Avrupa Birliği Adalet Divanı

Kärntner Landesregierung ve diğerleri tarafından sunulan Digital Rights Ireland Ltd ile Haberleşme, Denizcilik ve Doğal Kaynaklar Bakanlığı ve diğerleri (müdahil İrlanda İnsan Hakları Komisyonu) arasındaki davaya ilişkin İşlemler

(C-293/12 ve C-594/12 Birleşik Davası) EU:C:2013:845EU:C:2014:238

9 Temmuz 2013; 12 Aralık; 8 Nisan 2014

Başkan V. Skouris, Başkan Yardımcısı K. Lenaerts, Daire Başkanları A. Tizzano, R. Silva de Lapuerta, T. von Danwitz, E. Juhász, A. Borg Barthet, C.G. Fernlund, J.L. da Cruz Vilaça, Hakimler A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader, C. Vajda ve Başsavcı P. Cruz Villalón

Avrupa Birliği -- Parlamento ve Konsey Direktifi -- Geçerlilik -- Elektronik İletişim -- Kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı hizmet sağlayıcılarının çeşitli kişisel verileri saklamasını zorunlu kılan Direktif --Direktifin Şart'ta yer alan özel hayatın gizliliği ve kişisel verilerin korunması haklarına müdahale edip etmediği -- Müdahalenin orantılı ve gerekçeli olup olmadığı -- Direktifin geçerli olup olmadığı -- 2006/24/EC sayılı Parlamento ve Konsey Direktifi -- Avrupa Birliği Temel Haklar Şartı, Madde 7,8

2006/24/EC[1] sayılı Avrupa Parlamentosu ve Konseyi Direktifinin temel amacı, verilerin ciddi suçlarla mücadele amacıyla kullanılmasını sağlamak için, Üye Devletlerin kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı hizmet sağlayıcıları tarafından üretilen ve işlenen bazı verilerin tutulmasına ilişkin hükümlerini, Avrupa Birliği Temel Haklar Şartının[2] sırasıyla 7. ve 8. maddelerinde belirtilen gizlilik hakkı ve kişisel verilerin korunmasına uygun olarak uyumlaştırmaktır. Direktif; (i) 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi ile sağlanan gizlilik hakkının korunması sistemini ve elektronik iletişim sektöründe kişisel verilerin korunmasına ilişkin 2002/58/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifini ihlal etmiş, (ii) bir abone ya da kayıtlı kullanıcının iletişim kurduğu kişilerin kimliği, hangi araçlarla iletişim kurulduğu, iletişimin yeri ve zamanı gibi hususların bilinmesini mümkün kılan bir şekilde hizmet sağlayıcıların veri saklamasına olanak tanımış, ve (iii) belirli bir sürede abone ya da kayıtlı kullanıcıların bazı kişilerle ne sıklıkta iletişim kurduklarını bilmeyi mümkün hale getirmiştir. 2006/24 sayılı Direktifin gerekliliklerini ulusal yasaya geçiren yıllık önlemlerin gözetildiği, birleştirilen bu iki davada, İrlanda Yüksek Mahkemesi ve Avusturya Anayasa Mahkemesi, sırasıyla, Avrupa Birliği Adalet Divanına, 2006/24 sayılı Direktifin, Şart'ın 7. ve 8. maddesi ile uyumlu olup olmadığı hususunda bir ön karar talebi istemiyle başvurmuştur.

[1] 2006/24/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi:bkz, karar, paragraf 12-16

[2] Avrupa Birliği Temel Haklar Şartı, Madde 7: 'Herkes, özel hayatına, aile hayatına, konutuna ve haberleşme özgürlüğüne saygı gösterilmesini isteme hakkına sahiptir.'
Madde 8: ' 1. Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. 2. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. 3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.

Karar

1 Bu ön karar talebi, kamuya açık elektronik iletişim hizmetlerinin sağlanması veya kamu iletişim ağına ilişkin hükümler uyarınca üretilen veya işlenen verilerin saklanması hakkında ve 2002/58 / EC sayılı Direktifte (OJ 2006 L 105, sayfa 54) değişiklik yapan 15 Mart 2006 tarihli ve 2006/24/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifinin geçerliliğine ilişkindir.

2 Yüksek Mahkeme tarafından sunulan talep (Dava C 293/12), (i) Digital Rights Ireland Ltd. ('Dijital Haklar') ve (ii) İletişim, Deniz ve Tabii Kaynaklar Bakanı, Adalet, Eşitlik ve Hukuk Reformu Bakanı, İrlanda Komiseri Garda Síochána ve Başsavcı arasındaki, elektronik iletişimle ilgili verilerin saklanmasına ilişkin ulusal mevzuat ve idari tedbirlerin yasallığı konusundaki işlemler ile ilgilidir.

3 Verfassungsgerichtshof (Anayasa Mahkemesi) (Dava C 594/12) tarafından sunulan talep, Kärntner Landesregierung (Karintiya Bölgesi Hükümeti) ve Sn. Seitlinger, Sn Tschohl ve 11, 128 diğer başvuran tarafından mahkemeye taşınan anayasal eylemlerle ilgilidir. Dava, 2006/24 sayılı Direktifi Avusturya ulusal yasalarına aktaran yasanın Federal Anayasa Hukuku'na (Bundes-Verfassungsgesetz) uygunluğu ile ilgilidir.

Hukuki bağlam

95/46/EC sayılı Direktif

4 Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına (OJ 1995 L 281, p 31) ilişkin bireylerin korunması hakkında Avrupa Parlamentosu ve Konseyinin 24 Ekim 1995 tarihli ve 95/46/EC sayılı Direktifinin amacı, Madde 1 (1) uyarınca gerçek kişilerin temel hak ve hürriyetlerini ve özellikle kişisel verilerin işlenmesine ilişkin özel hayatın gizliliği haklarını korumaktır.

5 Bu verilerin işlenmesinin güvenliği ile ilgili olarak, bu Direktifin 17(1) Maddesi şunları sağlar:

'Üye Devletler, özellikle de veri işleme süreci verinin bir ağ üzerinden iletilmesini içeriyorsa, denetleyicinin, kişisel verilerin kazayla veya yasalara aykırı bir biçimde tahribi veya kazara kaybetme, değiştirme, yetkisiz olarak ifşa etme veya erişime karşı

korunmasına ilişkin ve diğer tüm yasadışı veri işleme biçimlerine karşı uygun teknik ve organizasyonel önlemleri uygulamasını sağlamalıdır.

Teknolojinin durumu ve uygulanmasının maliyeti göz önüne alındığında, bu gibi önlemler, işlemin maruz kaldığı risklere ve korunacak verilerin niteliğine uygun bir güvenlik düzeyini içerir.'

2002/58/EC sayılı Direktif

6 Avrupa Parlamentosu ve Konseyinin 25 Kasım 2009 tarihli ve 2009/136/EC (OJ 2009 L 337, s. 11,' 2002/58 sayılı Direktif) sayılı Direktifi ile değiştirilen, elektronik iletişim sektöründe kişisel bilgilerin işlenmesi ve özel hayatın gizliliğinin korunması hakkında 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifinin amacı (özel hayatın gizliliği ve elektronik iletişim direktifi), Madde 1 (1)'e göre, elektronik haberleşme sektöründeki kişisel verilerin işlenmesine ilişkin temel haklar ve özgürlüklerin, ve özellikle özel hayatın gizliliği ve gizlilik haklarının eşdeğer düzeyde korunmasını; ve bu tür verilerin serbest dolaşımını sağlamak ve Avrupa Birliği'nde bu veriler ile elektronik haberleşme teçhizatı ve hizmetlerinin serbest dolaşımına ilişkin Üye Devletlerce ihtiyaç duyulan hükümleri uyumlaştırmaktır. Madde 1 (2) 'ye göre, söz konusu direktifin hükümleri, Madde 1 (1)' de belirtilen amaçlar için 95/46 sayılı Direktifi özetler ve tamamlar.

7 Veri işlemenin güvenliği ile ilgili olarak, 2002/58 sayılı Direktifin 4. Maddesi şunları sağlamaktadır:

'1. Kamuya açık bir elektronik iletişim hizmet sağlayıcısı, hizmet güvenliğini sağlamak için gerekli olan teknik ve organizasyonel önlemleri almalı ve gerektiğinde ağ güvenliği konusunda kamu iletişim ağı sağlayıcısı ile bağlantı kurmalıdır. Teknolojinin mevcut durumu ve uygulanmasının maliyeti göz önüne alındığında, bu tedbirler maruz kalınan riske uygun bir güvenlik seviyesinde olmalıdır.

1a. 95/46/EC sayılı Direktife halel getirmeksizin, paragraf 1'de belirtilen önlemler en azından aşağıdaki hususları sağlamalıdır:

– kişisel verilere sadece yetkili personel tarafından yasal amaçlar için erişilebilmesini sağlamak,

– Kişisel verilerin: kazayla ya da kanunsuz olarak yok edilmesi, kazara kaybedilme ya da değiştirilmesi, ve yetkisiz ya da kanunsuz şekilde depolanması, işlenmesi, erişilmesi ya da ifşa edilmesine karşı korunmasını sağlamak, ve,

– kişisel bilgilerin işlenmesine ilişkin bir güvenlik politikasının uygulanmasını sağlamak.

