kullanımı aracılığıyla güvenli yetkilendirmeye kadar uzanabilir - bir hesap ya da iletişim verisi aracılığıyla bir servis sağlayıcı tarafından kimliği belirlenebilir. Bir servis sağlayıcısı aynı zamanda kullanıcılarına oldukça geniş ölçüde anonimlik sağlayabilir; bu durumda, kullanıcıların kimliklerini belirtmelerine gerek duyulmamaktadır ve bu kullanıcılar, internet erişim sağlayıcılarının elinde bulunan bilgiler aracılığıyla –sınırlı ölçüde izlenebilir konumda olurlar. Bu tür bir bilginin verilmesi, soruşturma ya da yargı makamlarının bir kararını gerektirmekte olup, kısıtlayıcı şartlara tabi tutulmaktadır. Bununla birlikte, bazı durumlarda faillerin kimliklerinin tespit edilmesi ve kovuşturulmaları için gerekli olabilir."

(ii) Yukarıdaki ilkelerin mevcut davaya uygulanması

(α) İlgili menfaatin mahiyeti

107. Hükümet, abonelik bilgilerinin prensip olarak kişisel verilerle ilgili olduğuna itiraz etmemiştir. (bkz. yukarıdaki paragraf 90 ve 92). Böyle bir sonuç, 1981 Sözleşmesi, Avrupa Birliği mevzuatı ve bunların uygulanmasını amaçlayan ulusal mevzuatta yer alan tanımlar ile uyumludur. (bkz. yukarıda paragraf 40, 46, 53 ve 57).

108. Ayrıca, Mahkeme, belirli zaman için tahsis edilmiş dinamik IP adresleriyle ilişkili abone bilgilerinin kamuya açık olmadığını ve bu nedenle, geleneksel telefon rehberinde veya hükumet tarafından tescil edilen araç plakaları kamuya açık veri tabanında bulunan bilgilerle mukayese edilemeyeceğinin altını çizmektedir (bkz. yukarıda paragraf 94.). Aslında, belirli bir dinamik IP adresinin belirli bir zamanda tahsis edildiği bir aboneyi tespit etmek için, İSS'nin belirli telekomünikasyon olaylarıyla ilgili saklanan verilere erişmesi gerektiği görülmektedir (bkz., yukarıda paragraf

29, 61, 65 ve 95). Bu gibi depolanmış verilerin kullanımı başlı başına, özel yaşam mülahazalarına yol açabilir (bkz. yukarıda paragraf 103).

109. Ayrıca, Mahkeme mevcut davada abone bilgilerinin aranan özel durumunu göz ardı edemez. Abone bilgisini elde etmenin tek amacı, paylaştığı verileri açığa çıkartan bağımsız olarak toplanan içeriğin arkasındaki belirli bir kişiyi tespit etmektir. Mahkeme, bu bağlamda, "özel hayat" kapsamına girebilecek diğer kişilerle bir etkileşim alanı bulunduğuna işaret etmektedir bkz. yukarıdaki paragraf 100). Bu tür faaliyetlere ilişkin bilgiler, tanımlan veya tanımlanabilir bir bireye atfedildiği veya o bireyle ilişkilendirildiği andaki gizlilik ile ilgilidir (daha farklı bir bağlamda da olsa tanımlanabilirliğe atıfta bulunmak için bkz. *Peck - Birleşik Krallık, no. 44647/98, §). 62, AİHM 2003 I ve JS / Birleşik Krallık (dec.), No 445/10, §§ 70 ve 72, 3 Mart 2015)*. Bu nedenle, polis tarafından aranan çevresel bilgi gibi görünen, yani bir abonenin adı ve adresi, bu davada olduğu gibi, konu ile alakalı önceden var olan içeriği açığa vuran verilerle ayrılmaz bir şekilde bağlı olarak ele alınmalıdır (31 ve 34 üncü paragraflarda atıfta bulunulan Anayasa Mahkemesi yargıçlarının muhalif görüşlerine bakınız; yukarıdaki 69 ve 72. paragraflarda belirtilen Kanada Yargıtayı'nın ve yukarıda 64 ve 65. paragraflarda geçen Alman Federal Anayasa Mahkemesi'nin görüşleri ile karşılaştırınız). Aksi düşünüldüğünde, ilgi alanlarını, inançlarını ve kişisel yaşam tarzlarını da havi hassas bilgileri de içerecek şekilde, bireyin çevrimiçi faaliyeti hakkında birçok şeyi ortaya dökebilecek bilgi için gerekli korumayı da, reddetmek olacaktır.

110. Yukarıdaki değerlendirmeler ışığında, Mahkeme mevcut davanın, Sözleşme'nin 8. maddesinin koruma ile bağlantılı olabilecek gizlilik konuları ile ilgili olduğu sonucuna ulaşmıştır.

(β) Başvurucunun itiraza konusu tedbir ile tespit edilip edilmediği hususu

111. Mahkeme, Hükumet'in polis tarafından alınan abone bilgilerinde, başvurucunun değil, yalnızca başvurucunun babasının adının ve adresinin verildiğine ilişkin argümanını ele almalıdır (bkz. yukarıdaki 91. paragraf). Bu bağlamda, Mahkeme, kişisel veri tanımında, sadece hali hazırda tespit edilmiş olanları değil, aynı zamanda tespit edilebilecek bireylerin de kastedildiği hususunun genel olarak kabul edildiğini gözlemlemektedir.(bkz. yukarıda paragraf 40, 47, 53, 54, 55 ve 58).

112. Mevcut bağlamda, başvurucunun internet kullanıcısı olduğuna bkz. yukarıdaki 56. paragraf) ve polis tarafından izlenen çevrimiçi aktivitesi olduğuna dair şüphe yoktur. Mahkeme ayrıca başvurucunun, kendi evinde kendi bilgisayarından İnterneti kullandığını gözlemlemektedir. Polisin elde ettiği abone bilgisinde başvurucunun isminden bahsedilmemesi önem arz etmemektedir. Gerçekten de, bir ev halkının, ailenin birkaç üyesi tarafından

kullanılan İnternet hizmeti için tek bir abonelik yapmaları olağandışı bir durum değildir. İnternet'in kişisel kullanımıyla ilgili abone bilgileri açığa çıkarıldığında dolaylı olarak bağlantılı kurulacağından, İnternet hizmetine kişisel olarak abone olmamaları, gizlilik beklentilerini etkilemeyecektir.

113. Davaya konu tedbirin amacının, yani polisin, mahkeme kararı olmaksızın, İsviçre polisi tarafından sağlanan dinamik IP adresi ile ilgili abone bilgilerinin elde etmesi, (bkz. yukarıdaki paragraf 7), bilgisayar kullanımını bir yere ve potansiyel olarak bir kişiye bağlamaktır. Adresi de içeren abone bilgileri, polisin söz konusu İnternet bağlantılarının yapıldığı evi tespit etmesine olanak sağlamıştır. Bu, başvurucunun Razorback ağının şüpheli kullanıcısı olduğunu tespit etmelerine yol açmıştır

114. Yukarıda belirtilenleri göz önünde bulundurarak ve ayrıca, yerel mahkemelerin başvurucunun söz konusu İnternet hizmetine abone olmadığı gerekçesiyle davayı reddetmediğini de dikkate alarak, Mahkeme, bu durumu, mevcut davada 8. maddenin uygulanmasında bir sorun olarak değerlendirmemektedir. Bu doğrultuda Hükümet'in, mağdurluk statüsünün bulunmadığı iddiasıyla ilgili itirazını reddetmiştir (bkz. yukarıdaki paragraf 83).

