MAHKEME KARARI (Büyük Daire)

21 ARALIK 2016 (*)

(Ön karar başvurusu — Elektronik iletişim — Kişisel verilerin işlenmesi — Elektronik iletişimin gizliliği — Koruma — 2002/58/EC — 5,6 ve 9'uncu maddeler ve 15'inci maddenin birinci fıkrası— Avrupa Birliği Temel Haklar Şartı — 7,8 ve 11'inci maddeler ve 52'nci maddenin birinci fıkrası— Ulusal mevzuat— Elektronik iletişim hizmetleri sağlayıcıları — Trafik ve konum bilgilerinin genel ve ayrımcılık yapılmadan saklanmasına ilişkin yükümlülük— Ulusal makamlar — Verilere erişim — Bir mahkeme veya bağımsız bir idari merci tarafından ön inceleme yapılmaması — AB hukuku ile uyumluluk)

C-203/15 ve C-698/15 sayılı Ortak Kararlar için,

Kammarrätten i Stockholm (İdari Temyiz Mahkemesi, Stockholm, İsveç) ve (İngiltere & Galler) (Hukuk Birimi) (Birleşik Krallık) Temyiz Mahkemesi'nin sırasıyla 29 Nisan 2015 ve 9 Aralık 2015 kararlarıyla, Avrupa Birliği'nin İşleyişi Hakkında Anlaşma'nın (ABİHA) 267'nci maddesi kapsamında yapılan ön karar başvurusu 4 Mayıs 2015 ve 28 Aralık 2015 tarihlerinde mahkemeye ulaşmıştır.

(C-203/15) sayılı dava **Tele2 Sverige AB** ve **Post-och telestyrelsen** arasında, (C-698/15) sayılı dava ise **İçişleri Bakanı** ve **Tom Watson, Peter Brice, Geoffrey Lewis** ile aşağıda belirtilen müdahiller arasındadır**: Open Rights Group, Privacy International (Uluslararası Mahremiyet), The Law Society of England and Wales (İngiltere ve Galler Hukuk Topluluğu).**

MAHKEME (Büyük Daire);

Başkan K. Lenaerts, Başkan Yardımcısı A. Tizzano, R. Silva de Lapuerta, Rapportör T. von Danwitz, Daire Başkanları J.L. da Cruz Vilaça, E. Juhász ve M. Vilaras, Hakimler A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen ve C. Lycourgos,

Baş avukat: H. Saugmandsgaard Øe,

Kalem amiri: Yönetici C. Strömholm'den oluşmaktadır.

Mahkeme, Mahkeme Başkanı'nın 1 Şubat 2016 tarihinde C-698/15 sayılı davanın Mahkeme İçtüzüğü'nün 105'inci maddesinin birinci fıkrasında öngörülen hızlandırılmış usul uyarınca düzenlenmesi gerektiğini belirten kararını göz önünde tutarak,

Yazılı usulü ve 12 Nisan 2016'daki duruşmayı göz önünde tutarak,

- Tele2 Sverige AB adına, M. Johansson ve avukat N. Torgerzon ve E. Lagerlöf ile S. Backman tarafından,
- Sayın Watson adına, Dava vekilleri J. Welch ve E. Norton, Avukat I. Steele, Savunma avukatı B. Jaffey ve D. Rose QC tarafından,
- Sayın Brice ve Lewis adına, Savunma avukatları A. Suterwalla ve R. de Mello, R. Drabble QC ve dava vekili S. Luke tarafından,
- Open Rights Group ve Privacy International adına, Dava vekili D. Carret ve Savunma Avukatları R.Mehta ve J. Simor tarafından,

- İngiltere ve Galler Barosu adına, Savunma avukatı T. Hickman ve N. Turner tarafından,
- İsveç hükümeti adına, Temsilciler A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren ve L. Swedenborg tarafından,
- Birleşik Krallık Hükümeti adına, Temsilciler S. Brandon, L. Christie, V. Kaye ile Beard QC, G. Facenna QC, J. Eadie QC ve Savunma avukatı S. Ford tarafından,
- Belçika Hükümeti adına, Temsilciler J.-C. Halleux, S. Vanrie ve C. Pochet tarafından,
- Çek Hükümeti adına, Temsilciler M. Smolek ve J. Vláčil tarafından,
- Danimarka Hükümeti adına, Temsilciler C. Thorning ve M. Wolff tarafından,
- Alman Hükümeti adına, Temsilciler T. Henze, M. Hellmann ve J. Kemper ile M. Kottmann ve U. Karpenstein, Rechtsanwalte tarafından,
- Estonya Hükümeti adına, Temsilci K. Kraavi-Käerdi tarafından,
- İrlanda adına, Temsilciler E. Creedon, L. Williams ve A. Joyce ile D. Fennelly BL tarafından,
- İspanya Hükümeti adına, Temsilci A. Rubio González tarafından,
- Fransız Hükümeti adına, Temsilciler G. de Bergues, D. Colas, F.-X. Bréchot ve C. David tarafından,
- Kıbrıs Hükümeti adına, Temsilci K. Kleanthous tarafından,
- Macaristan Hükümeti adına, Temsilciler M. Fehér ve G. Koós tarafından,
- Hollanda Hükümeti adına, Temsilciler M. Bulterman, M. Gijzen ve. J. Langer tarafından,
- Polonya Hükümeti adına, Temsilci B. Majczyna tarafından,
- Finlandiya Hükümeti adına Temsilci J. Heliskoski tarafından,
- Avrupa Komisyonu adına Temsilciler H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira ve J. Vondung tarafından ibraz edilen belgeleri dikkate alarak,