İlgili ulusal otoriteler, kamuya açık elektronik iletişim hizmet sağlayıcıları tarafından alınan tedbirleri denetleyebilir ve bu önlemlerin ulaşması gereken güvenlik düzeyiyle ilgili en iyi uygulamalar hakkında öneriler sunabilir.

2. Ağ güvenliğini ihlal etme hususunda belirli bir risk olması durumunda, kamuya açık bir elektronik iletişim hizmet sağlayıcısı, abonelerine bu risk hakkında bilgi vermelidir; ayrıca eğer bu risk, hizmet sağlayıcı tarafından alınacak tedbirlerin kapsamı dışındaysa, muhtemel masrafları da içerecek şekilde olası tüm telafi yollarını belirtmelidir. ’

8 Söz konusu Direktifin 5 (1) ve (3) numaralı fıkraları, haberleşme ve trafik verilerinin gizliliğine ilişkin olarak aşağıdakileri sağlar:

‘1. Üye Devletler, ulusal mevzuat uyarınca, kamu iletişim ağı ve kamuya açık elektronik iletişim hizmetleri vasıtasıyla, haberleşme ve ilgili trafik verisinin gizliliğini sağlayacaklardır. Özellikle, kullanıcıların rızası olmaksızın, ve Madde 15 (1) uyarınca yasal olarak yetkilendirilmiş olmaları hariç olmak üzere, Üye Devletler dinlemeyi, tapeyi, depolama veya diğer tür iletişim ve trafik verilerinin izlenmesini veya gözlenmesini yasaklar. Bu fıkra, gizlilik ilkesine halel getirmeksizin, bir iletinin iletilmesi için gerekli teknik depolamayı engellemez.

...

3. Üye Devletler, bir abone veya kullanıcının, bir uçbirim ekipmanına bilgi depolanmasına ya da önceden kaydedilmiş bilgilere erişilmesine, veri işleme amaçlarının yanı sıra, 95/46/EC sayılı Direktif uyarınca, ilgili abone veya kullanıcıya açık ve kapsamlı bilgi verilmesi suretiyle rızası alınarak izin verilmesini sağlar. Bu, elektronik iletişim ağı üzerinden yalnızca bir iletişimi iletmek amacıyla teknik depolama veya erişimi engellemez, veya abone veya kullanıcılarca bilgi toplumu hizmet sağlayıcısından açıkça hizmet talep edilmesi durumunda kesinlikle gereklidir.'

9 2002/58 sayılı Direktif Madde 6(1) şunu ifade eder:

'Bir kamu iletişim ağı sağlayıcısı veya kamuya açık elektronik iletişim hizmetleri sağlayıcısı tarafından işlenmiş ve saklanan, abone ve kullanıcılar ile ilgili trafik verileri, bu maddenin 2. 3.ve 5. fıkraları ile Madde 15 (1)'e halel getirmeksizin, bir iletinin iletilmesi amacıyla artık gerek duyulmadığında silinmeli veya anonim(isimsiz) hale getirilmelidir. ’

10 2002/58 sayılı Direktifin 15. maddesinin 1. paragrafı şunu ifade eder:

'Üye Devletler, bu Direktifin 5, 6, 8 (1)(2)(3)(4) ve 9. maddesinde öngörülen hak ve yükümlülüklerin kapsamını sınırlamak için yasal önlemler alabilir. Bu tür bir kısıtlama, 95/46/EC sayılı Direktifin 13 (1) Maddesinde atıfta bulunulan şekilde ulusal güvenliği (yani Devlet güvenliği), savunma, kamu güvenliği ve cezai suçların önlenmesi, araştırılması, tespit edilmesi ve yargılanması veya elektronik iletişim sisteminin yetkisiz kullanımının önlenmesi için demokratik bir toplum içinde gerekli, uygun ve orantılı bir önlem oluşturulması gerektiğinde geçerlidir. Bu amaçla, Üye Devletler, diğerlerinin yanı sıra, bu paragrafta belirtilen gerekçelerle doğrulanmış olan sınırlı bir süre boyunca verilerin saklanmasını teminen yasal önlemleri alabilirler. Bu paragrafta belirtilen tüm tedbirler, Avrupa Birliği Antlaşması'nın 6 (1) ve (2) Maddelerinde belirtilenler de dahil olmak üzere, Topluluk hukukunun genel ilkelerine uygundur. "

2006/24 sayılı Direktif

11 21 Eylül 2005 tarihinde Komisyon, emniyet yetkilileri, elektronik iletişim endüstrisi ve veri koruma uzmanları temsilcileri ile istişare başlattıktan sonra, trafik verilerinin saklanması hakkında kurallarla ilgili politika seçeneklerine ilişkin bir etki değerlendirmesi sundu. Bu değerlendirme, kamuya açık elektronik iletişim hizmetlerinin sağlanmasıyla bağlantılı olarak işlenen verilerin saklanmasına yönelik bir Avrupa Parlamentosu ve Konseyi direktif önerisinin hazırlanmasına, ve EC 95. Madde uyarınca 2006/24 sayılı Direktifin kabulünü sağlayan 21 Eylül 2005 tarihinde sunulan 2002/58 / EC (COM (2005) 438 nihai, 'direktif önerisi') sayılı Direktifin değiştirilmesine zemin hazırlamıştır.

12 2006/24 sayılı Direktifin önsözünde yer alan 4. ifadeye göre:

'2002/58/EC sayılı Direktifin 15 (1) Maddesi, Üye Devletlerin, Direktifin 5, 6, 8 (1)(2)(3)(4) ve 9. Maddesinde öngörülen hak ve yükümlülüklerin kapsamını kısıtlayabileceği koşulları belirlemektedir. Söz konusu kısıtlamaların, demokratik bir toplumda kamu

düzenini sağlamak amacıyla, yani ulusal güvenliği (yani Devlet güvenliği), savunma, kamu güvenliği veya cezai suçların veya yetkisiz kişilerce elektronik haberleşme sistemlerinin kullanımının önlenmesi, soruşturulması, sorgulanması ve yargılanması için, gerekli, uygun ve orantılı olması gerekir.

13 2006/24 sayılı Direktifin önsözünde yer alan 5. ifadenin 5 ilk cümlesine göre, ' bazı Üye Devletler, cezai suçların önlenmesi, soruşturulması, tespit edilmesi ve kovuşturulmasına yönelik olarak hizmet sunucular tarafından verilerin saklanmasını sağlayan mevzuatı kabul etmiştir'

14 2006/24 sayılı Direktifin önsözünde yer alan 7. ifadeye göre:

‘(7) 19 Aralık 2002 tarihli Adalet ve İçişleri Konseyi Kararları, elektronik haberleşmelerin sağladığı olanakların önemli ölçüde büyümesi nedeniyle elektronik haberleşme kullanımına ilişkin verilerin özellikle önemli olduğunu ve bu nedenle özellikle organize suçlar başta olmak üzere, cezai suçların önlenmesi, araştırılması, tespiti ve kovuşturulması konularında değerli bir araç olduğunu vurgulamıştır.

(8) 25 Mart 2004'te Avrupa Konseyi tarafından kabul edilen Terörle Mücadele Bildirgesi, Konseye, servis sağlayıcıları tarafından iletişim trafiği verilerini saklamaya ilişkin kuralların oluşturulmasına yönelik tedbirleri inceleme görevi vermiştir.

(9) 4 Kasım 1950'de Roma'da imzalanan Avrupa İnsan Hakları ve Temel Özgürlükleri Koruma Sözleşmesi'nin (AİHS) 8. maddesine göre, herkes özel hayatına ve yazışmalarına saygı hakkına sahiptir. Demokratik bir toplumda, kamu otoriteleri, bu hakka yalnızca yasa uyarınca ve gerektiğinde, diğerlerinin yanı sıra, ulusal güvenliğin ya da kamu güvenliğinin, suçun önlenmesi ya da başkalarının hak ve özürlüklerinin korunması amacıyla müdahale edebilirler. Verilerin saklanmasının, çeşitli Üye Devletlerde ve özellikle organize suç ve terörizm gibi ciddi konularda kolluk kuvvetince uygulanması gerekli ve etkili bir soruşturma aracı olduğu kanıtlandığından, Bu Direktifte öngörülen şartlara tabi olmak kaydıyla, saklanan bu verilerin belirli bir süre için kolluk kuvvetlerine açık tutulmasını sağlamak gereklidir.

…

(10) Konsey, 13 Temmuz 2005'te Londra'daki terörist saldırılarını kınayan bildirgesinde, telekomünikasyon verilerinin saklanmasına ilişkin olarak mümkün olan en kısa sürede ortak önlemlerin benimsenmesi gerekliliğini yinelemiştir.