(γ) Başvurucunun makul bir gizlilik beklentisi olup olmadığı

115. "Özel yaşam" kavramının mevcut davaya uygulanıp uygulanamayacağını tespit edebilmesi için, Mahkeme, söz konusu ağın kamuya açık olarak erişilebilir niteliği göz önünde bulundurulduğunda, başvurucunun gizliliğine saygı gösterileceği ve korunacağı konusunda makul bir beklentisi olup olmadığını incelemeye devam edecektir (bkz. yukarıda paragraf 101). Bu bağlamda, Slovenya Anayasa Mahkemesi ve davalı Hükümet (bkz. yukarıda paragraf 29'da atıfta bulunulan Anayasa Mahkemesi kararının 14 ve 18. paragrafları ve ayrıca bkz. yukarıdaki paragraf 92), başvurucunun erişimin kısıtlanmadığı Razorback ağına katılmasını önemli bulmuştur. Çevrimiçi etkinliğini ve bağlantılı dinamik IP adresini bilerek kamuoyuna açıkladığını değerlendirmektedirler. Bu nedenle, kendi görüşlerine göre, gizlilik beklentisi meşru değildir ve dahası, bundan feragat ettiği düşünülebilirdi (a.g.e).

116. Mahkeme, Anayasa Mahkemesi gibi, başvurucunun, Razorback ağından pornografik materyalleri paylaşırken, öznel açıdan, bu faaliyetin gizli kalacağı ve kimliğinin açıklanmayacağı beklentisi içinde olduğunu kabul etmektedir (bkz. yukarıda 29. paragrafta belirtilen Anayasa Mahkemesinin kararının 12. paragrafı). Bununla birlikte, Anayasa Mahkemesinin aksine, Mahkeme, başvurucunun kendi dinamik IP adresini gizlememesinin, bunun mümkün olduğunu varsayarak, gizlilik beklentisinin, objektif bir bakış açısıyla makul olup olmadığının değerlendirilmesinde, belirleyici bir rolünün olmayacağını değerlendirmektedir. Bu bağlamda, Mahkeme, başvurucunun dinamik IP

adresini gizli tutma hususunda değil, kimliğiyle ilgili olarak makul bir gizlilik beklentisi içinde olup olmayabileceğinin açık olduğuna işaret etmektedir.

117. Mahkeme, daha önce, kullanıcıların mutlaka tanımlanabilir olmaksızın katıldığı çevrimiçi etkinliğin doğasıyla ilgili çevrimiçi gizliliğin anonimlik yönünü kabul etmiştir (bkz. yukarıda paragraf 105'de atıfta bulunulan *Delfi AS* kararı, ayrıca, yukarıda paragraf 29'da atıfta bulunulan Anayasa Mahkemesi kararının 12. paragrafına bakınız). Gizliliğin anonimliliği kavramı, mevcut değerlendirmede dikkate alınması gereken önemli bir faktördür. Özellikle, başvurucunun söz konusu çevrimiçi etkinliğinde kimliğini açıklamış olduğu (bu bağlamda, yukarıdaki paragraf 33'te belirtilen Yargıç Jadek Pensa'nın muhalif görüşüne bakınız) ya da örneğin belirli bir web sitesi sağlayıcısı tarafından bir hesap veya iletişim verileri aracılığıyla tanımlanabilir olduğu hususları iddia edilmemiştir. Bu nedenle, atanan dinamik IP adresinin, ağın diğer kullanıcıları tarafından görünür olsa bile, İSS'nin polisten gelen bir talep üzerine verileri incelemeden sözkonusu bilgisayara kadar takip edilemeyeceği gerçeğince teyit edildiğinden dolayı çevrimiçi aktivitesi yüksek derecede anonimlikle bağlantılıdır. (bkz. yukarıda paragraf 105'de atıf yapılan *Delfi AS*, § 148),

118. Son olarak, Mahkeme, uygulanabilir hukuk ve mevzuat çerçevesinin, makul gizlilik beklentisinin tespitinde kesin olarak belirleyici bir faktör olmasa da, amaca uygun olabileceğini belirtmektedir (bkz. Örneğin, yukarıda belirtilen *J.S. /Birleşik Krallık* (karar). § 70 ve Peev / Bulgaristan, no. 64209/01, § 39, 26 Temmuz 2007). Mevcut davada, taraflardan hiçbiri, İnternet hizmetinin başvurucunun babasına sağlanması ile ilgili abonelik sözleşmsinin şartlarına ilişkin bilgi sunmamışlardır. Yasal çerçeve ile ilgili olarak, Mahkeme, yazışma ve haberleşmenin gizliliğinin Anayasa'nın 37. maddesi ile güvence altına aldığını ve bu hakka yapılacak herhangi bir müdahalenin mahkeme kararına dayanmasının şart koşulduğunu belirtmeyi yeterli görmektedir (bkz. yukarıda paragraf 35). Bu nedenle, olay zamanında yürürlükte olan mevzuat açısından, başvurucunun çevrimiçi faaliyetine ilişkin gizlilik beklentisinin teminatsız veya akıldışı olduğu söylenemez.

(δ) Sonuç

119. Yukarıdaki tüm gerekçelerle, Mahkeme, başvurucunun kendi çevrimiçi etkinliğiyle ilgili kimliğini korunması konusundaki menfaati "özel yaşam" kavramının kapsamına girdiği ve bu nedenle 8. Madde'nin bu şikayete uygulanabileceği sonucuna varmıştır.

(c) 8. Maddeye uygunluğu

(i) Müdahalenin olup olmadığı

120. Yukarıdaki sonuca göre, başvurucunun 8. maddenin 1. fıkrası ile güvence altına alınan özel hayata saygı hakkı mevcut dava ile bağlantılı olup, Mahkeme ayrıca, polisin İSS'den talepte bulunması ve başvurucunun kimliğinin ortaya çıkmasına yol açan abonelik bilgilerini kullanması bu hakka bir müdahale oluşturmuştur. (*bkz. uyduğu ölçüde,* yukarıda adı geçen *Rotaru, § 46 ve Uzun, § 52*). Yukarıda belirtilenler göz önünde bulundurulduğunda, söz konusu tedbirin, başvurucunun haberleşmelerine saygı gösterilme hakkına yapılan bir müdahaleye de neden olup olmadığını belirleme gerekli görülmemiştir.

121. Mahkeme, bu nedenle, başvurucunun gizlilik hakkına yapılan müdahalenin, 8. maddenin ikinci fıkrasındaki koşullarla uyum içinde olup olmadığını, başka bir deyişle "yasaya uygun" olup olmadığını, bu paragrafta öngörülen meşru amaçları güdüp gütmediğini ve söz konusu amaç ya da amaçlara ulaşmak için "demokratik bir toplumda gerekli" olup olmadığını incelemelidir.

(ii) Müdahalenin yasaya uygun olup olmadığı

122. Mahkeme, ilk olarak Sözleşmenin 8 § 2 Maddesi anlamı dahilinde, "yasaya uygunluk" ifadesinin, itiraza konu tedbirin iç hukukta bir temelinin bulunması gerektirdiğini kaydetmektedir. İkincisi, iç hukuk ilgili kişiye erişilebilir olmalıdır. Üçüncüsü, etkilenen kişi iç hukukun sonuçlarını kendisi açısından öngörebilmelidir ve dördüncüsü iç hukukun, hukukun üstünlüğü ile uyum içinde olması gereklidir. (bkz., diğer birçok otoriteler arasında, *Rotaru,* yukarıda anılan, § 52; *Liberty ve Diğerleri / Birleşik Krallık,* no. 58243/00, § 59, 1 Temmuz 2008 ve *Sallinen ve Diğerleri / Finlandiya,* no. 50882 / 99, § 76, 27 Eylül 2005).