19 Temmuz 2016 oturumunda Baş Avukatın Görüşünü aldıktan sonra aşağıdaki kararı vermiştir.

Karar

1. Ön karar başvuruları elektronik iletişim sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunmasını ilgilendiren 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'nin (mahremiyet ve elektronik iletişimle ilgili Direktif) (RG 2002 L201, s. 37) 15'inci maddesinin birinci fıkrasının yorumlanmasıyla ilgilidir. Bu Direktif, Avrupa Birliği Temel Haklar Şartı'nın 7'nci ve 8'inci maddesi ve 52'nci maddesinin birinci fıkrası dikkate alınarak okunan, 25 Kasım 2009 tarihli ve 2009/136/EC sayılı Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi (RG 2009 L 337, s. 11) ile değiştirilmiştir ('2002/58 sayılı Direktif').
2. (i) Post- och telestyrelsen'in (İsveç Posta ve Telekom Makamı; 'PTS') Tele2 Sverige AB'ye katılımcıların ve kayıtlı kullanıcıların trafik ve konum verilerini saklamasını emrettiği dava (Dava C-203/15) ve (ii) Tom Watson, Peter Brice, Geoffrey Lewis ve İç İşleri Bakanı (Büyük Britanya Birleşik Krallığı ve Kuzey İrlanda) arasında 2014 Veri Saklama ve Soruşturma Yetkileri Kanunu'nun Birinci Kısmı ile AB Hukukunun uyumluluğunu ilgilendiren iki dava için başvuru yapılmıştır ('DRIPA') (Dava C-698/15).

Hukuki bağlam

AB Hukuku

2002/58 sayılı Direktif

3. 2002/58 sayılı Direktif'in 2, 6, 7, 11, 21, 22, 26 ve 30'uncu gerekçeleri aşağıdadır:

'(2) İşbu Direktif temel haklara saygı duymayı ve özellikle [Şart]ın tanıdığı ilkeleri göz önünde bulundurmayı amaçlar. Özellikle, bu Direktif Şart'ın 7'nci ve 8'inci maddelerinde açıklanan haklara tamamen saygı duymayı amaçlar.

...

(6) İnternet geniş bir yelpazede elektronik iletişim hizmetlerini sağlarken ortak ve küresel bir altyapı oluşturarak geleneksel piyasa yapılarını tersine çevirmektedir. İnternette bulunan ve kamuya açık olan elektronik iletişim hizmetleri kullanıcılara yeni fırsatlar sunarken kişisel veri ve mahremiyetlerini de yeni riskler altına sokmaktadır.

(7) Kamu iletişim ağları söz konusu olduğunda, gerçek kişilerin temel hak ve özgürlüklerini ve tüzel kişilerin meşru menfaatlerini korumak için özellikle otomatik depolamanın kapasitesini arttırmayla ve katılımcılara ve kullanıcılara ait bilginin işlenmesiyle ilgili özel, düzenleyici ve teknik hükümler oluşturulmalıdır.

...

(11) 95/46/EC sayılı Direktif gibi [kişisel verilerin işlenmesiyle ilgili olarak kişilerin korunması ve verilerin özgürce iletilmesi hakkındaki 24 Ekim 1995 sayılı (RG 1995 L281, s. 31) Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi], bu Direktif Topluluk Hukuku'nun yönetmediği faaliyetlerle ilgili temel hakların ve özgürlüklerin korunmasıyla ilgili alanları düzenlemez. Bu nedenle, bireylerin mahremiyet hakkını ve bu Direktifin 15'inci maddesinin birinci fıkrasında geçen; kamu güvenliğinin korunması, savunma, Devlet güvenliği (Devlet Güvenliğini ilgilendiren konularda ekonomik refahın sağlanması dahil olmak üzere) ve ceza hukukunun infazı için gerekli olan tedbirlerin Üye Devletlerce alınma olasılığını değiştirmez. Sonuç olarak, bu Direktif, Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi uyarınca, Avrupa İnsan Hakları Mahkemesi'nin hükümlerinde yorumlandığı üzere, bahsedilen amaçlardan herhangi biri gerektirdiğinde, Üye Devletlerin elektronik iletişimi hukuki bir şekilde denetleme veya tedbir alma gücünü etkilemez. Bu tedbirler uygun olmalı, buna ilaveten niyetlenen amaçla tamamen orantılı ve demokratik toplumlarda gereken tedbirler olmalıdır. Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi uyarınca yeterli sayıda teminat bulunmalıdır.