(11) Bazı Üye Devletleri araştırmaları ve pratik tecrübesinden de anlaşıldığı üzere, ceza gerektiren suçların soruşturulması, tespit edilmesi ve kovuşturulması için trafik ve konum verilerinin önemi göz önüne alındığında, iletişim hizmetlerinin sağlanması sırasında, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı sağlayıcıları tarafından üretilen veya işlenen verilerin, bu Yönerge'de öngörülen şartlara tabi olmak kaydıyla, belirli bir süre muhafaza edilmesinin Avrupa düzeyinde sağlanmasına ihtiyaç duyulmaktadır. "

15 2006/24 sayılı Direktifin önsözünde yer alan 16., 21. ve 22. ifadeye göre:

‘(16) 95/46/EC sayılı Direktifin 6. Maddesi'nden kaynaklanan veri kalitesinin sağlanması için alınacak önlemlerle ilgili olarak hizmet sağlayıcılar tarafından yerine getirilen yükümlülükler ile aynı Direktifin 16. ve 17. maddelerinden kaynaklanan verilerin işlenmesinin gizliliğini ve güvenliğini sağlamak için alınması gereken tedbirlerle ilgili yükümlülükler, bu Yönerge'nin kapsamı çerçevesinde saklanan verilere tam olarak uygulanır.

(21) Bu Direktifin amaçları, yani belirli verilerin korunması için sağlayıcılar üzerindeki yükümlülükleri uyumlaştırmak ve bu verilerin, ulusal hukukta her Üye Devlet tarafından tanımlanan ciddi suçların sorgulanması ve kovuşturulması amacıyla kullanılabilmesini sağlamak için, Üye Devletler tarafından yeterince sağlanamadığından ve dolayısıyla, bu Direktifin ölçeği ve etkileri nedeniyle Topluluk düzeyinde daha iyi bir şekilde elde edilebilir olduğundan, Topluluk, Antlaşma'nın 5. maddesinde yer alan tamamlama ilkesine uygun olarak önlemler alabilir. Orantılılık ilkesine uygun olarak, bu Maddede belirtildiği gibi, bu Direktif, bu hedefleri gerçekleştirmek için gerekenin ötesine geçmemektedir.

(22) Bu Direktif, temel haklara riayet eder ve özellikle Avrupa Birliği Temel Haklar Şartı ile tanınan ilkeleri gözetir. Özellikle, bu Direktif, 2002/58/EC sayılı Direktif ile birlikte, Şart'ın 7. ve 8. maddelerinde belirtildiği, vatandaşların özel yaşam ve iletişimlerine saygı gösterilmesi ve kişisel verilerin korunması temel haklarına tam olarak uyum sağlamayı amaçlamaktadır.

16 2006/24 sayılı Direktif, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı sağlayıcıları tarafından üretilen veya işlenen bazı verilerin korunması yükümlülüğünü ortaya koymaktadır. Bu bağlamda, Direktifin 1 ila 9, 11 ve 13. maddeleri şu şekildedir:

‘Madde 1

Konu ve kapsam

1. Bu Direktif, bilgilerin kamuya açık elektronik iletişim hizmet sağlayıcıları ve kamu iletişim ağı hizmet sağlayıcılarının yükümlülüklerine ilişkin Üye Devlet hükümlerini, bu sağlayıcılar tarafından üretilen veya işlenen belirli verilerin, her Üye Devletin kendi ulusal hukukunda tanımlanan ciddi suçların soruşturulması, tespit edilmesi ve kovuşturulması amacıyla mevcut tutulması bakımından uyumlaştırmayı amaçlamaktadır.

2. Bu Direktif, hem tüzel kişiler hem de gerçek kişiler hakkındaki trafik ve konum verileri ile abone veya kayıtlı kullanıcıları tanımlamak için gerekli olan ilgili verilere uygulanır. Bir elektronik iletişim ağı kullanılarak istişare edilen bilgiler de dahil olmak üzere, bu durum elektronik iletişimin içeriği için geçerli değildir.

Madde 2

Tanımlar

1. Bu Direktifin amacı için, 95/46/EC sayılı Direktif, elektronik haberleşme ağları ve hizmetleri için ortak bir düzenleyici çerçeve hakkında Avrupa Parlamentosu ve Konseyinin 2002/21/EC sayılı ve 7 Mart 2002 tarihli Direktifi...., ile 2002/58/EC sayılı Direktifte yer alan tanımlar uygulanacaktır.

2. Bu Direktifin uygulanmasında:

(a) "veri"; trafik verisi ve konum verisi ile abone veya kullanıcıyı tanımlamak için gerekli olan ilgili verileri;

(b) "kullanıcı"; söz konusu servise abone olması gerekmeksizin, özel veya ticari amaçlarla kamuya açık bir elektronik iletişim hizmetini kullanan herhangi bir tüzel veya gerçek kişiyi,

(c) "telefon hizmeti"; çağrıları (ses, sesli mesaj ile konferans ve veri aramaları dahil), ek hizmetleri (çağrı yönlendirme ve çağrı transferi dahil) ve mesajlaşma ile çoklu

ortam servislerini (kısa mesaj hizmetleri, gelişmiş medya hizmetleri ve çoklu ortam servisleri dahil olmak üzere);

(d) "kullanıcı kimliği"; bir İnternet erişim hizmetine veya İnternet iletişim hizmetine abone olduklarında kişilere tahsis edilen benzersiz bir tanımlayıcıyı,

(e) "hücre kimliği"; bir mobil telefon aramasının kaynaklandığı veya sonlandırıldığı hücrenin kimliğini;

(f) "başarısız arama girişimi"; bir telefon görüşmesinin başarılı bir şekilde bağlandığını, ancak cevaplanmadığı veya bir ağ yönetim müdahalesinin yapıldığı bir iletişimi

ifade eder.

Madde 3

Verilerin saklanması zorunluluğu

1. Üye Devletler, 2002/58/EC sayılı Direktifin 5, 6 ve 9. Maddelerindeki istisnalarla, bu Direktifin 5. maddesinde belirtilen verilerin, iletişim hizmetlerini tedarik etme sürecinde, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı sağlayıcıları tarafından kendi yetki alanı içinde üretilmesi veya işlenmesi halinde, Direktif hükümleri uyarınca saklanmasını sağlayacak önlemleri alır.

2. Paragraf 1'de belirtilen verilerin saklanması yükümlülüğü, kamuya açık elektronik iletişim hizmet sağlayıcıları veya söz konusu iletişim hizmetlerinin sağlanması sürecinde ilgili Üye Devletin yetkisi dahilinde kamuya açık elektronik iletişim hizmeti veya kamu iletişim ağı sağlayıcıları tarafından bu verilerin üretildiği veya işlendiği veya(telefon verileri bakımından) depolandığı veya (İnternet verileri açısından) kaydedildiği başarısız arama girişimleri ile ilgili olarak 5. Maddede belirtilen verilerin tutulmasını içerir. Bu Direktif, bağlantı sağlanamamış aramalara ilişkin verileri muhafaza etmeyi gerektirmez.

Madde 4

Veriye erişim

Üye Devletler, bu Direktif uyarınca tutulan verilerin sadece belirli durumlarda ve ulusal yasalara uygun olarak yetkili ulusal otoritelere verilmesini sağlamak için önlemler alır. Gerekli ve orantısal gerekliliklere uygun olarak korunan verilere erişmek için izlenecek usuller ve yerine getirilmesi gereken şartlar, her Üye Devlet tarafından, AB yasalarının veya uluslararası kamu hukukunun ve özellikle Avrupa İnsan Hakları Mahkemesi

tarafından yorumlandığı şekliyle AİHS'nin ilgili hükümlerine tabi olarak, kendi ulusal yasalarında tanımlanacaktır .

Madde 5

Saklanacak veri kategorileri

1. Üye Devletler, aşağıdaki veri kategorilerinin bu Direktif'e göre saklanmasını sağlar:

(a) Bir iletişim kaynağını izlemek ve tanımlamak için gerekli veriler:

(1) Sabit telefon şebekesi ve cep telefonu ile ilgili olarak:

(i) arayan telefon numarası;

(ii) abone ya da kayıtlı kullanıcının adı ve adresi;

(2) İnternet erişimi, İnternet e-mail ve İnternet telefonculuğu ile ilgili olarak:

(i) tahsis edilen kullanıcı kimliği(kimlikleri);

(ii) Kamu telefon şebekesine giren herhangi bir iletişime tahsis edilen kullanıcı kimliği ve telefon numarası;

(iii) İletişim anında kendisine bir Internet Protokol (IP) adresi, kullanıcı kimliği veya telefon numarası tahsis edilen abone veya kayıtlı kullanıcının adı ve adresi;

(b) Bir iletişimin varış yerini belirlemek için gerekli veriler:

(1) Sabit telefon şebekesi ve cep telefonu ile ilgili olarak:

(i) Çevrilen numara(lar) (aranan telefon numarası(ları) ,ve, çağrı yönlendirme veya çağrı transferi gibi ek hizmetleri içeren durumlarda, çağrının yönlendirileceği numara veya numaralar;

(ii) abone ya da kayıtlı kullanıcı(lar)nın ad(lar)ı ve adres(ler)i;

(2) İnternet e-mail ve İnternet telefonculuğu ile ilgili olarak:

(i) İnternet telefon görüşmesinin amaçlanan alıcısının kullanıcı kimliği veya telefon numarası;

(ii) Aboneler in veya kayıtlı kullanıcıların isimler ve adresleri ve iletişimin amaçlanan alıcısının kimliği;

(c) Bir iletişim tarihini, zamanını ve süresini belirlemek için gerekli veriler:

(1) Sabit şebeke telefon ve mobil telefonculuğu ile ilgili olarak, iletişimin başlama ve bitiş tarih ve saati;

(2) İnternet erişimi, İnternet e-posta ve İnternet telefonculuğu ile ilgili olarak:

(i) İnternet erişim hizmet sağlayıcısı tarafından bir iletişim için tahsis edilen dinamik veya statik IP adresi ile birlikte, belirli bir zaman dilimine dayalı olarak İnternet erişim hizmetinin oturum açma ve kapatma tarih ve saati ve abonenin veya kayıtlı kullanıcının kullanıcı kimliği;

(ii) Belirli bir zaman dilimine dayalı olarak, İnternet e-posta hizmeti veya İnternet telefon hizmetinin oturum açma ve oturum kapanışının tarih ve saati;

(d) iletişim türünü belirlemek için gerekli olan veriler:

(1) sabit şebeke telefon ve mobil telefonculuk ile ilgili olarak: kullanılan telefon servisi;

(2) İnternet e-postası ve İnternet telefonculuğu ile ilgili olarak: Kullanılan İnternet servisi;

(e) kullanıcıların iletişim ekipmanını tanımlamak için gerekli olan veya ekipmanı olarak neyin kastedildiğini gösteren veriler:

(1) sabit şebeke telefonculuğu, arayan ve aranan telefon numaraları ile ilgili olarak;

(2) cep telefonculuğu ile ilgili olarak :

(i) arayan ve aranan telefon numaraları;

(ii) arayan tarafın Uluslararası Mobil Abone Kimliği'ni (IMSI);

(iii) arayan tarafın Uluslararası Mobil Cihaz Kimliği (IMEI);;

(iv) aranan tarafın IMSI'sı;

(v) aranan tarafın IMEI si;

(vi) ön ödemeli isimsiz hizmetler söz konusu olduğunda, hizmetin ilk kez etkinleştirildiği tarih ve saat ile hizmetin etkinleştirildiği konum etiketi (Hücre Kimliği);

3) Internet erişimi, Internet e-posta ve Internet telefonculuğu ile ilgili olarak:

(i) Çevirmeli erişim için arama yapan telefon numarası;

(ii) Dijital abone hattı (DSL) veya iletişim başlatıcısının diğer uç noktası;

(f) Mobil iletişim ekipmanının yerini belirlemek için gerekli veriler:

(1) İletişim başlangıcındaki konum etiketi (Hücre Kimliği);

(2) İletişim verisinin muhafaza edildiği süre boyunca konum etiketlerine (Hücre Kimliği) referans olarak hücrelerin coğrafi konumunu tanımlayan veriler

2. Bu Direktif uyarınca iletişim içeriğini gösteren hiç bir veri muhafaza edilemez

Madde 6

Saklama süreleri

Üye Devletler, 5. Maddede belirtilen veri kategorilerinin, iletişim tarihinden itibaren altı aydan az olmamak ve iki yıldan fazla olmamak kaydıyla saklanmasını sağlar.

Madde 7

Veri koruma ve veri güvenliği

95/46/EC sayılı Direktif ve 2002/58/EC sayılı Direktif uyarınca kabul edilen hükümlere halel getirmeksizin, her Üye Devlet, kamuya açık elektronik iletişim hizmet sağlayıcılarının veya bir kamu iletişim şebekesinin, asgari olarak, Bu Yönerge uyarınca saklanan verilere ilişkin aşağıda belirtilen güvenlik ilkelerine riayet etmesini sağlar.

(a) Tutulan veriler aynı kalitede olmalı ve ağdaki verilerle aynı güvenlik ve korumaya tabi olmalıdır;

(b) Veriler, kazayla veya yasadışı olarak imha, kazara kaybolma ya da değiştirilme veya yetkisiz veya yasadışı depolama, işleme, erişim veya ifşaya karşı verileri korumak için uygun teknik ve organizasyonel önlemlere tabidir;

(c) Veriler, yalnızca yetkili personel tarafından erişilebilmesini sağlamak için uygun teknik ve organizasyonel önlemlere tabidir;

ve

(d) Erişilen ve korunanlar haricinde, veriler saklama süresinin sonunda imha edilir.

Madde 8

Saklanan veriye ilişkin depolama gereklilikleri

Üye Devletler, bu Direktifin 5. Maddesi uyarınca saklanan verilerin, gerek bu veriler gerekse bu verilerle ilgili gerekli diğer bilgiler ve talep edilen bilgilerin gerekli makamlara gecikmeksizin iletilebileceği şekilde tutulmasını sağlar.

Madde 9

Denetim otoritesi

1. Her Üye Devlet, depolanmış verilerin güvenliği ile ilgili olarak 7. Madde uyarınca Üye Ülkeler tarafından kabul edilen hükümler çerçevesinde kendi topraklarında başvuruyu izlemekle sorumlu bir veya daha fazla kamu yetkilisi tayin eder. Bu yetkili makamlar, 95/46/EC sayılı Direktifin 28 inci maddesinde belirtilen makamlar olabilir

2. Paragraf 1'de belirtilen yetkililer, bu paragrafta atıfta bulunulan izleme işleminin gerçekleştirilmesinde tam bağımsız hareket eder.

…

Madde 11

2002/58/EC sayılı Direktifte Değişiklik

Aşağıdaki paragraf, 2002/58/EC sayılı Direktifin 15. maddesine eklenecektir:

"1 a. Paragraf 1, 2006/24/EC sayılı Direktif tarafından özellikle bu Direktifin Madde 1 (1) 'inde atıfta bulunulan amaçlar için saklanacak veriler için geçerli değildir. "

…

Madde 13

Yargı yolu, yükümlülük ve cezalar

1. Her Üye Devlet, yargı yolu, yükümlülük ve yaptırımlara ilişkin 95/46/EC sayılı Direktifin III. Bölümünü uygulayan ulusal tedbirlerin, bu Direktif kapsamındaki verilerin işlenmesine ilişkin olarak tamamen uygulanmasını sağlamak için gerekli önlemleri alır.

2. Her Üye Devlet, özellikle, bu Direktif uyarınca kabul edilmiş ulusal yasalar uyarınca izin verilmeyen verilere kasıtlı olarak erişilmesinin ya da transfer edilmesinin, etkili,

orantılı ve caydırıcı idari veya cezai yaptırımlar dahil olmak üzere, cezalandırılmasını sağlamak için gerekli önlemleri alır. '

Ana davadaki eylemler ve ön karar için atıf yapılan sorular

Dava C-293/12

17 11 Ağustos 2006'da Dijital Haklar, Yüksek Mahkemeye 3 Haziran 2006'da tescil edilmiş bir cep telefonuna sahip olduğunu ve bu tarihten itibaren o cep telefonunu kullandığını iddia eden bir dava sundu. Elektronik iletişimle ilgili verilerin saklanmasına ilişkin ulusal mevzuat ve idari önlemlerin yasallığına itiraz etti ve ulusal mahkemeden özellikle 2006/24 Sayılı Direktifin ve suçu önlemek, tespit etmek, araştırmak ve kovuşturmak ve Devletin güvenliğini korumak için telefonla iletişim hizmeti sağlayıcılarının, yasa ile belirlenen bir süre boyunca, ilgili trafik ve konum bilgilerini saklamasını gerektiren Ceza Adaleti (Terörle Mücadele) Yasasının 7. Bölümünün geçersizliğini ilan etmesini istedi.

18 Yüksek Mahkeme, 2006/24 sayılı Direktifin geçerliliği incelenmediği sürece ulusal hukuka ilişkin soruları çözemediğinden, davayı askıya alma ve ön karar için Divan'a şu soruları sevk etme kararı aldı :

‘1. Davacının 2006/24/EC sayılı Direktifin 3., 4...ve 6. maddelerinin gerekliliklerinden kaynaklanan mobil telefon kullanımı haklarına ilişkin kısıtlama, aşağıda belirtilen meşru amaçlara ulaşmak için orantısız ve gereksiz ya da uygunsuz olması nedeniyle EU'nun 5 (4). maddesi ile uyumsuz mudur:

(a) belirli bir veri inceleme, tespit ve ciddi suç kovuşturma amaçlarına yönelik olarak kullanılabilir olmasını sağlamak,

ve/veya

(b) Avrupa Birliği iç pazarının düzgün işleyişini sağlamak.

2. Özellikle,

(i) 2006/24 sayılı Direktif, vatandaşların, FEU'nun 21. maddesinde belirtilen Üye Devletlerin topraklarında özgürce hareket etmeleri ve ikamet etme hakkı ile uyumlu mudur?

(ii) 2006/24 sayılı Direktif, [Avrupa Birliği Temel Haklar Şartı ("Şart") Madde 7'de ve AİHS'nin 8. maddesinde belirtilen gizlilik hakkı ile uyumlu mudur?

(iii) 2006/24 sayılı Direktif, Şartın 8. maddesinde belirtilen kişisel verilerin korunması ile uyumlu mudur?

(iv) 2006/24 sayılı Direktif, Şart'ın 11. maddesinde ve AİHS'nin 10. maddesinde yer alan ifade özgürlüğü ile uyumlu mudur?