123. Mahkeme ayrıca, bu prensiplerin iç hukukun yorumlanması ve uygulanması için öncelikle ulusal makamlar, özellikle de mahkemeler için olduğunu yinelemektedir. Ancak, Mahkeme, iç hukukun yorumlanıp uygulanma biçiminin, AİHM'nin içtihatları ışığında yorumlandığı gibi, Sözleşme'nin prensipleri ile uyumlu sonuçlar doğurup doğurmayacağını incelemek zorundadır (Bkz. *Cocchiarella v. İtalya* [GC], no. 64886/01, §§ 81 and 82, AİHM 2006-V).

124. Mevcut davada, söz konusu dinamik IP adresi ile ilişkili abone bilgilerinin polis tarafından elde edilmesinin, SCMK'nın 149b (3) maddesinde polisin, elektronik iletişim aracının sahibi yada kullanıcısına ilişkin bilgileri İSS'den alabilmesi öngörüldüğünden dolayı (bkz. yukarıdaki 36. paragraf), iç hukukta bir temeli olduğu varsayılsa da, Mahkeme, bu kanunun erişilebilir ve öngörülebilir olup olmadığını ve hukukun üstünlüğü ile uyumlu olup olmadığını incelemelidir.

125. Mahkeme, mevcut davanın hukuka erişilebilirlikle ilgili herhangi bir sorun ortaya çıkarmadığını kaydetmektedir. Mahkeme, bir kimsenin davranışını düzenlemesine imkan tanıması için yeterli hassasiyetle formüle edilirse, - uygun tavsiyede bulunulması gerekiyorsa- bir kuralın "öngörülebilir" olduğunu yineler. (bkz. yukarıda anılan, bkz. *Rotaru*, § 55 ve orada özetlenen ilkeler). Buna ek olarak, hukukun üstünlüğü ile uyumlu olmak, iç hukukun 8. maddeye ilişkin keyfi hak ihlallerine karşı yeterli koruma sağlamasını gerektirir (bkz. *uygun olduğu ölçüde*, *Amann*, yukarıda anılan, §§ 76-77; *Bykov / Rusya* [BD], no. 4378/02, § 76, 10 Mart 2009, ayrıca bkz. *Weber ve Saravia / Almanya* (karar), 54934/00, § 94, AİHM 2006 XI ve yukarıda anılan Liberty ve Diğerleri, § 62). Mahkeme bu nedenle, istismara karşı yeterli ve etkili güvencelerin bulunduğu konusunda da ikna olmalıdır. Bu değerlendirme, muhtemel tedbirlerin niteliği, kapsamı ve süresi, bunların verilmesi için gerekli gerekçeler, izin verme, yürütme ve denetleme yetkisi olan makamlar ve iç hukuk tarafından sağlanan hukuk yolları gibi, davanın tüm koşullarına bağlıdır. (bkz. *Avrupa Entegrasyonu ve İnsan Hakları Derneği ve Ekimdzhiev / Bulgaristan*, no 62540/00, § 77, 28 Haziran 2007, *Klass ve Diğerleri / Almanya*, 6 Eylül 1978, § 50, Seri A no. 28 ve yukarıda adı geçen *Uzun*, § 63).

126. Davanın özel muhtevası göz önünde bulundurarak, Mahkeme, Siber Suç Konvansiyonu'nun, gerçek zamanlı trafik verileri toplaması ve çocuk pornografisi ile ilgili suçlalarla mücadelede yetkililere sağlanan üretim talimatlarının düzenlenmesi gibi önlemleri almaları konusunda Devletlere sorumluluk yüklediğini vurgulamaktadır. (bkz. yukarıdaki paragraflar 47 ila 51). Ancak, söz konusu tedbirler, bu Sözleşmenin 15. maddesine göre, "[Taraf Devletlerin] iç hukukunda öngörülen koşullara ve güvencelere tabidir" ve" usulün veya ilgili yetkinin niteliğine uygun olarak, *diğerlerinin yanı sıra*, yargısal veya diğer bağımsız denetimleri, uygulamayı haklı kılan gerekçeleri ve bu yetki ya da usulün kapsamının ve süresinin sınırlarını" içermelidir (bkz. yukarıda paragraf 52).

127. Mevcut davada, Mahkeme, yerel makamlarca dayanılan SCMK'nın 149b (3) maddesinin (bkz. yukarıda paragraf 36), bir elektronik iletişim aracının sahibi veya kullanıcısı hakkında bilgi talebiyle ilgili olduğuna işaret etmektedir. Bu Madde, dinamik IP adresi ile abone bilgisi arasındaki ilişki hakkında kesin kuralları içermemektedir. Mahkeme ayrıca, Anayasanın 37. maddesinin, iletişimin gizliliğine yönelik yapılacak bir müdahalede mahkeme kararı gerektirdiğini not etmektedir (bkz. yukarıda paragraf 35). Ayrıca, elektronik iletişimin gizliliğini özel olarak düzenleyen Elektronik İletişim Yasası (yukarıda paragraf 37), olay zamanında, ceza soruşturması amaçları için abone bilgilerine ve ilgili trafik verilerine erişilip verilmesine imkan tanıyan bir hüküm içermemektedir. Bu yasa, ilgili trafik verileri de dahil olmak üzere elektronik haberleşmelerin gizli olduğunu ve bu itibarla İSS tarafından korunması gerektiğini düzenlemiştir (bkz. yukarıda paragraf 37). Ayrıca, bu yasa İSS'nin, yetkili merciler tarafından iletişimin tespiti ve

dinlenilmesi konusunda bir karar verilmesi hariç olmak üzere ve kendi hizmetlerini yerine getirmesi için gerekli olmadıkça, trafik verilerini başkalarına veremeyeceğini şart koşmuştur (bkz. yukarıda paragraf 37, Elektronik Haberleşme Yasası 103. Maddesi). Dolaysıyla bu mevzuat, en azından, başvurucunun gizlilik menfaatine sağlanan koruma seviyesi açısından tutarlı değildir.

128. Bunların ışığı altında, Mahkeme, bu davada hangi yasanın üstün gelmesi ve uygulanması gerektiğine dair bir karar verebilmek için ulusal mahkemelerin yerine geçecektir. Bunun yerine yerel mahkemelerin gerekçelerine dönmelidir. Mahkeme, bu bağlamda, Anayasa Mahkemesi'nin "iletişim halindeki kişinin kimliğinin, iletişimin gizliliğinin önemli yönlerinden biri olduğu" ve verilmesinin Anayasa'nın 37. maddesinin 2. paragrafı uyarınca bir mahkeme kararı gerektirdiği yönündeki değerlendirmesini kaydetmektedir (bkz. Anayasa Mahkemesi kararının 18. paragraf, yukarıda paragraf 29). Daha spesifik olarak, Anayasa Mahkemesi'nin daha önceki içtihatları ile uyumlu olan yorumuna göre, iç hukukta tanımlanan trafik verileri Anayasa'nın 37. Maddesi kapsamında korunmaktadır (a.g.e), belirli bir dinamik IP adresi ile ilişkili abone bilgilerinin verilmesi, kural olarak mahkeme kararına tabidir ve polisin basit bir yazılı talebi ile elde edilemez.