...

(21) İletişimin içeriği ve bununla ilgili her veri dahil iletişimin gizliliğini korumak için kamu iletişim ağları ve kamuya açık elektronik iletişim hizmetleri yoluyla haberleşmeye izinsiz erişimi önleyecek tedbirler konmalıdır. Bazı Üye Devletlerdeki ulusal mevzuatlar haberleşmeye yalnızca kasıtlı izinsiz erişimi yasaklamıştır.

(22) Verilerin otomatik ve geçici olarak depolanmasını engellemek nedeniyle, iletişim ve ilgili trafik verilerinin kullanıcılar tarafından değil şahıslar tarafından yasaklanması veya

kullanıcıların rızaları alınmadan yasaklanması hedeflenmemektedir. Veri depolama yalnızca veri iletiminin elektronik iletişim ağında yapılması amacını taşıdığı sürece gerçekleşir. Ayrıca bilginin iletilmesi için gerekli süreyi aşmama, trafik yönetimi amaçları dışında veri saklamama ve veri saklanması sırasında gizliliğin garanti edilmesi şartı bulunmaktadır.

...

(26) Bağlantılar oluşturmak ve bilgi iletmek amacıyla elektronik iletişim ağlarında işleme konulan katılımcı verileri, gerçek kişilerin özel hayatına dair bilgiler içerir ve haberleşmeye saygı hakkını ya da tüzel kişilerin meşru menfaatlerini ilgilendirir. Bu veriler, ancak hizmetin sağlanması için gerekli olduğu sürece, faturalama ve ara bağlantı ödemelerini yapmak için kısa süreliğine depolanabilir. Kamuya açık elektronik iletişim hizmetleri sağlayıcısının uygulamak istediği ileri işleme yöntemleri, katılımcının rıza göstermeme veya rızasını geri çekme haklarıyla ilgili doğru ve tam bilgi vermesi sonucunda, yalnızca katılımcı olan kişi onay verirse ileri işleme ... yapılabilir.

...

(30) Elektronik iletişim ağı ve hizmetlerinin sistemleri ihtiyaç olan kişisel veri miktarını en aza indirmek için tasarlanmalıdır. ...'

4. 2002/58 sayılı Direktif'in 'Kapsam ve hedef' başlıklı birinci maddesi:

'

1. İşbu Direktif temel hak ve özgürlüklerin eşit düzeyde korunması ve elektronik iletişim sektöründe kişisel verilerin işlenmesi sırasında özellikle mahremiyet ve gizlilik haklarının korunması için gerekli olan ulusal hükümlerin uyumlu olmasını öngörür ve bu verilerle elektronik iletişim araç ve hizmetlerinin Topluluk içinde özgürce dolaşmasını sağlar.
2. Bu Direktifin hükümleri birinci fıkrada belirtilen amaçlar sebebiyle [95/46] sayılı Direktif'i detaylı olarak açıklar ve tamamlar. Ayrıca, tüzel kişiliği olan katılımcıların meşru menfaatlerini korumayı öngörür.
3. Bu Direktif, Avrupa Birliği Anlaşması'nın 5'inci ve 6'ncı Başlıklı bölümlerinde olduğu gibi Avrupa Topluluğu'nu kuran Anlaşma'nın kapsamı dışına çıkan faaliyetlere ve her durumda, kamu güvenliği, savunma, Devlet güvenliğini ilgilendiren faaliyetlerde (devletin ekonomik refahını ilgilendirenler dahil) ve ceza hukukuyla ilgili Devlet faaliyetlerinde uygulanmaz.'

5. 2002/58 sayılı Direktif'in 'Tanımlar' başlıklı 2'nci maddesi:

'Aksi belirtilmedikçe, [95/46] sayılı Direktif ve 2002/21/EC sayılı 7 Mart 2002 tarihli elektronik iletişim ağı ve hizmetleri için düzenleyici ortak bir çerçeveye ilişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'ndeki (Çerçeve Direktif) tanımlar uygulanır [(RG 2002 L 108 s. 33)].