(v) 2006/24 sayılı Direktif, Şart'ın 41. Maddesi'nde belirtilen iyi yönetim hakkıyla uyumlu mudur?

3. Antlaşmalar - ve özellikle Avrupa Birliği Anlaşması Madde 4 (3) 'de belirtilen sadık işbirliği ilkesi -, 2006/24 sayılı Direktifte yer alan ve (AİHS'nin 8. maddesi uyarınca) madde 7 de dahil olmak üzere Şart tarafından koruma sağlanan ulusal uygulama önlemlerinin uyumluluğunun sorgulanması ve değerlendirilmesi için ne ölçüde ulusal mahkemeye başvurulmasını gerektirir?"

Dava C–594/12

19 C 594/12 davasındaki ön karar talebinin kaynağı, Kärntner Landesregierung ve Sn. Seitlinger, Sn. Tschohl ve diğer 11.128 başvuran tarafından Verfassungsgerichtshof nezdinde, 2006/24 sayılı Direktifi Avusturya ulusal yasalarına aktarmak amacıyla federal kanunla (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) değiştirilen 2003 sayılı Telekomünikasyon Kanunu'nun 102a maddesinin yürürlükten kaldırılmasını isteyen, sırasıyla birkaç davaya dayanmaktadır. Bu kişiler Telekommunikationsgesetz 2003 Kanunun 102a maddesinin, bireylerin verilerini koruma temel hakkını ihlal ettiği görüşünü benimsemektedirler.

20 Verfassungsgerichtshof, özellikle, 2006/24 sayılı Direktifin, sınırsız sayıda kişiye uzun süre boyunca birçok veri çeşidinin depolanmasına izin verdiği gerekçesiyle, Şart ile uyumlu olup olmadığı hususunu öğrenmek istemektedir. Verfassungsgerichtshof, iletişimde bulunmalarının, kendileri ile ilgili verilerin saklanmasını hiçbir şekilde gerekçelendirmeyen bu durumun kişileri etkilediği görüşündedir. Çok sayıda kişinin en az altı ay süreyle erişime sahip olacağı göz önünde bulundurulduğunda, bu kişiler, yetkililerin kendileri ile ilgili verileri araştırıp, bu verilerin içeriği hakkında bilgi sahibi olarak, özel hayatlarını öğreneceği ve bu verileri birden fazla amaç için kullanacakları daha büyük bir riske maruz kalmaktadırlar. Sevk mahkemesine göre, söz konusu Direktifin hedeflediği amaca ulaşıp ulaşamayacağı ve ilgili temel haklara müdahalesinin orantılılığı konusunda şüpheler bulunmaktadır.

21 Bu durumda, Verfassungsgerichtshof, yargılamayı durdurarak, ön karar talebiyle aşağıdaki soruları Avrupa Birliği Adalet Divanı'na sevk etmeye karar vermiştir:

‘1. Avrupa Birliği kurumlarının eylemlerinin geçerliliği ile ilgili olarak:

2006/24 sayılı Direktifin 3 ila 9. maddeleri, Şart'ın 7, 8 ve 11. maddeleri ile uyumlu mudur?

2. Antlaşmaların yorumlanması ile ilgili olarak:

(a) Şart'ın yorumlanmasında rehberlik edebilecek bir yol olarak Şart'ın 52(7) maddesi uyarınca hazırlanan 8. Maddeye ilişkin ve Verfassungsgerichtshof tarafından dikkat gösterilmesi gereken açıklamalar ışığında, kişisel verilerin Topluluk kurumları ve organları tarafından işlenmesi ve bu tür verilerin serbest dolaşımı konusunda bireylerin korunması hakkında 95/46 sayılı Direktif ve Avrupa Parlamentosu ve Konseyinin 18 Aralık 2000 tarihli 45/2001 sayılı Yönetmeliği [OJ 2001 L 8, s. 1,], müdahalenin kabul edilebilirliğinin değerlendirilmesi amacıyla, Şartın 8 (2) Maddesi ve 52 (1) Maddesi koşulları ile eşit ölçüde dikkate alınır mı?

(b) Şart'ın 52 (3) Maddesi'nin son cümlesinde değinilen "Birlik yasası" ile veri koruma yasası alanındaki Direktifler arasındaki ilişki nedir?

(c) 95/26 Sayılı Direktif ve 45/2001 Sayılı Yönetmeliğin, Şart kapsamında verilerin korunmasına ilişkin temel hakların güvence altına alınması için şartlar ve kısıtlamalar içerdiği gerçeğinden hareketle, Şartın 8. Maddesini yorumlamak amacıyla, daha sonraki ikincil kanunlardan kaynaklanan değişiklikler dikkate alınmalıdır mı?

(d) Şart'ın 52 (4) maddesini göz önünde bulundurarak, Şart'ın 53. maddesinde daha yüksek koruma seviyeleri bulundurma ilkesinden hareket edip, izin verilen kısıtlamalara ilişkin olarak Şart'ın uygulanabilir sınırlarının İkincil kanun tarafından daha dar bir şekilde sınırlandırılması gerekir mi?

(e) Şartın 52 (3) maddesini, başlangıcındaki beşinci paragrafı ve bu maddede güvence altına alınan hakların AİHS 8. Maddede güvence altına alınanlarla örtüştüğü Şart'ın 7. maddesiyle ilgili açıklamaları dikkate alarak, bu ikinci maddenin yorumlanmasına katkı için Şart'ın 8. maddesini yorumlamak amacıyla, Avrupa İnsan Hakları Mahkemesinin içtihadından yararlanılabilir mi? '

22 Mahkeme Başkanı'nın 11 Haziran 2013 tarihli kararı ile sözlü prosedür ve karar amaçları doğrultusunda C 293/12 ve C 594/12 davaları birleştirilmiştir.

Atıfta bulunulan soruların değerlendirilmesi

C- 594/12 C 293/12 davasındaki (b) ila (d) bölümlerindeki ikinci soru ile C 594/12 davasındaki ilk soru

23 C 293/12 davasındaki (b) ila (d) bölümlerindeki ikinci soru ve C 594/12 davasındaki ilk sorunun birlikte incelenmesi gerektiği için, sevk mahkemeleri esasen Divan'dan 2006/24 sayılı Direktifin Şartın 7, 8 ve 11. Maddeleri ışığında geçerliliğinin incelemesini talep etmektedir.

Şart'ın 7, 8 ve 11. Maddelerinin 2006/24 sayılı Direktifin Geçerliliği Sorusu ile İlişkisi

24 2006/24 sayılı Direktifin 1 ve 4, 5, 7 ila 11, 21 ve 22 no.lu maddelerinden yola çıkarak, bu direktifin ana amacı, Üye Devletlerin, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağları tarafından, kendileri tarafından üretilen veya işlenen belirli verilerin, Şart'ın 7. ve 8. Maddelerinde belirtilen haklara uygun olarak, organize suç ve terörizm gibi ciddi suçların önlenmesi, araştırılması, tespit edilmesi ve kovuşturulması amacıyla verilerin temin edilebilmesini sağlamak amacıyla tutulması ile ilgili hükümlerini uyumlaştırmaktır.

25 2006/24 sayılı Direktifin 3. maddesi uyarınca, kamuya açık elektronik iletişim hizmetleri veya kamu iletişim hizmet sağlayıcılarının, direktifin 5. maddesinde listelenen verileri gerektiği takdirde yetkili ulusal makamlarca erişim sağlanması amacıyla muhafaza etme yükümlülüğü, Şart'ın 7. Maddesi uyarınca özel hayat ve iletişime saygı, Şart'ın 8. Maddesi kapsamında kişisel verilerin korunması ve Şart'ın 11. Maddesi kapsamında ifade özgürlüğüne saygıya ilişkin soruları gündeme getirir.

26 Bu bağlamda, kamuya açık elektronik iletişim hizmet sağlayıcılarının veya kamu iletişim ağı sağlayıcılarının, 2006/24 sayılı Direktifin 3. ve 5. Maddeleri uyarınca tutmaları gereken veriler, kaynakların izini sürüp tespit etmek, iletişimin tarihini, saatini, süresini ve türünü belirlemek, kullanıcıların iletişim ekipmanını tanımlamak ve mobil iletişim ekipmanının yerini tespit etmek ve diğerlerinin yanı sıra, abone veya kayıtlı kullanıcının adı ve adresi, arayan telefon numarası, aranan numara ve İnternet hizmetleri için bir IP adresini tanımlamak için gerekli verileri içermektedir. Bu veriler, özellikle, bir abone veya kayıtlı kullanıcının iletişim kurduğu kişinin kimliğini ve hangi araçla iletişim

kurduğunu bilmeyi ve bu iletişimin gerçekleştiği yerin yanı sıra iletişim zamanını tanımlamayı mümkün kılar. Ayrıca, belli bir süre zarfında abone veya kayıtlı kullanıcının belirli kişilerle gerçekleştirdiği iletişim sıklığını bilmeyi de mümkün kılar.

27 Bu veriler bir bütün olarak ele alındığında, günlük yaşam alışkanlıkları, daimi veya geçici ikamet yerleri, günlük ya da diğer hareketleri, sosyal ilişkileri ve sosyal çevreleri gibi verileri muhafaza edilen kişilerin özel hayatlarıyla ilgili çok kesin sonuçlar çıkarılmasına yol açabilir.