129. Mahkeme, Anayasa Mahkemesi'nin başvurucunun şikayetini reddetmesinin tek nedeninin, - yani abone bilgilerinin mahkeme kararı olmadan verilmesini onaylamak için – başvurucunun "gizliliğe ilişkin meşru beklentisinden feragat ettiği" varsayımı olduğunu gözlemlemektedir. (Bkz. Anayasa Mahkemesi kararı paragraf 18, paragraf 29). Bununla birlikte, Mahkeme, 8. Maddenin uygulanabilirliği bağlamındaki tespitlerini dikkate alarak, Anayasa Mahkemesinin bu konudaki duruşunun Sözleşme koşulları altında gizlilik hakkının kapsamı ile uyum sağlamadığını tespit etmiştir (bkz. Paragraf 115 ila 118). Anayasa Mahkemesinin "iletişim kuran şahsın kimliği" nin Anayasa'nın 37. Maddesinin (bkz. yukarıda 128. paragrafın) koruması kapsamına girdiği ve Mahkeme'nin başvurucunun çevrimiçi aktivitelerine ilişkin kimliğinin gizli kalmaya devam edeceğine dair meşru beklentisi bulunduğu tespitleri (bkz. paragraf 115 ila 118) göz önüne alındığında somut davada mahkeme kararı gereklidir. Abone bilgisinin alınmasından sonra birkaç aylık zaman zarfında, söz konusu davada zaten ellerinde olan aynı bilgilere göre, herhangi bir soruşturma işleminin yapılmadığını en azından kısmen mahkeme kararının talep edilip alınmadığını düşünürsek iç hukukta polisin mahkeme kararı almasında elini kolunu bağlayan hiçbir şey bulunmamaktadır (bkz. paragraf 8). Yerel

mercilerin SCMK'nın 149b (3) maddesine bağımlı olmaları açıkça yersizdir ve dahası, keyfi müdahaleye karşı neredeyse hiçbir koruma sağlanmamıştır.

130. Bu bağlamda, Mahkeme, olay anında SCMK'nın 149b (3) maddesine göre elde edilen verilerin saklanmasına ilişkin şartları belirten bir düzenleme olmadığı ve verilere erişilmesi ve bunların verilmesi usulünde Devlet görevlilerinin istismarlarına karşı hiçbir güvencenin bulunmadığının anlaşıldığını not etmektedir. İkincisi ile ilgili olarak, polis, elinin altındaki belirli bir çevrimiçi etkinlikle ilgili bilgilerle sadece İSS'den bu bilgiyi aramalarını isteyerek kişiyi tespit edebilirdi. Daha da ötesi bu yetkililer, İSS'yi yerel mahkemeler tarafından yorumlandığı gibi, depolanan çevrimiçi aktiviteleri ile ilgili büyük miktardaki bilgileri incelemesi ve bunu kişilerin rızası olmaksızın polise vermesi hususunda mecbur kılmalarına rağmen, olay anında, polisin bu yetkilerini kullanmasını denetleyecek bağımsız bir denetim mekanizmasının varlığı gösterilmemiştir (Bkz. paragraf 108 ve 109).

131. Mahkeme ayrıca, itiraza konu başvurucuya karşı bu tedbirlerin alınmasından kısa bir süre sonra, Parlamentonun Elektronik Haberleşme Yasasında değişiklik yaptığına işaret etmektedir (bkz. Paragraf 38, paragraf 39'da belirtilen yeni yasadaki ilgili hükümler). Bu değişiklikler, iletişimin kaynağıyla ilgili verilerin saklanması, yani diğerlerinin yanı sıra, belirli bir IP adresi tahsis edilen abonenin adı ve adresi ile verilere erişim ve bunların kurumlara verilmesi usulü ilgili kurallar getirmiştir. Ancak bunun, başvurucunun durumuna bir etkisi olmamıştır.

132. Yukarıda belirtilenler göz önünde bulundurularak, Mahkemeye göre, itiraza konu tedbirin, yani söz konusu dinamik IP adresi ile ilişkili abone bilgilerinin polis tarafından alınması ile ilgili yasanın (yukarıdaki paragraf 7'ye bakınız) dayanağı ve yerel mahkemeler tarafından uygulanma şekli netlikten yoksundur ve 8. madde ile ilgili keyfi müdahalelere karşı yeterli koruma sağlamamaktadır.

133. Bu koşullar altında, Mahkeme, başvurucunun özel hayatına saygı gösterilme hakkına yapılan müdahalenin, Sözleşme'nin 8 § 2 maddesindeki "yasaya uygunluk" koşulunu sağlamadığına karar vermiştir. Bu nedenle, Mahkeme, itiraza konu tedbirin meşru bir amacı olup olmadığını ve orantılı olup olmadığını incelemeye gerek duymamıştır.

134. Yukarıdakilerin tümünü dikkate alarak, Mahkeme, Sözleşme'nin 8. maddesinin ihlal edildiği sonucuna varmıştır.

II. SÖZLEŞME'NİN 41. MADDESİNİN UYGULANMASI

135. Sözleşme'nin 41. maddesi aşağıdaki gibidir:

"Eğer Mahkeme bu Sözleşme ve Protokollerinin ihlal edildiğine karar verirse ve ilgili Yüksek Sözleşmeci Taraf'ın iç hukuku bu ihlalin sonuçlarını ancak kısmen ortadan kaldırabiliyorsa, Mahkeme, gerektiği takdirde, zarar gören taraf lehine adil bir tazmin verilmesine hükmeder."

A. Zarar

136. Başvurucu, kendisine karşı açılan dava nedeniyle yaşadığı sıkıntı için 7,000 Avro, haksız bir şekilde tutuklandığı için 15.000 Avro ve mahkûmiyetinin bir sonucu olarak toplumda yediği suçlu damgası için 10.000 Avro olmak üzere manevi tazminat olarak 32.000 avro talep etmiştir.

137. Hükümet, söz konusu meblağın temelden yoksun ve aşırı olduğunu beyan ederek, başvurucunun talebine itiraz etmiştir. Ayrıca, Hükümet, mevcut davada iddia edilen 8. maddenin ihlali ile mahkûm edilmesi ve hapis cezasına çarptırılmasına ilişkin manevi tazminat iddiaları arasında herhangi bir bağlantı bulunmadığını ileri sürmüştür. Özellikle, söz konusu bilgiler başvurucuyla ilgili yerel mahkemedeki dava dosyasından çıkarılmış olsa bile, kendisine karşı bir ceza soruşturması ve kovuşturmasından kaçınamayacaktı. Ayrıca, Hükümet, başvurucunun, kendisinin de kabul ettiği gibi ihlal tespiti halinde yargılamanın yenilenmesini talep edebileceğinden Mahkemenin tespit hükümleri yeterli olacaktır.

138. Mahkeme, ihlal tespitinin, başvurucunun maruz kaldığı manevi zararlar için yeterli adil tazmin teşkil ettiği kanaatindedir.

B. Masraf ve giderler

139. Başvurucu ayrıca, yerel mahkemelerde gerçekleşen masraf ve giderler için 4,335,50 avro ve Mahkemede yapılan harcamalar için katma değer vergisi (KDV) dahil 2.600 Avro talep etmiştir. Bu miktarların avukatlık ücret tarifesine göre hesaplandığını belirtmiştir.

140. Hükümet, başvurucunun iç hukukta temsiline ilişkin olarak talep ettiği masrafların KDV'yi içerdiğini ileri sürmüştür. Ayrıca, yerel mahkemelerdeki yargılama için gerekli olmayan 2.000 avroluk bir hukuki danışma masraflarını da içermektedir. Mahkeme önündeki yargılama masraflarına ilişkin talep konusunda, Hükümet aşırı olduğunu iddia etmiştir. Ayrıca, yukarıda belirtilen hukuki danışmanın faturası dışında, başvurucu, yasal temsilinden dolayı masrafları olduğuna dair herhangi bir kanıt sunmamıştır.