Aşağıdaki tanımlar da uygulanır:

...

(b) "Trafik verileri" elektronik iletişim ağında bir yazışmanın iletilmesi veya bu işlemin faturalandırılması amacıyla işlenen her tür veri anlamına gelir,

(c) "Konum verileri" kamuya açık bir elektronik iletişim hizmeti kullanıcısının bağlantı aracının coğrafi konumunu gösteren ve bir elektronik iletişim ağı içinde veya elektronik iletişim hizmeti tarafından işlenen her tür veri anlamına gelir,

(d) "İletişim" kamuya açık bir elektronik iletişim hizmeti vasıtasıyla sınırlı sayıda taraflar arasında alışverişi yapılan veya iletilen her türlü bilgi anlamına gelir. Bu bilgi, bir yayın hizmeti yoluyla herhangi bir elektronik iletişim ağı üzerinden halka verilen her bilgiyi içine almaz. Ancak kimliği tespit edilebilen bir katılımcı veya kullanıcıyı ilgilendiren bir bilgi söz konusu ise bu bilgi yazışma tanımı içindedir.

...'

6. 2002/58 sayılı Direktif'in 'İlgili hizmetler' başlıklı üçüncü maddesi:

'Bu Direktif, veri toplama ve tespit cihazlarını destekleyen kamu iletişim ağları dahil olmak üzere Topluluk içindeki kamu iletişim ağlarında bulunan kamuya açık elektronik iletişim hizmetlerinin verilmesi ile bağlantılı kişisel verilerin işlenmesinde uygulanır.'

7. Bu Direktifin, 'İşlem güvenliği' başlıklı dördüncü maddesi aşağıdadır:

'1. Kamuya açık bir elektronik iletişim hizmeti sağlayıcısı, hizmetlerinin güvenliği için uygun teknik ve kurumsal tedbirler almalıdır. Bu tedbirleri gerektiğinde ağ güvenliğine ilişkin kamu iletişim ağının sağlayıcısıyla ortak çalışarak almalıdır. Tedbirlerin çağdaş oluşu ve maliyetleri göz önünde tutulduğunda, bu tedbirler mevcut riske uygun bir güvenlik düzeyi oluşturur.

1a. [95/46] sayılı Direktif'e halel getirmeksizin, birinci fıkrada yazılan tedbirler asgari olarak:

- Kişisel verilere yalnızca yetkilendirilen personelin kanunlarla izin verilmiş amaçlar için erişmesini sağlar,
- Depolanan ve iletilen kişisel verileri kazara veya hukuksuz şekilde yok etme, kazara kaybolma ya da değiştirilme ve yetkisiz veya hukuksuz depolama, işlemden geçme, erişilme veya açıklanmaya karşı korur ve
- Kişisel verilerin işlenmesine ilişkin güvenlik politikasının yürütülmesini sağlar.

...'

8. 2002/58 sayılı Direktif'in 'İletişimin gizliliği' başlıklı beşinci maddesi:

'1. Üye Devletler, kamu iletişim ağı ve kamuya açık elektronik iletişim hizmetleri vasıtasıyla ve ulusal mevzuat yoluyla, iletişimin ve ilgili trafik verilerinin gizliliğini sağlar. Özellikle, 15'inci maddenin birinci fıkrası uyarınca hukuken yetki verilmesi dışında, iletişimin ve ilgili trafik verilerinin kullanıcılar dışındaki şahıslar tarafından ilgili kullanıcıların rızası dışında dinlenmesi, saklanması veya diğer yollarla tespit edilmesini ve denetimini engellerler. Bu paragraf, gizlilik ilkesine halel getirmeksizin, haberleşmenin iletilmesi için gerekli olan teknik depolamanın yapılmasını engellemez.

...

3. Üye Devletler, bilgi depolama işlemi veya halihazırda katılımcının veya kullanıcının bağlantı aracında depolanmış bilgiye erişim sağlama işleminin, ancak işlemin amaçları hakkında açık ve anlaşılır bilgi sunulan katılımcı veya kullanıcının, diğer hususlarla birlikte [95/46] sayılı Direktif uyarınca, rıza göstermesi şartıyla gerçekleşmesini sağlar. Bu durum, yalnızca bir haberleşmenin elektronik iletişim ağı üzerinden iletimini sağlamak veya bilgi toplumu hizmet sağlayıcısının katılımcı ya da kullanıcının açık talebi üzerine bu hizmeti yerine getirmesinin kesinlikle gerekmesi gibi amaçlar için teknik depolama veya erişim işlemlerini önlemez.'