28 Bu gibi durumlarda, 2006/24 sayılı Direktifin 1 (2) ve 5 (2) Maddelerinden anlaşılacağı üzere, direktif, iletişim içeriğinin veya bir elektronik iletişim ağı kullanılarak istifade edilen bilgilerin muhafaza edilmesine izin vermese bile, söz konusu verilerin tutulmasının, söz konusu direktifin kapsadığı iletişim araçlarının abone ya da kayıtlı kullanıcılar tarafından kullanılması ve dolayısıyla, Şart'ın 11. Maddesi ile güvence altına alınan ifade özgürlüğünün kullanılması üzerinde etkili olabileceği aşikardır.

29 2006/24 sayılı Direktif uyarınca, verilerin, yetkili ulusal otoritelerin muhtemel erişimi amacıyla saklanması, doğrudan ve özel olarak, özel hayatı ve dolayısıyla Şart'ın 7. Maddesinde güvence altına alınan hakları etkiler. Ayrıca, bu tür bir verinin tutulması, Şart'ın 8. Maddesi kapsamındadır, çünkü kişisel verilerin bu maddenin kapsamı dahilinde işlenmesini içerir ve bu nedenle mutlaka bu maddeden kaynaklanan veri koruma şartlarını yerine getirmek zorundadır (C 92 / 09 ve C 93/09 Davaları Volker und Markus Schecke ve Eifert EU: C: 2010: 662, 47. paragraf).

30 Ön karar talebiyle incelenen mevcut davadaki gibi, özellikle Şart'ın 7. Maddesi ışığında abone ve kayıtlı kullanıcıların verilerinin saklanıp saklanamayacağına ilişkin soru gündeme gelirken, 2006/24 sayılı Direktifin Şart'ın 8. Maddesi'nden kaynaklanan kişisel verilerin korunması gerekliliklerini karşılayıp karşılamadığına ilişkin soru da gündeme gelir.

31 Yukarıdaki hususlar ışığında, C 293/12 davasındaki (b) ila (d) bentlerinde yer alan ikinci soru ve C 594/12 davasındaki birinci soruyu cevaplamak amacıyla, Şart'ın 7. ve 8. Maddeleri ışığında Direktifin geçerliliğini incelmek yerinde olur.

Şart'ın 7. ve 8. Maddelerinde belirtilen haklara müdahale

32 2006/24 sayılı Direktifin 5 (1) Maddesinde listelenen verilerin tutulmasına ve yetkili ulusal otoritelerin verilere erişmesine izin vererek, Başsavcı Görüşünün özellikle 39. ve 40. paragraflarında belirttiği gibi, 2006/24 Sayılı Direktif, elektronik haberleşme sektöründeki kişisel verilerin işlenmesi ile ilgili olarak, 95/46 ve 2002/58 sayılı Direktifler tarafından belirlenen mahremiyet hakkının korunması sistemini ihlal eder. Bu Direktifler, haberleşme ve trafik verilerinin gizliliğini, bu verilerin faturalama amacıyla gerekli olmadığı ve yalnızca gerekli olduğu sürece, bir iletinin iletilmesi amacıyla artık gerek duyulmadığı hallerde, silinmesi veya isminin gizlenmesi yükümlülüğünü sağlamaktadır.

33 Temel gizlilik hakkına müdahalenin varlığını ortaya koymak için, özel hayatla ilgili bilgilerin hassas olup olmadığı veya ilgili kişilerin herhangi bir şekilde bundan rahatsız olup olmadığına bakılmaz (bkz., Dava C 465 / 00, C 138/01 ve C 139/01 Österreichischer Rundfunk ve Diğerleri AB: C: 2003: 294, 75. paragraf).

34 Sonuç olarak, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim hizmet sağlayıcılarının, bir kişinin özel hayatı ve iletişimi ile ilgili verileri belirli bir süre muhafaza etmeleri hakkındaki 2006/24 Sayılı Direktifin 3. ve 6. Maddeleri tarafından getirilen yükümlülük, Direktifin 5. maddesinde belirtilenler gibi, Şart'ın 7. Maddesinde güvence altına alınan haklara kendi içinde bir müdahale oluşturmaktadır.

35 Dahası, yetkili ulusal mercilerin verilere erişimi, bu temel hakka daha fazla müdahale oluşturmaktadır (bkz. AİHS'nin 8. Maddesi, AİHMi, Leander / İsveç, 26 Mart 1987, § 48, Seri A No. 116; Rotaru / Romanya [GC], no. 28341/95, § 46, AİHM 2000-V ve Weber ve Saravia / Almanya (karar), 54934/00, § 79, AİHM 2006-XI). Buna göre, yetkili ulusal otoritelerin verilere erişimi ile ilgili kuralları ortaya koyan 2006/24 sayılı Direktifin 4 ve 8. Maddeleri de Şart'ın 7. Maddesinde güvence altına alınan haklara müdahale teşkil etmektedir.

36 Benzer şekilde, 2006/24 sayılı Direktif, kişisel verilerin işlenmesini sağlaması nedeniyle, Şart'ın 8. Maddesiyle güvence altına alınan kişisel verilerin korunmasına ilişkin temel hakka müdahale teşkil eder.

37 Başsavcı Görüşünün 77 ve 80. paragraflarında da belirttiği gibi, 2006/24 sayılı Direktifin Şart'ın 7. ve 8. Maddelerinde belirtilen temel haklara müdahalesinin, geniş kapsamlı olduğu ve de ciddi bir müdahale olduğunun özellikle belirtilmesi gerekir. Dahası, Başsavcının, Görüşünün 52 ve 72. paragraflarında belirttiği gibi, verilerin muhafaza edilmesi ve daha sonra abone veya kayıtlı kullanıcıya bildirilmeden kullanılması, ilgili kişilerin zihninde kendi özel hayatlarının sürekli gözetim altında olduğu hissini vermektedir.

Şart'ın 7. ve 8. Maddelerince güvence altına alınan haklara müdahalenin gerekçelendirilmesi

38 Şart'ın 52 (1) Maddesi, Şart'ın öngördüğü hak ve özgürlüklerin kullanılmasına ilişkin herhangi bir sınırlamanın yasalarca öngörülmesini sağlar, ve orantılılık ilkesine bağlı olarak, hak ve özgürlüklere ilişkin kısıtlamalar yalnızca, Birlik tarafından tanınan genel çıkarların gereklerini veya başkalarının hak ve özgürlüklerini korumak için gerekli olması halinde uygulanır.

39 Şartın 7. maddesinde belirtilen özel hayatın gizliliği ve diğer haklara ilişkin esasları ilgilendiren hususlarla ilgili olarak, 2006/24 Sayılı Direktifin gerektirdiği verilerin saklanması bu haklara ciddi bir müdahale oluşturmasına rağmen, Direktifin 1 (2) maddesinden de anlaşılacağı üzere, direktif, elektronik haberleşmenin içeriği ile ilgili bilgi edinilmesine izin vermediği için, bu hakların özünü olumsuz bir şekilde etkilememektedir.

40 Verinin saklanması, Şart'ın 8. maddesinde belirtilen kişisel verilerin korunması temel hakkının özünü olumsuz yönde etkilememektedir; çünkü 2006/24 Sayılı Direktifin 7. Maddesi veri koruma ve veri güvenliği ile ilgili olarak, 95/46 ve 2002/58 sayılı Direktifler uyarınca kabul edilen hükümlere halel getirmeksizin, veri koruma ve veri güvenliği ile ilgili bazı ilkelere, kamuya açık elektronik iletişim hizmet sağlayıcıları veya kamu iletişim ağı sağlayıcıları tarafından riayet edilir. Bu ilkelere göre Üye Devletler, verilerin, kazara veya yasadışı olarak imha edilmesine, kazara kaybolmasına veya değiştirilmesine karşı uygun teknik ve organizasyon önlemlerinin alınmasını sağlamalıdır.

41 Söz konusu müdahalenin genel menfaat hedefini sağlayıp sağlamadığı sorusu ile ilgili olarak, 2006/24 Sayılı Direktif, Üye Devletlerin bu sağlayıcıların kendilerince üretilen ya da işlenen belirli verilerin saklanmasına ilişkin yükümlülükleri ile ilgili hükümlerini uyumlaştırmayı amaçlarken, bu direktifin ana amacı, Madde 1 (1) 'den anlaşılacağı üzere, her bir Üye Devlet tarafından kendi ulusal yasalarında tanımlandığı üzere, ciddi suçların soruşturulması, tespit edilmesi ve kovuşturulması amacıyla verilerin mevcut olmasını sağlamaktır. Bu nedenle, söz konusu direktifin ana amacı, ciddi suçlarla mücadeleye ve dolayısıyla kamu güvenliğine katkıda bulunmaktır.