141.Mahkeme'nin içtihatlarına göre, başvurucunun masraf ve giderlerini geri alabilmesi için, söz konusu masraf ve giderlerin fiilen ve gerekli olduğu için yapılmış olduğunun belgelenmesi ve makul miktarda olması

gerekmektedir. Mevcut davada, sahip olduğu belgeler ve yukarıdaki kriterler dikkate alındığında, Mahkemece, iç hukuktaki yargılama masraf ve giderler için 922 Euro ve Mahkeme önündeki yargılama giderleri için 2,600 avro ödenmesi makul görülmüştür. Toplamda, masraf ve giderler için 3,522 Euro ödenmelidir.

C. Gecikme faizi

142. Mahkeme, gecikme faizi olarak Avrupa Merkez Bankasının kısa vadeli kredilere uyguladığı marjinal faiz oranına üç puan eklemek suretiyle elde edilecek oranın uygun olduğunu değerlendirmektedir.

BU GEREKÇELERLE, MAHKEME

1. Bire karşı altı oyla, abone bilgilerinin verilmesine ilişkin Sözleşme'nin 8. maddesi kapsamında mağdurluk statüsünün bulunmadığı yönündeki Hükümetin itirazının birleştirilmesine ve *reddine*;

2. Çoğunluğun oyuyla, Sözleşme'nin 8. maddesine göre abone bilgilerinin verilmesi ile ilgili şikayetin kabul edilebilir olduğuna ve başvurunun geri kalanının kabuledilemez olduğuna;

3. Bire karşı altı oyla, Sözleşme'nin 8. maddesinin ihlal edildiğine;

4. Oybirliğiyle, ihlal tespitinin, başvurucunun maruz kaldığı manevi zarar için yeterli adil tazmin teşkil ettiğine;

5. Bire karşı altı oyla

   (a) İlgili Devletin, başvurucuya, Sözleşme'nin 44 § 2 maddesi uyarınca, kararın kesinleştiği tarihten itibaren üç ay içinde, 3.522 EUR (üç bin beş yüz yirmi iki avro) ve başvurucuya yüklenebilecek muhtemel vergileri, masraf ve harcamalar karşılığı olarak ödemesine ;

   (b) Yukarıda bahsi geçen üç aylık sürenin bittiği tarihten itibaren, ödeme gününe kadar, Avrupa Merkez Bankasının kısa vadeli kredilere uyguladığı marjinal faiz oranına üç puan eklemek suretiyle elde edilecek oranda, yukarıda bahsedilen meblağlara basit faiz uygulanmasına;

6. Başvurucunun adil tazmine ilişkin diğer taleplerinin reddedilmesine, *karar verilmiştir.*

İşbu karar İngilizce olarak tanzim edilmiş ve Mahkeme İçtüzüğü'nün 77. maddesinin 2 ve 3. fıkraları uyarınca 24 Nisan 2018 tarihinde yazılı olarak tebliğ edilmiştir.

Andrea Tamietti	Ganna Yudkivska
Yazı İşleri Müdür Vekili	Başkan

Sözleşme'nin 45 § 2 ve Mahkeme İçtüzüğünün 74 § 2 maddeleri uyarınca, bu karara aşağıdaki ayrık görüşler eklenmiştir:

(a) Yargıç M. Bošnjak'ın da iştirak ettiği Yargıç G. Yudkivska'nın mutabık görüşü;

(b) Hakim F. Vehabović'in muhalif görüşü;

G.Y.
A.N.T.

YARGIÇ BOŠNJAK'IN DA İŞTİRAK ETTİĞİ YARGIÇ YUDKIVSKA'NIN MUTABIK GÖRÜŞÜ

Çoğunluğun kullandığı metodolojinin yanı sıra kararın sonuçlarına katılıyorum. Bununla birlikte, beni şaşırtan şey, bu davada müdahalenin varlığına ilişkin sonuca ulaşılmasının ve özellikle 115-118. Paragraflardaki gizliliğin makul beklentisine yönelik çok ihtiyatlı bir yaklaşımın ortaya çıkmasındaki zorluktur.

Söz konusu dava, özel hayatımızla ilgili çarpıcı bilgilerin, kontrolümüz dışında kolayca çıktığı dijital çağda gizlilik beklentisinin kapsamını açıklığa kavuşturmak için eşsiz bir fırsat sunmaktadır. Ayn Rand'ın dediği gibi[1] "Uygarlık bir gizlilik toplumuna doğru ilerlemektedir". Bununla birlikte, modern realite, gizliliğin her geçen gün daha fazla korunması icap eden, giderek daha fazla el üstünde tutulması gereken bir değer haline gelmesidir. Sayısız bilim adamı, gizliliğin "ölümünü", "sonunu" veya "yıkımını" çoktan duyurmuştur[2]. Modern çağda gizliliğin korunması için, yalın gizliliğin modası geçmiş anlayışı gözden geçirilmesi gerekliliği, güvenin, gizliliğin ve bilginin nasıl yayıldığına ve kullanıldığına dair denetleme hakkının hukuki korumasına doğru hareket edilmesinin gerekliliği tartışılmaktadır.[3] Bu gibi davalarda gizlilik paradigmasını yeniden düşünme görevi yargıçlar olarak bize tevdi edilmiştir.

Bu davada Mahkeme, - bu koşullar altında gerekli olduğu ölçüde, İnternet Protokolü ve IP adresleme biçimleri, yani statik ve dinamik IP adresleri ile ilgili ilk kez bir araştırmaya girmiştir. *Benedik* davasında biz, bir kullanıcının İnternet'e bağladığı her defasında İnternet servis sağlayıcısına atanmış adres havuzundan rastgele yeni bir IP adreslerinin bu kullanıcıya tahsis edildiği dinamik IP adresleme sistemini tartışmaktayız. Günümüzde dinamik IP adresleme, İnternet kullanıcıları için en yaygın biçimdir ve bu nedenle Mahkemenin mevcut davadaki gizlilik konusunda ulaştığı sonuçlar, Avrupa'da bulunan internet kullanıcılarının büyük çoğunluğunu etkileyecektir.

Samuel D. Warren ve Louis D. Brandeis'in 1890 yılında "Gizlilik Hakkı" başlıklı ünlü makalesini yayınlayana kadar gizliliğin hukuki tanımı ile ilgili tartışmalara değinmek olağan değildi. Bahsedilmesi gereken şey, bu yazarlar, modern teknolojilerin, yani yakın zamanda taşınabilir kameranın keşfi ve basılı medyanın hızla gelişmesi, sıradan insanların yaşamları hakkında istenmeyen detayları ortaya çıkaracağı endişesiyle hareket etmiş olmalarıdır: "Şipşak fotoğraflar ve gazeteler, özel ve ailevi yaşamın kutsal

1. Ayn Rand, The Fountainhead.
2. Bkz. Daniel Solove, "Speech, Privacy and Reputation on the Internet" at: Saul Levmore and Martha Nussbaum, Eds., The Offensive Internet: Speech, Privacy, and Reputation, Cambridge, Mass.: Harvard Üniversitesi Yayınları, 2011, daha fazla referans ile.
3. A.g.e., pp. 20 and 22.

bölgelerini işgal etti; ve çok sayıda mekanik cihaz, klozetin içindeki fısıltının evin çatısından ilan edileceği öngörüsünü yapmayı tehlikeye sokmaktadır."[4]