9. 2002/58 sayılı Direktif'in 'Trafik verileri' başlıklı altıncı maddesi:

'1. Bu maddenin 2'nci, 3'üncü ve 5'inci paragrafları ve 15'inci maddenin birinci paragrafına halel getirmeksizin bir haberleşmenin iletilmesi için trafik verilerine gerek olmadığı hallerde, katılımcılar ve kullanıcılarla ilgili ve kamu iletişim ağı veya kamuya açık elektronik iletişim hizmeti sağlayıcısının işlediği ve depoladığı trafik verileri silinmeli veya anonim olmalıdır.

2. Katılımcı faturalandırması ve ara bağlantı ödemeleri için gerekli olan trafik verileri işlenebilir. Bu işleme, yalnızca faturaya kanunen itiraz edilebileceği ya da ödemenin talep edilebileceği sürenin sonuna kadar izin verilir.

3. Elektronik iletişim hizmetlerini pazarlama veya katma değer hizmetlerini temin etme amaçlarını gerçekleştirmek adına, kamuya açık bir elektronik iletişim hizmeti sağlayıcısı, birinci paragrafta belirtilen verileri; hizmetler ve pazarlama için gereken kapsam ve süre içerisinde olması ve bilginin ait olduğu katılımcı veya kullanıcının öncesinde rıza vermiş olması kaydıyla, işleme alabilir. Kullanıcı veya katılımcılar trafik verilerinin işlenmesi konusunda istedikleri zaman rızalarını geri çekme imkanına sahip olur.

...

5. 1'inci, 2'nci, 3'üncü ve 4'üncü paragraflar uyarınca, trafik verilerinin işlenmesi, kamu iletişim ağları ve kamuya açık elektronik iletişim hizmetleri sağlayıcılarının yetkileri altında bulunan ve faturalama ya da trafik yönetimi, müşteri incelemesi, dolandırıcılık tespiti, elektronik iletişim hizmetlerinin pazarlaması veya katma değer hizmetlerinin temini üzerinde çalışan kişilerle sınırlandırılmalı ve verilerin işlenmesi bu faaliyetlerin amaçları çerçevesinde kalmalıdır.'

10. Direktif'in 'Trafik verilerinin dışında konum verileri' başlıklı dokuzuncu maddesinin birinci paragrafı:

'Kamu iletişim ağları veya kamuya açık elektronik iletişim hizmetleri kullanıcıları ya da katılımcıları hakkındaki trafik verileri dışında konum verileri, yalnızca anonim hale gelirse ya da kullanıcı veya katılımcıların rızası alınırsa, katma değer hizmetinin verilmesi için gereken kapsam ve süre içerisinde işleme alınabilir. Hizmet sağlayıcısı, kullanıcı veya katılımcıların rızalarını almadan önce, onlara trafik verileri dışında işlenecek olan konum verilerinin türü, bu işlemin amaçları, süresi ve katma değer hizmeti sağlamak için verilerin üçüncü bir tarafa iletilip iletilmeyeceği hakkında bilgi vermelidir. ...'

11. Direktif'in '[95/46] sayılı Direktif'in bazı hükümlerinin uygulanması' başlıklı 15'inci maddesi:

'1. Üye Devletler, demokratik bir toplumda milli güvenliği (Devlet güvenliğini), milli savunmayı, kamu güvenliğini garanti altına almak ve ceza eylemlerini ya da elektronik iletişim sisteminin izinsiz kullanımını önlemek, soruşturmak, tespit etmek ve kovuşturmasını yapmak için gerekli, uygun ve orantılı bir adım teşkil etmesi halinde, bu Direktif'in 5'inci, 6'ncı maddelerinde, 8'inci maddenin birinci, ikinci, üçüncü ve dördüncü paragrafında ve 9'uncu maddesinde öngörülen hak ve yükümlülüklerin kapsamını sınırlayacak mevzuat tedbirleri alabilir. Bu maksatla, Üye Devletler, diğer hususlarla birlikte, bu paragrafta belirtilen gerekçelerin bulunması halinde sınırlı süre için verilerin saklanmasını öngören yasama tedbirlerini benimseyebilir. Bu paragrafta bahsedilen tüm tedbirler, Avrupa Birliği Anlaşması'nın 6'ncı maddesinin birinci ve ikinci paragraflarında bahsedilen tedbirlerle birlikte Topluluk Hukuku'nun genel ilkeleri uyarınca alınır.

...

1b. Sağlayıcılar, kullanıcıların kişisel verilerine erişim isteklerine cevap vermek için birinci paragraf uyarınca kabul edilen ulusal hükümlere dayanan iç usuller oluşturur. Sağlayıcılar, talep üzerine yetkili ulusal makamı usuller, alınan talep sayısı, yasal gerekçe ve cevabına ilişkin bilgilendirir.