42 Uluslararası barış ve güvenliği korumak için uluslararası terörle mücadelenin genel çıkar amacı oluşturduğu, Divanın yerleşik içtihatlarından açıkça anlaşılmaktadır. (bkz, Dava C-402/05 P ve C-415/05 P *Kadi ve Al Barakaat International Foundation* v *Council ve Commission* EU:C:2008:461, paragraf 363, ve Dava C-539/10 P ve C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraf 130) Aynı durum, kamu güvenliğini sağlamak amacıyla ciddi suçla mücadelede de geçerlidir. (bkz,Dava C-145/09 *Tsakouridis* EU:C:2010:708, paragraf 46 ve 47)Ayrıca, bu bakımdan unutulmamalıdır ki, Şart'ın 6. maddesi kişilere yalnızca özgürlük hakkı değil, aynı zamanda güvenlik hakkı da vermektedir.

43 Bu bağlamda, 2006/24 Direktifin önsözünde yer alan 7. ifadeden anlaşıldığı üzere, elektronik iletişimin sağladığı olanaklarla ilgili belirgin büyüme nedeniyle, Adalet ve İçişleri Konseyi 19 Aralık 2002 tarihinde, elektronik haberleşme kullanımına ilişkin verilerin son derece önemli olduğu ve bu nedenle özellikle organize suçlar olmak üzere, suçların önlenmesi ve suçla mücadelede çok değerli bir araç olduğuna karar vermiştir.

44 Dolayısıyla, 2006/24 Sayılı Direktifin gerektirdiği gibi, yetkili ulusal otoritelerce, bu verilere erişebilmesine olanak tanımak amacıyla verilerin tutulmasının, gerçekten de genel çıkar hedefini gerçekleştirdiğini kabul etmeliyiz

45 Bu durumda, yapılan müdahalenin orantılılığını doğrulamak gereklidir.

46 Bu bağlamda, Divanın yerleşik içtihatlarına göre, orantılılık ilkesi AB kurumlarının eylemlerinin, mevzuata göre meşru hedeflere ulaşmak için uygun olmasını ve bu amaçlara ulaşmak için uygun ve gerekli olan sınırları aşmamasını gerektirir (bkz, Dava C 343/09 Afton Chemical AB: C: 2010: 419, paragraf 45; Volker und Markus Schecke ve Eifert AB: C: 2010: 662, paragraf 74; Dava C 581/10 ve 629/10 C Nelson ve Diğerleri

AB: C: 2012: 657, paragraf 71; Dava C 283/11 Sky Österreich AB: C: 2013: 28, paragraf 50; ve Dava C 101/12 Schaible AB: C: 2013: 661, paragraf 29).

47 Temel haklara müdahalenin söz konusu olduğu koşullara uyumun yargısal olarak gözden geçirilmesine ilişkin olarak, AB yasama organının takdir yetkisinin kapsamı, özellikle, ilgili alan, Şart kapsamında güvence altına alınan hakkın doğası, müdahalenin doğası ve ciddiyeti, ve müdahalenin amacı da dahil olmak üzere, çeşitli faktörlere bağlı olarak sınırlı kalabilir. (bkz. AİHS 8. madde, AİHS, S. ve Marper - Birleşik Krallık [GC], no. 30562/04 ve 30566/04, § 102, AİHS, 2008-V).

48 Mevcut davada, kişisel verilerin korunmasına ilişkin özel hayata saygı temel hakkı ve 2006/24 sayılı Direktiften kaynaklanan bu hakka müdahalenin kapsamı ve ciddiyetinin ışığında oynadığı önemli rol nedeniyle, AB Yasama organının takdir yetkisi azalmaktadır ve bu kararın gözden geçirilmesi çok sıkı bir şekilde olmalıdır.

49 Verilerin saklanmasının, 2006/24 sayılı Direktifin hedeflediği amaca ulaşmak için uygun olup olmadığı sorusuna ilişkin olarak, elektronik iletişim araçlarının artan önemi dikkate alınarak, söz konusu direktif uyarınca korunması gereken verilerin, cezai kovuşturma yetkisine sahip ulusal makamların ciddi suçlara ışık tutacak ek fırsatlara sahip olmasına izin verdiği göz önünde bulundurulmalıdır, ve bu bakımdan cezai soruşturmalar için değerli araçlardır. Dolayısıyla, bu tür verilerin saklanması, söz konusu Direktif ile hedeflenen amaca ulaşmak için uygun kabul edilebilir.

50 Bu değerlendirme, özellikle Sn Tschohl ve Seitlinger'in ile Portekiz Hükümetinin Divana gönderdiği yazılı gözlemlerinde, 2006/24 sayılı Direktifin kapsamına girmeyen veya anonim iletişimi sağlayan birkaç elektronik iletişim yönteminin bulunduğu gerçeğine dayanarak, sorgulanamaz. Kuşkusuz, bu gerçek, istenen amaca ulaşmak için veri saklama önleminin kabiliyetini sınırlamakla birlikte, Savcının Görüşünün 137. paragrafında belirttiği üzere, bu önlemi uygunsuz hale getirmez.

51 2006/24 sayılı Direktifin gerektirdiği verilerin saklanması gereği ile ilgili olarak, özellikle organize suç ve terörle mücadele alanları olmak üzere ciddi suçlarla mücadelenin kamu güvenliğini sağlamak için büyük önem taşıdığı kabul edilmeli ve büyük ölçüde modern araştırma tekniklerinin kullanımına bağlı olduğu göz önünde bulundurulmalıdır. Bununla birlikte, ne kadar temel olursa olsun böyle bir amaç, 2006/24 sayılı Direktifle getirilen veri saklama önleminin bu mücadele için gerekli olmasını haklı çıkarmaz.

52 Özel hayata saygı hakkına ilişkin olarak, bu temel hakkın korunması,Divanın yerleşik içtihatlarına göre, her halükarda, kişisel verilerin korunmasıyla ilgili istisna ve sınırlamaların yalnızca gerçekten gerekli olduğunda uygulanır (dava C 473/12 IPI AB IPI: C: 2013: 715, 39. paragraf ve anılan içtihat).

53 Bu bağlamda, Şart'ın 8(1) Maddesi'nde belirtilen açık yükümlülükten kaynaklanan kişisel verilerin korunmasının, Şart'ın 7. Maddesi'nde belirtilmiş olan özel hayata saygı hakkı bağlamında önemli olduğu göz önünde bulundurulmalıdır.

54 Dolayısıyla, verileri muhafaza edilen kişilerin kişisel verilerini, istismar ve bu verilere herhangi bir şekilde hukuka aykırı olarak erişim ve kullanılmaları riskine karşı etkili bir şekilde korumak için yeterli güvence sağlamak amacıyla, söz konusu AB mevzuatı, söz konusu tedbirin kapsamı ve uygulanmasına ve minimum koruma önlemlerinin uygulanmasına ilişkin açık ve kesin kuralları belirlemelidir. (bkz., AİHM 8. madde, AİHS, Özgürlük ve Diğerleri - İngiltere, 1 Temmuz 2008, No. 58243/00, 62 ve 63, Rotaru / Romanya, § 57 ila 59 ve S. ve Marper / Birleşik Krallık, § 99).

55 Bu tür güvencelere duyulan ihtiyaç, 2006/24 sayılı Direktifte belirtildiği üzere, kişisel verilerin otomatik olarak işleme tabi tutulduğu ve bu verilere yasadışı olarak erişim riski bulunduğu durumlarda daha büyüktür (bkz. AİHS Madde 8, S. ve Marper - Birleşik Krallık, § 103, ve M. K. - Fransa, 18 Nisan 2013, No. 19522/09, § 35).

56 2006/24 sayılı Direktiften kaynaklı müdahalenin kesinlikle gerekli hallerle sınırlı olup olmadığı sorusuna ilişkin olarak, bu direktifin 5 (1) Maddesiyle bağlantılı olarak okunan 3. maddeye uygun olarak, Direktif, sabit telefon, mobil telefon, internet erişimi, internet e-postası ve İnternet telefonu ile ilgili tüm trafik verilerinin tutulmasını gerektirir. Bu nedenle, kullanımı yaygın olan ve insanların gündelik hayatlarında önemi artan her türlü elektronik iletişim aracı için geçerlidir. Ayrıca, 2006/24 sayılı Direktifin 3. Maddesi uyarınca, Direktif tüm aboneleri ve kayıtlı kullanıcıları kapsamaktadır. Dolayısıyla, bu, pratik olarak tüm Avrupa nüfusunun temel haklarına müdahaleyi kapsamaktadır.

57 Bu bağlamda, öncelikle, 2006/24 sayılı Direktifin, genel olarak, tüm kişileri ve tüm elektronik iletişim araçlarını ve ayrıca ciddi suçlarla mücadele ışığında, herhangi bir ayrım, sınırlama veya istisna olmaksızın tüm trafik verilerini kapsadığını belirtmek gerekir.

58 2006/24 sayılı Direktif, cezai kovuşturmaya neden olabilecek bir durumda, dolaylı olarak bile olsa, verileri saklanan kişiler hariç, elektronik iletişim servislerini kullanan tüm kişileri kapsamlı bir şekilde etkiler. Bu nedenle, davranışlarının ciddi bir suçla dolaylı veya uzak bir bağlantıya bile sahip olabileceğini düşündürecek kanıt bulunmayan kişilere bile uygulanır. Dahası, sonuç olarak, ulusal hukuk kurallarına göre mesleki gizlilik yükümlülüğüne tabi olan kişilerin iletişimi için bile geçerli olması nedeniyle herhangi bir istisna da sağlamaz.