O zamandan beri, mevcut teknolojilerdeki her gelişme ve yenilerinin ortaya çıkması, gizlilik doktrininin ve makul beklentilerinin yeniden gözden geçirilmesine neden olmuştur: 20. yüzyılın başlarında telefon görüşmelerinin izlenmesi konusundaki endişelerden, 21. yüzyılın başlarında kitlesel gözetim, meta verilerin toplanması ve işlenmesi üzerine geniş tartışmalara gelinmiştir. Ancak 1966 tarihli *Osborn / Birleşik Devletler* davasındaki muhalif görüşünde Yargıç William Douglas şöyle uyarılarda bulunmaktadır: "Herkesin her zaman gözetlemeye açık olacağı, hükümetten gizli hiçbir sırrın kalmayacağı sırların olmadığı bir asra hızla giriyoruz"[5]. Günümüzde var olan teknik imkanlar, Yargıç Douglas'ın elli yıl önce hayal edebileceğinden çok daha müdahalecidir. Ancak internetin geniş kitlelere yayılması eski bir problemle ilgili sadece yeni bir yoğunluk derecesi sunmaktadır.

"Makul gizlilik beklentisi" kavramı, Mahkeme tarafından mevcut dava da dahil olmak üzere birçok davada kullanılmıştır, ancak bu kavram bize *Katz / Amerika Birleşik Devletleri*[6] davasının görüldüğü Amerika Birleşik Devletleri Yüksek Mahkemesinden gelmiştir. Bu dava, şüphelinin yasadışı kumar konusundaki bir telefon kulübesinden yaptığı konuşmalarını dinlemek için gizli dinleme cihazlarının FBI tarafından kullanılması ile ilgilidir. Yüksek Mahkeme'nin gözlemlediği gibi, "işyerinde, bir arkadaşın evinde veya taksideki bir kişiden daha fazla bir telefon kulübesindeki kişi Anayasanın Dördüncü maddesindeki korumaya güvenebilecektir. Telefon kulübesine giren, kapıyı arkasından kapatan ve jetonu atan kişi, ağzından çıkan sözlerin dünyaya yayınlanmayacağı varsayımı ile hareket etmeyi hak etmektedir."

Bunlar söz konusu özel kavramı ortaya atan Yargıç Harlan'ın mutabık görüşünde geçmektedir: "önceki kararlardan ortaya çıkan kuralı anlamanın, iki yönlü bir gereklilik olduğunu" ifade etmiştir: (1) bir kişi "(öznel) kişisel gizlilik beklentisini ortaya koymuştur" ve (2) toplum, bu beklentinin (objektif olarak) makul olduğunu kabul etmeye hazırdır. Bu, Yüksek Mahkemenin Dördüncü maddeye ilişkin içtihadında daha sonra atıf yapılan bir testtir.

"Makul gizlilik beklentisi" kavramı Mahkeme tarafından ilk defa *Halford v. the Birleşik Krallık*[7]davasında kullanılmıştır. Mahkeme, orada telefonunun dinlenebileceğine dair bir uyarı olmaksızın, bir polis

4. Warren & Brandeis, the Right to Privacy, 4 HARV. L. REV. 193 (1890).
5. Osborn v. United States, 385 U.S. 323 (1966).
6. Katz v. United States, 389 U.S. 347 (1967).
7. *Halford v. the United Kingdom*, 25 June 1997, *Reports of Judgments and Decisions* 1997-III.

memurunun işyerlerinde yaptığı telefon görüşmelerinin gizliliği konusunda makul beklentiye sahip olduğu sonucuna varmıştır.

Mahkeme, on yıl sonra *Copland / Birleşik Krallık* davasında[8] aynı kavramdan bahsetmiş ve herhangi bir uyarı olmadan, bir üniversite çalışanının, üniversite posta kutusu hesabından gönderdiği e-postaların gizliliği hakkında makul beklentilere sahip olduğunu tespit etmiştir.

Daha yakın zamanlarda, bu kavramdan *Bărbulescu / Romanya* davasında Büyük Daire tarafından bahsedilmiştir [9]. Dava, başvurucunun müşterilerle iletişim kurması için talimat verildiği Yahoo Messenger hesabı aracılığıyla elektronik iletişiminin izlenmesini takiben başvurucunun işten çıkarılmasıyla ilgilidir. Mahkeme, İnterneti, iç talimatnamelere aykırı olarak, bütün iş günü boyunca kişisel amaçlar için kullandığına karar vermiştir. Mahkeme, işverenin işyerindeki herhangi bir kişisel faaliyetten kaçınmak için açık talimatlarına bakılmaksızın, başvurucunun makul bir gizlilik beklentisi olup olmadığı sorusunu açık bırakmıştır. Çünkü "işveren işyerinde özel sosyal yaşamı sıfıra indiremez".

Mevcut dava, trafik verisi (ölçüm veya meta veriler) söz konusu olduğunda makul bir gizlilik beklentisi konusunu gündeme getirmektedir ve Mahkeme'nin bunun üzerinde net bir duruş sergileme fırsatını kaçırmasından esef duymaktayım. Slovenya Anayasa Mahkemesinin kararındaki ilgi çeken tartışma konularına(bkz. Kararın 28-34. Paragrafları) değinilmemiştir.

Amerikan yargısı arasında da benzer tartışmalar sürmektedir. ABD anayasa hukukunun özgün anlayışı kapsamında, Yüksek Mahkeme, içeriğe ilişkin makul bir gizlilik beklentisi olduğu söylenebilirken, meta veriler (trafik verileri) söz konusu olduğunda böyle bir beklentinin bulunmaması temelinde açıkça hareket etmektedir. Yaklaşık kırk yıl önce, Smith / Maryland davasında[10], Yüksek Mahkeme, telefon numaraları ile aranan numaralar ve konuşmaların süresi hakkında bilgi veren meta verilerinin elde edilmesini değerlendirmiştir. Mahkeme "Bu şartlar altında, telefon abonelerinin, aradıkları numaraların gizli kalacağı yönünde genel bir beklenti barındırdığına inanmak çok zor" olduğunu gözlemlemiştir. Bu nedenle, söz konusu kavram kapsamında bu tür bilgilerle ilgili bireyin kişisel olarak makul bir gizlilik beklentisi bulunmamaktadır.

Amerikan mahkemeleri, IP adreslerine uygulamak için Smith davasında ortaya atılan "üçüncü taraf doktrini" yorumlamışlardır ve internet kullanıcılarının IP adreslerini, üçüncü şahıslara, kullanıcılara, İSS'lere ve web sayfası sunucularına[11] gönüllü olarak ilettikleri için gizlilik

---

[8] Copland v. the United Kingdom, no. 62617/00, ECHR 2007 I.