2. [95/46] sayılı Direktif'in Üçüncü Bölümünde yer alan yargı yolları, yükümlülük ve yaptırımlara ilişkin hükümler bu Direktif gereğince alınan ulusal hükümler ve bu Direktif'ten doğan bireysel haklar açısından uygulanır.

…'

95/46 sayılı Direktif

12. 95/46 sayılı Direktif'in Üçüncü Bölümündeki 22'nci madde:

'28'inci maddede bahsedilen denetleyici makam huzurunda, diğer hususlarla birlikte, hakkında hüküm verilebilecek olan idari kanun yollarına halel getirmeksizin, yargı makamına sevk edilmeden önce, Üye Devletler, söz konusu işlemi düzenleyen ulusal hukukun garanti altına aldığı hakların bir şekilde ihlal edilmesi halinde herkesin yargı yolu hakkına sahip olmasını öngörür.'

2006/24/EC sayılı Direktif

13. 2002/58/EC sayılı Direktif'i değiştiren (RG 2006 L 105, s. 54) 2006/24/EC sayılı 15 Mart 2006 tarihli kamuya açık elektronik iletişim hizmetlerinin ve kamu iletişim ağlarının temin edilmesiyle ilgili oluşturulan ve işleme alınan verilerin saklanması hakkındaki Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'nin 'Konu ve kapsam' başlıklı birinci maddesinin ikinci paragrafı:

> 'Bu Direktif hem tüzel hem de gerçek kişilerle ilgili trafik ve konum verileri hakkında ve katılımcı ya da kayıtlı kullanıcıyı tespit etmek için gereken verilere uygulanır. Elektronik iletişimin içeriği ve elektronik iletişim ağı kullanılarak başvurulan bilgi söz konusu olduğunda bu Direktif uygulanmaz.'

14. Direktif'in 'Veri saklama yükümlülüğü' başlıklı 3'üncü maddesi:

'1. [2002/58 sayılı Direktif]in 5'inci, 6'ncı ve 9'uncu maddelerine istisna teşkil ederek, Üye Devletler, haberleşme hizmetleri sunulurken ve yetkileri dahilinde, bu Direktif'in 5'inci

maddesindeki verilerin Direktif hükümleri uyarınca saklanmasını sağlamak amacıyla, bu verilerin kamuya açık elektronik iletişim hizmetleri veya kamu iletişim ağının sağlayıcıları tarafından üretilmesi ve işlenmesini sağlayacak tedbirler alır.

2. Birinci paragrafta öngörülen veri saklama yükümlülüğü 5'inci maddedeki başarısız çağrı denemeleriyle ilgili verilerin saklanmasını içerir. Bu veriler, ilgili Üye Devletlerin yetki alanları içerisinde, iletişim hizmetlerinin sunulma aşamasında, kamuya açık elektronik iletişim hizmetleri veya kamu iletişim ağlarının sağlayıcıları tarafından üretilen, işlenen, saklanan (telefon verileri) ya da kaydedilen (internet verileri) verilerdir. Bu Direktif, bağlantısız çağrılara ait verilerin saklanmasını gerektirmez.

İsveç Hukuku

15. C-203/15 sayılı Dava'nın referans listesine bakıldığında, İsveç meclisinin 2006/24 sayılı Direktif'i iç hukuka aktarabilmek için the lagen (2003:389) om elektronisk kommunikation [Elektronik iletişim kanunu (2003:389); 'LEK'] ve förordningen (2003:396) om elektronik kommunikation [Elektronik iletişim tüzüğünü (2003:396)] değiştirdiği görülmektedir. Her iki metin de ana yargılamadaki uyuşmazlığa uygulanabilen versiyonlarında, elektronik iletişim verilerinin saklanması ve ulusal makamların bu verilere erişmesiyle ilgili kurallar içermektedir.
16. Bu verilere erişim, yukarıdakine ek olarak, the lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (kolluk makamlarının topladığı istihbaratın parçası olan elektronik iletişim verilerinin toplanmasına ilişkin (2012:278) sayılı Kanun: '2012:278 sayılı Kanun') tarafından ve rättegångsbalken (Yargı Usulü Kanunu: 'RB') tarafından düzenlenmiştir.