59 Ayrıca, ciddi suçlarla mücadeleye katkıda bulunmaya çalışırken, 2006/24 sayılı Direktif, saklanması sağlanan veriler ile kamu güvenliğini tehdit eden veriler arasında herhangi bir ilişki gerektirmemektedir ve özellikle, (i) belirli bir zaman aralığına ve/veya belirli bir coğrafi bölgeye ve/veya ciddi bir suçta bir şekilde yer alması muhtemel kişilere ait bir çevreye ilişkin verilere ya da (ii) başka sebeplerden ötürü, verilerini saklı tutarak, ciddi suçların önlenmesi, tespit edilmesi veya yargılanmasına katkıda bulunabilecek kişilerle ilgili olarak bir veri saklama ile sınırlandırılmamaktadır.

60 İkincisi, 2006/24 sayılı Direktif, yalnızca genel sınırlamalar konusunda eksiklik içermemekte, aynı zamanda verilere yetkili ulusal makamların erişim sınırlarını ve suçun önlenmesi, tespiti veya cezai kovuşturma amaçlı olarak sonraki kullanımını belirlemek için objektif kriterler belirlemekte de başarısız olmaktadır, ki bu kriterlerin eksikliği durumunda, bu müdahalenin kapsam ve ciddiyeti Şart'ın 7. ve 8. maddelerinde belirlenen temel hakların ihlalini gerekçelendirmekte yeterli olarak kabul edilebilir. Diğer taraftan, 2006/24 sayılı Direktif Madde (1) 1'de, her Üye devlet ve bunların ulusal yasalarında tanımlanan ciddi suçlara atıfta bulunulduğu açıkça belirtilmektedir.

61 Ayrıca, 2006/24 sayılı Direktif, verilere ve verilerin sonraki kullanımına yetkili ulusal makamlarca erişimle ilgili esas ve usule ilişkin şartları içermez. söz konusu yetkililerin saklanan verilere erişimini düzenleyen Direktifin 4. maddesi, bu erişim ve veri kullanımının, kesin olarak tanımlanmış ciddi suçların önlenmesi ve tespiti veya bunlara ilişkin cezai kovuşturma amaçlarıyla sınırlı olması gerektiğini belirtir; gereklilik ve orantılılık gereksinimlerine uygun olarak tutulan verilere erişim kazanmak için her Üye Devletin takip edeceği prosedürleri ve yerine getireceği şartları tanımlamasını sağlar.

62 Özellikle, 2006/24 sayılı Direktif, tutulan verilere erişmek ve daha sonra kullanmak üzere yetkilendirilen kişi sayısının, izlenen hedef ışığında kesinlikle gerekli olanlarla sınırlı olduğuna dair herhangi bir objektif kriter ortaya koymamaktadır. Her şeyden önce,

yetkili ulusal otoritelerin elinde tuttuğu verilere erişimi, kararları veri erişimine ya da yalnızca gerekli olduğunda kullanılmasına yönelik olarak çeşitli kısıtlamalar getirebilecek bir mahkeme tarafından ya da verilere erişimi kısıtlamaya yetkili bağımsız bir idari organ tarafından yapılan ön incelemeye tabi değildir. Ayrıca, bu limitleri belirlemek üzere Üye Devletlere belirli bir yükümlülük de getirmemektedir.

63 Üçüncü olarak, veri saklama süresiyle ilgili olarak, 2006/24 sayılı Direktifin 6. Maddesi, bu verilerin, en az altı aylık bir süre boyunca muhafaza edilmesini ve bu verilerin, hedeflenen amaç temelinde veya ilgili kişilere ilişkin olarak, Madde 5'de belirtilen veri kategorileri arasında herhangi bir ayrım yapılmaksızın tutulmasını gerektirir.

64 Ayrıca, bu süre minimum 6 ay ile maksimum 24 ay arasında belirlenmiş, ancak kesin surette gerekli olduğu kadar süreyle sınırlanmasını sağlamak üzere, saklama döneminin belirlenmesinin objektif kriterlere dayanması gerektiği belirtilmemiştir.

65 Yukarıda belirtildiği üzere, 2006/24 sayılı Direktif Şartın 7. ve 8. maddelerinde belirlenen temel haklara müdahale kapsamını düzenleyen net ve kesin kurallar koymamaktadır. Bu nedenle 2006/24 sayılı Direktif aslında, böyle bir müdahalenin yalnızca gerekli olanla sınırlı olmasını sağlayacak hükümler açıkça belirlenmeden, AB'nin hukuk düzenindeki bu temel haklara geniş çaplı ve ciddi müdahale içermektedir.

66 Ayrıca, kamuya açık elektronik haberleşme hizmeti sağlayıcıları ya da kamu iletişim ağı hizmet sağlayıcıları tarafından tutulan verilerin güvenlik ve korunmasına ilişkin kuralları ile ilgili olarak, 2006/24 sayılı Direktif, Şartın 8. maddesinde belirtilen, istismar riski ve bu verilerin herhangi bir yasadışı erişim ve kullanıma karşı etkin bir şekilde korunmasını sağlamak için gerekli olan güvenceleri yeterli ölçüde sağlamamaktadır. Öncelikle, 2006/24 sayılı Direktifin 7. maddesi; (i) saklanması bu direktif uyarınca gerekli olan büyük miktardaki veriye (ii) bu verinin hassas doğasına (iii) bu verilere yasadışı erişim riskine ilişkin, bu verilerin tam bütünlüğünü ve gizliliğini sağlamak için açık ve kesin bir şekilde söz konusu verilerin korunması ve güvenliğini sağlamaya yönelik özel ve uyumlu kurallar koymamaktadır. Ayrıca, Üye Devletlerin bu tür kuralları oluşturulmasına ilişkin belirli bir yükümlülük de konmamıştır.

67 2002/58 sayılı Direktifin 4 (1) Maddesi ve 95/46 Sayılı Direktifin 17 (1) Maddesinin ikinci bendi ile bağlantılı olarak, 2006/24 sayılı Direktifin 7. Maddesi, bu hizmet sağlayıcılar tarafından teknik ve organizasyonel önlemler alınarak yüksek düzeyde bir

koruma ve güvenlik uygulanmasını sağlamaz, ancak hizmet sağlayıcıların uygulayacakları güvenlik düzeylerini belirlerken, özellikle uygulama masrafları ile ilgili olarak, ekonomik hususları dikkate almalarına olanak tanır. 2006/24 sayılı Direktif , özellikle, veri saklama döneminin sonunda verinin geri döndürülemez biçimde imha edilmesini sağlamamaktadır.

68 İkinci olarak, iki önceki paragrafta belirtildiği üzere, Şart'ın 8 (3) Maddesinin gerektirdiği koruma ve güvenlik şartlarına uyum, bağımsız bir makam tarafından tamamen kontrol altına alınmadığından, bu direktif söz konusu verilerin Avrupa Birliğinde tutulmasını gerektirmemektedir. AB yasalarına dayanılarak yapılan böyle bir kontrol, kişisel verilerin işlenmesinde bireylerin korunmasının vazgeçilmez bir unsurudur (bkz. C 614/10 Komisyon/ Avusturya EU: C: 2012 : 631, paragraf 37).

69 Yukarıdaki tüm hususları dikkate alarak, 2006/24 sayılı Direktifi kabul ederek, AB yasama organı, Şart'ın 7., 8. ve 52 (1). Maddesi ışığında orantılılık ilkesine uyulması ile ilgili öngörülen sınırları aşmıştır.

70 Bu şartlar altında, 2006/24 Sayılı Direktifin geçerliliğini, Şart'ın 11. Maddesi ışığında incelemeye hiç gerek yoktur.

71 Sonuç olarak, C 293/12 davasının (b) ila (d) bölümlerindeki ikinci soruya ve C 594/12 davasındaki ilk soruya verilen cevap, 2006/24 sayılı Direktifin geçersiz olduğudur.

C 293/12 davasında (a) ve (e) bölümlerindeki İlk ve ikinci soru ile üçüncü soru, ve C 594/12 davasında ikinci soru

72 Bir önceki paragraftan anlaşılacağı üzere, C 293/12 davasında (a) ve (e) bölümlerindeki İlk ve ikinci soru ile üçüncü soru, ve C 594/12 davasında ikinci sorusunun cevaplanmasına gerek yoktur.

Masraflar

73 Ana dava tarafları bakımından bu takibat ulusal mahkeme nezdinde devam eden ana davanın bir aşamasını teşkil ettiğinden, masraflarla ilgili karar verme yetkisi ulusal yargınındır. İlgili tarafların harcamaları hariç, Divan'a gözlem sunulmasına ilişkin masraflar geri ödemeye konu olamaz.

Bu gerekçelerle, Divan (Büyük Daire) aşağıdakilere hükmetmiştir:

Kamuya açık elektronik iletişim hizmetleri veya kamu iletişim ağı hizmetlerine ilişkin hükümlerle bağlantılı olarak üretilen ve işlenen verilerin saklanması hakkında 15 Mart 2006 tarihli ve 2006/24 / EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi ile 2002/58 / EC sayılı değişiklik yapılmasına dair Direktif geçersizdir.