9. GC, no. 61496/08, ECHR 2017 (extracts).

10. Smith v. Maryland, 442 U.S. 735 (1979).

11. Bkz Alexandra D. Vesalga, Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data, 43 GOLDEN GATE U.L.REV. 459(2013), referring to United States v. Bynum, 604 F.3d 161, 164 & n.2 (4th

beklentilerinin olmadığına, bununla birlikte "sadece bir ağa erişim eyleminin kendi içinde gizlilik beklentilerini ortadan kaldırmadığı[12]" ve "bireylerin bilgisayarlarının içeriğinde gizlilik konusunda objektif olarak makul beklentilere sahip olduklarına" karar vermiştir[13]." Bununla birlikte, 2008 yılında New Jersey Yüksek Mahkemesi, *Devlet v. Reid*[14] davasındaki kararında "bireylerin İnternet'e erişmek için bir İSS adresine ihtiyaç duydukları" tespitini yapmıştır. Ancak, kullanıcılar evlerinin gizliliğinde İnternette sörf yaptıklarında eylemlerinin gizli kalmasını beklemek için sebepleri vardır. Birçoğu, ziyaret ettikleri web siteleri tarafından sayısal bir IP adresinin tutulduğunun farkında değillerdir. Daha sofistike kullanıcılar tek başlarına duran bu rakamlar dizisinin dış dünyaya çok şey açıklayabileceğinin farkındadırlar. Sadece internet servis sağlayıcısı bir IP adresini kullanıcısının adına dönüştürebilir. "

New Jersey Mahkemesi, daha sonra modern internet faaliyetlerinin başlattığı gizlilik modelinin önemli ölçüde yeniden şekillendirilmesi ile devam etmiştir: "...şifrelenmiş IP adresleri İnternet iletişiminin içeriğini ortaya çıkarmazken, abone bilgileri tek başına bir kişi hakkında çok şey söyleyebilir. IP adreslerinin tam listesiyle, bir kişinin İnternet kullanımı izlenilebilir ... Bu tür bilgiler, telefon fatura kayıtlarında olduğu gibi, kişisel ilişkilerle ilgili özel ayrıntıları ortaya çıkarabilir. İnternet iletişiminin içeriği daha da açığa çıksa da, her iki bilgi de gizlilik çıkarlarını etkilemektedir."

Benim görüşüme göre, bu açıkça ifade edilen en önemli zorluktur - trafik verileri veya meta veriler günümüzde içerik verisinden (iletişimin gerçek içeriği) çok daha geniş kapsamlı olarak toplanır ve böyle bir müdahale "hukuk tarafından, "devletin bireylerin iletişimini dinlemesine, iletişim verilerini veya "meta verilerini" toplamasına ya da gizlilikle ilgili makul beklentilerin bulunduğu alanları işgal ederek izlemesi veya gözetlemesine olanak tanıyan nedenleri ve koşulları tanımlayarak önceden öngörülmeli ve açıkça, her yönüyle, kesin ve net bir şekilde düzenlenmelidir"[15]. Avrupa Konseyi Parlamenterler Meclisi, Toplu İzleme Konusundaki Kararı[16], "ulusal yasalarının, yalnızca kişisel verilerin (*meta data dahil olmak üzere*), kişinin rızasıyla veya suç faaliyeti içinde yer alan hedefe dair makul şüpheye dayanarak verilen bir mahkeme kararı ile toplanması ve analiz edilmesine izin vermesinin temin edilmesi için Avrupa Konseyi'ne üye devletleri teşvik etmektedir... ".

Meta verilerinin toplanması, içeriklerin toplanmasından daha az müdahaleci olarak görüldüğü (ve hala görülüyor) kabul edilmektedir.

Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500, 509-10 (9th Cir. 2008), etc.

12. United States v. Heckenkamp, 482 F.3d 1 142, 1 146 (9th Cir. 2007).
13. United States v. Howe, 2011 WL 2160472 at. 7 (W.D.N .Y. May 27, 2011).
14. State v. Reid, 945 A.2d 26, 28 (N.J. 2008).
15. Amerikan İnsan Hakları Komisyonu, İfade Özgürlüğü ve İnternet Özgürlüğü Özel Raportörlüğü (31 Aralık 2013).
16 .PACE Resolution on Mass Surveillance 2045 (21 April 2015).

İnternet öncesi çağda 1984'te Avrupa İnsan Hakları Mahkemesi, içerikleri toplamanın meta verilerini toplamaktan daha büyük bir müdahale olduğunu, meta verilerinin toplanmasının yine de 8. maddeyi ihlal edeceğine karar vermiştir. Bu karar *Malone / Birleşik Krallık davasında*[17] verilmiştir. Bu davada polis, konuşmaların içeriklerini dinlemek ve kaydetmeksizin, belirli bir telefondan aranan numaraları, ayrıca her bir aramanın anını ve süresini, kaydeden cihazları kullanmıştır. Hükümet, bu tür bilgilerin toplanmasının 8. Madde ile garanti edilen haklara müdahale teşkil edilmediğini ileri sürmüştür.

Mahkeme, *Malone* kararında "şartlar ve amaçlar ne olursa olsun metrajlardan alınan verilerin kullanılması 8. madde kapsamında bir soruna yol açmayacağı" nı kabul etmediğini, telefonla aranan numaraların "iletişimin ayrılmaz bir parçası olduğunu" ve abonenin rızası olmaksızın, telefon servis sağlayıcısından bu verilerin alınarak polise verilmesinin 8. Madde ile garanti edilen bir hakka müdahale teşkil ettiğini kaydetmiştir. (*Malone*, § 84).

Bu bakış açısının bugün büyük ölçüde güçlendirilmesi gerekiyor. Meta verilerin, içerik verileriyle aynı koruma seviyesini hak etmediği görüşü, günümüz gerçekleriyle bağdaşmamaktadır: Şu anda meta datanın birçok şekli vardır: telefon görüşmelerinden, e-postalardan, sörf geçmişinizi gösteren arama motorlarından, konumunuzu gösteren Google Haritalar'a v.b. ve eğer bu veriler bir araya getirilirse, kişisel ve mesleki ilişkileri, etnik kökenini, politik eğilimi, dini inançları, farklı gruplara üyeliği, finansal durumu, alışveriş veya hastalık öyküsü gibi ilgili kişiden olağanüstü derecede müdahaleci portre elde edilebilir. Bu bilgileri elde etmek için, eski güzel günlerde olduğu gibi, konuşmaları dinleme veya harfleri okuma zahmetine gitmeye gerek yoktur. Bu noktada, Birleşmiş Milletler İnsan Hakları Konseyi'nin Dijital Çağda Gizlilik Hakkı Konusundaki Kararında belirtildiği gibi, "meta veriler fayda sağlayabilse de, bir araya getirildiklerinde belirli türdeki meta verileri, iletişimin gerçek içeriğinden daha az duyarlı olmayan kişisel bilgilerini veya bir bireyin davranışını, sosyal ilişkilerini, özel tercihlerini ve kimliğini açığa çıkarabileceğinin altı çizilmiştir"[18].

Önde gelen güvenlik uzmanı Bruce Schneier,"İzlemenin altın çağı" na adanan "Data and Goliath[19]" adlı kitabında, Stanford Üniversitesi tarafından yürütülen ve birçok kişinin telefon meta verilerini inceleyen ve - sadece çeşitli telefon görüşmeleri hakkında trafik bilgisi kullanarak - aralarında bir kalp krizi kurbanı, bir ev esrar yetiştiricisi ve kürtaj planlayan hamile bir kadın olan kişileri kolayca tespit eden bir deneyin etkileyici bir örneğini vermektedir.

17. *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82.
18. BM İnsan Hakları Konseyi Dijital Çağda Gizlilik Hakkı Kararı, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017).
19. Bruce Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World", New York, N.Y.: W.W. Norton & Company, 2015.

Çeşitli kaynaklardan korunan birçok bilgi türlerinin toplanması ve birleştirilmesi, yaptığımız hemen hemen her şeyin bir dijital ayak izi bıraktığı göz önüne alındığında, Mahkeme'nin göz ardı edemeyeceği insan hakları için yeni riskler yaratır.

Mevcut davada, mercilerden gelen talep üzerine ilgili servis sağlayıcısı tarafından özel olarak verilmişse, dinamik IP adresler ile bir kişinin kimliği ilişkilendirilebileceğinden dolayı başvurucu, diğer tüm internet kullanıcıları gibi, anonimlikten yararlanmıştır.