Elektronik iletişim verilerini saklama yükümlülüğü

17. C-203/15 sayılı Dava'da sevk eden mahkemenin verdiği bilgiye göre, LEK'in Altıncı Bölümünün 16a paragrafındaki hükümler, bu kanunun İkinci Bölümünün birinci paragrafıyla birlikte okunduğunda, 2006/24 sayılı Direktif'in de gerekli gördüğü üzere, elektronik iletişim hizmetleri sağlayıcılarına veriyi saklama yükümlülüğü getirmektedir. Abonelik ve tüm elektronik iletişimle ilgili olan veriler; bir haberleşmenin kaynağını ve son varış yerini izlemek ve tespit etmek, tarih, zaman ve türünü belirlemek, kullanılan haberleşme aracını tanımlamak ve haberleşmenin başı ve sonunda kullanılan mobil iletişim aracının konumunu belirlemek için gereklidir. Saklı tutulması için yükümlülük getirilen veriler telefon hizmetleri, mobil bağlantı kullanan telefon hizmetleri, elektronik mesajlaşma sistemleri, internet erişim hizmetleri ve internet erişim kapasitesi (bağlantı modu) sağlama hizmetleri bağlamında üretilen ve işleme alınan verilerdir. Bu yükümlülük başarısız iletişimle ilgili verileri de kapsar, ancak iletişimin içeriğini kapsamaz.
18. Elektronik iletişimle ilgili Tüzüğün (2003:396) 38-43'üncü maddeleri, saklı tutulması gereken verilerin kategorilerine yer vermiştir. Telefon hizmetleri için çağrılar, aranan numaralar ve iletişimin başı ve sonunu belirten tanımlanabilir tarih ve zamanlarla ilgili verilerin saklanması zorunludur. Mobil bağlantı kullanan telefon hizmetleri için iletişimin başı ve sonundaki konum verilerinin saklanması gibi bazı ek zorunluluklar getirilmiştir. IP paketi kullanan telefon hizmetleri, yukarıda belirtilen verilere ek olarak arayan ve aranan kişinin IP adreslerine ilişkin verileri de saklamak zorundadır. Elektronik mesajlaşma sistemleri, gönderici ve alıcının numaralarıyla ve IP adresleri ve diğer mesajlaşma adresleriyle ilgili verileri saklamak zorundadır. İnternet erişim hizmetleri söz konusu olduğunda ise, kullanıcıların IP adresleri, internet erişim hizmetine giriş ve çıkışın yapıldığı izlenebilen tarih ve zamanlar gibi veriler saklanmalıdır.

Verilerin saklanma süresi

19. LEK Altıncı Bölümün 16d paragrafı uyarınca, bu Bölümün 16a paragrafının kapsadığı verilerin elektronik iletişim hizmetleri sağlayıcıları tarafından iletişimin bitmesinden itibaren altı ay süreliğine saklanması gerekmektedir. Veriler, 16d paragrafının ikinci bendinde aksi belirtilmedikçe bu süre sonunda derhal silinmelidir.

Saklı verilere erişim

20. Ulusal makamlarca saklı verilere erişim 2012:278 sayılı Kanun hükümleri, LEK ve RB tarafından belirlenir.

– 2012:278 sayılı Kanun

21. İstihbarat toplama bağlamında, ulusal polis, Säkerhetspolisen (İsveç Güvenlik Servisi) ve Tullverket (İsveç Gümrük Kurumu), 2012:278 sayılı Kanun'un birinci paragrafına dayanarak, bu Kanun'daki şartlara uymak suretiyle, LEK tarafından yetkilendirilen bir elektronik iletişim ağının veya elektronik iletişim hizmeti sağlayıcısını bilgilendirmeden, bir elektronik iletişim ağından, belli bir coğrafi bölgede bulunan bir elektronik iletişim aracından ve elektronik iletişim aracının bulunduğu veya önceden bulunduğu coğrafi alan(lar)dan iletilen mesajlarla ilgili verileri toplayabilir.

22. 2012:278 sayılı Kanun'un ikinci ve üçüncü paragrafları uyarınca, şartlara bağlı olarak, eğer tedbir en az iki yıllık hapis cezası gerektiren suçlardan biri veya birden fazlasını içeren ya da Kanun'un üçüncü paragrafında geçen iki yıldan az hapis cezası gerektiren suçları içeren cezai eylemi engellemek, önlemek veya tespit etmek için gerekliyse, veriler genel bir kural olarak toplanabilir. Bu tedbiri destekleyen gerekçeler, tedbirin etkileyeceği kişiye ya da tedbire karşı çıkan bir menfaate herhangi bir zarar veya halel gelme ihtimalini ortadan kaldıracak nitelikte olmalıdır. Bu Kanun'un beşinci paragrafı uyarınca, tedbirin süresi bir ayı geçmemelidir.
23. Bu tedbiri uygulama kararını ilgili makamın müdürü veya sorumluluğun devredildiği kişi almalıdır. Karar bir yargı makamı veya bağımsız idari bir makamın ön denetimine tabi değildir.
24. 2012:278 sayılı Kanun'un altıncı paragrafı uyarınca, the Säkerhets och integritetsskyddsnämnden (İsveç Güvenlik ve Bütünlük Koruma Komisyonu), veri toplama yetkisi veren her karar hakkında bilgilendirilmelidir. Lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (bazı kolluk faaliyetlerinin denetimine ilişkin (2007:980) sayılı Kanun'un) birinci paragrafı uyarınca, bu makam kolluk makamlarının mevzuat uygulamalarını denetlemekle yükümlüdür.