Dolayısıyla, 99 nolu paragrafta açıklandığı gibi, faaliyetinin nefret uyandıran yasadışı karakterine rağmen, gizlilik beklentilerinin tamamen meşru olduğu şüphesizdir (müdahale hukuka uygun olarak yapıldığında, Mahkeme suçun niteliğine gereken önemi vermiş olsaydı, müdahalenin orantılılığı hususunda daha ileri bir inceleme yapmış olurdu).

Yukarıda belirtilenler ışığında, Mahkeme IP adreslerinin teknik olarak anonimliğini göz önüne alarak internette gezinirken kullanıcıların gizlilik beklentileri bulunduğunu açıkça belirtmek zorunda olduğuna inanıyorum. Bu meta verilerin daha fazla işleme tabi tutulması, yalnızca yukarıda tartışıldığı gibi kalite şartlarını sağlayan bir yasaya uygun olarak gerçekleştirilebilir.

Gizliliğin korunması, Avrupa politik ve hukuk kültüründe, en azından Nazi ve komünist rejimlerin dehşetlerine zemin oluşturduğu için, hayati bir kazanımdır. Uzun vadede, gizlilik, toplum tarafından savunulduğu sürece temel bir hak olarak duracak ve toplumun bunu temel değer olarak görmeyi bıraktığı zaman ortadan kalkacaktır. Çevrimiçi olduğumuzda bile gizliliğin korunacağına dair makul bir beklentimiz var. Kendimizi dış dünyaya nasıl sunduğumuzu kontrol etmek için temel haklarımız hayatidir ve bu bakış açısı Mahkeme tarafından güçlendirilmelidir.

YARGIÇ VEHABOVIĆ'İN MUHALEFET ŞERHİ

Başvurucunun gizliliğe ilişkin makul beklentisi ile alakalı Sözleşme'nin 8. maddesinin ihlal edildiği ve Sözleşme'nin 8. maddesi kapsamında korunan başvurucunun haklarına müdahale edildiği yönündeki çoğunluğa katılmamaktayım.

7 Ağustos 2006 tarihinde, Internet Servis Sağlayıcının (İSS) yerel yetkililere verdiği bilgiler, başvurucu ile ilgili trafik verileri veya kişisel bilgiler değildir; bunlar internet servisinin abonesi olan başvurucunun babasının adı ve adresidir. Bu başvurucunun mağdur olduğunu iddia edememesi gerçeğinden de anlaşılmaktadır, çünkü Hükumet tarafından işaret edildiği üzere İSS'nin polise verdiği abone bilgileri bu davada başvuru sahibi olmayan babasına aittir.

Bir suç eylemi olan çocuk pornografisi de dahil olmak üzere dosya aktarımının makul bir şüphesi, yerel yetkililerin soruşturmayı genişletmelerini ve başvurucuyla ilgili bilgileri araştırmalarını gerektirir. Yani bu IP adresinden yapılan internet aktivitelerin ilgili trafik verileri, Bölge Mahkemesi, İSS'nin hem abonenin kişisel verilerini hem de söz konusu IP adresine bağlı trafik verilerini teslim etmesi konusunda karar vermesinden sonra, 14 Aralık 2006 tarihinde polise verilmiştir.

Buna ek olarak, Kranj Bölge Mahkemesi sorgu hakimi 12 Ocak 2007 tarihinde evde arama yapılması için arama kararı vermiş ve ancak o zamandan sonra söz konusu trafik bilgileri ile başvurucu ilişkilendirilmiş ve o andan sonra mağdur olduğunu iddia edebilmiştir.

Benim görüşüme göre, başvurucunun babasının adı ve adresinin tespit edilmesine neden olan alınan IP adresi başvurucunun kendisi için kişisel veri olarak değerlendirmek için yeterli yakınlıkta değildir.

Mahkeme, 2. maddedeki kişisel verileri "tanımlanmış veya tanımlanabilir bir bireyle ilgili herhangi bir bilgi" olarak tarif eden Veri Koruma Sözleşmesi'ne birçok olayda atıfta bulunmuştur. (bkz. *Satakunnan Markkinapörssi Oy ve Satamedia Oy / Finlandiya*, 931/13, § 133 ve *Amann / İsviçre,* 27798/95, §65). Yerel makamlar başvurucu hakkında herhangi bir bilgi elde etmemişlerdir; Başvurucu, Mahkeme'nin Sözleşme'nin 8. maddesinin ihlal edildiğine dair tespitinin dayandırıldığı mahkeme kararından önce tanımlanmış veya tanımlanabilir bir kişi değildir. Bu nedenle, başvurucunun Sözleşme'nin 8. maddesi kapsamındaki hakkına aykırı bir müdahalenin bulunduğuna dair çoğunluğun tespitlerine katılmamaktayım.

Makul gizlilik beklentisi ile ilgili olarak, ortada bir suç oluşturan eylemin bulunması halinde başvurucunun gizlilik beklentisi konusundaki sübjektif bakış açısının göz önüne bulundurulması gerekliliğine katılmamaktayım. Neredeyse tüm olaylarda, suçlular faaliyetlerinin başkaları tarafından

bilinmesini istemezler. Bu tür bir gizlilik beklentisi, hukuka aykırı olduğunda veya bu davadaki gibi suçlu veya suça teşvik edici olduğunda makul addedilemeyecektir. Suç aktivitesini gizleme beklentisi makul kabul edilmemelidir. Makul gizlilik beklentisi ile ilgili ikinci bir konuda, başvurucu, başkalarına görülebilen halka açık bir ağ hesabı aracılığıyla çocuk pornografisi (bence, Daire, 115. paragraftan bilerek çıkarmıştır.) de dahil olmak üzere materyaller paylaşmıştır. Başvurucu, bu nedenle, eylemlerinin anonim olmadığını bilmektedir veya bilmesi gerekmektedir. Başvurucu, suçun işlendiği sırada faaliyetini gizlemeye niyetlenmemiştir.

Buna ek olarak, bir müdahalenin tespit edildiği birçok davada, Mahkeme, suçun önlenmesinin meşru bir amaç teşkil ettiğini değerlendirmiştir. Örneğin, *Nada / İsviçre* davasında, Mahkeme, başvurucunun, meşru amaca matuf olarak ihtilaf konusu kısıtlamaların uygulandığını reddetmediğine karar vermiştir. Mahkeme, bu kısıtlamaların, 8 § 2 maddesinde sayılan meşru amaçlardan bir veya birden fazlasını güttüğünü tespit etmiştir: ilk olarak, suçu önlemeyi amaçlamaktadır ”(*Nada v. İsviçre*, 10593/08, § 174). Ayrıca, *S. ve Marper / Birleşik Krallık* davasında “Mahkeme, parmak izi ve DNA bilgilerinin saklanmasının suçun ve suçlunun tespit edilmesi dolayısıyla suçun önlenmesi amacını güttüğü konusunda Hükumet ile hemfikirdir Bu bilginin alınması, bir kimsenin şüphelenildiği bir suçla bağlantısının kurulması amacını güttüğü halde, bu bilgilerin saklanması, gelecekteki suçluların tespit edilmesine yardımcı olma gibi daha geniş bir amaç izlemektedir ”(bkz. S. ve *Marper v. Birleşik Krallık*, 30562/04 30566/04, § 100). Bu nedenlerden dolayı, başvurucunun Sözleşme’nin 8. maddesi kapsamındaki haklarının ihlal edildiğini tespit eden çoğunluğun görüşüne katılmamaktayım.