– LEK

25. LEK Altıncı Bölüm 22'nci paragrafının, birinci bendindeki ikinci madde uyarınca, savcılık makamı, ulusal polis, Güvenlik Servisi ya da diğer kolluk makamlarının talebi üzerine, elektronik iletişim hizmeti sağlayıcılarının tümü, bir aboneliğe ait verilerin varsayılan cezai bir eylemle bağlantısı olması halinde bu verileri açıklamalıdır. C-203/15 sayılı Dava'da sevk eden mahkemenin sağladığı bilgilere göre, eylemin ağır bir suç olması gerekmez.

– RB

26. RB, ön soruşturmalar çerçevesinde tutulan bilginin ulusal makamlara açıklanması sürecini yönetir. RB'nin 27'nci Bölümünün 19'uncu paragrafı uyarınca, üçüncü tarafların bilgisi dışında 'elektronik iletişimin incelemeye alınması', genel bir kural gereği, diğer hususlarla birlikte en az altı ay hapis cezası gerektiren eylemlerle ilgili ön soruşturmalar çerçevesinde izin verilen bir durumdur. 'Elektronik iletişimin incelemeye alınması' ifadesi, RB'nin 27'nci Bölümünün 19'uncu paragrafı uyarınca, bir elektronik iletişim ağı, belli bir coğrafi bölgede bulunan veya o güne kadar bulunmuş olan elektronik iletişim aracı ve özel elektronik iletişim araçlarının bulunduğu veya o güne kadar bulunmuş olduğu coğrafi bölge(ler) tarafından iletilen mesajla ilgili verilerin üçüncü kişilerin bilgisi dışında elde edilmesi anlamına gelir.

27. C-203/15 Dava'sında sevk eden mahkemenin belirttiğine göre, RB'nin 27'nci Bölümünün 19'uncu paragrafı uyarınca bir mesajın içeriğiyle ilgili bilgiye ulaşılamaz. Genel bir kural olarak, kişinin bir suç işlediğine dair şüphe bulunması için makul gerekçelerin olması ve tedbirin soruşturmanın amaçları gereği özellikle gerekli olması halinde (soruşturmanın konusu en az iki yıl hapis cezası ile cezalandırılabilecek bir suç, suça girişim, hazırlık veya bu suça teşebbüs olmalıdır), RB'nin 27'nci Bölümünün 20'nci paragrafı kapsamında, elektronik iletişimin incelemeye alınması hükmü verilebilir. RB'nin 27'nci Bölümünün 21'inci paragrafı uyarınca, acil durumlar dışında, savcı yargı yetkisi olan mahkemeden elektronik iletişimi incelemesini talep etmelidir.

Saklı verilerin güvenliği ve korunması

28. LEK 6'ncı Bölümünün 3a paragrafı uyarınca, verileri saklama yükümlülüğü olan elektronik iletişim hizmeti sağlayıcıları işlenen verinin güvenliğini sağlamak için uygun teknik ve örgütsel tedbirleri almalıdır. Ancak, C-203/15 sayılı Dava'da sevk eden mahkemenin sağladığı bilgiye göre, İsveç hukuku verilerin saklanacağı yere dair herhangi bir hüküm koymamıştır.

Birleşik Krallık Hukuku

DRIPA (Veri Saklama ve Araştırma Yetkileri Kanunu)

29. DRIPA'nın 'Teminatlara tabi ilgili iletişim verilerini saklama yetkisi' başlıklı Birinci Kısmı:

'(1) Eğer Dışişleri Bakanı zorunluluğun 2000 Araştırma Yetkileri Kanunu Tüzüğü'nün 22(2)'nci kısmının (a)-(h) paragrafları arasında bahsedilen amaçlardan (iletişim verilerinin elde edilmesindeki amaçlar) bir veya daha fazlası için gerekli ve orantılı olduğunu düşünürse, Dışişleri Bakanı tebligat yoluyla ("veri saklama bildirimi") bir kamu telekomünikasyon işletmecisine ilgili iletişim verilerini saklamasını rica edebilir.

(2) Veri saklama bildirimi:

(a) belli bir işletmeciyle veya işletmecilerin tanımlarıyla ilgili olabilir,
(b) Tüm verilerin saklanmasını veya verilerin tanımlanmasını gerektirebilir,
(c) verilerin saklanması gereken süreyi veya süreleri belirtebilir,
(d) verilerin saklanmasıyla ilgili diğer gereklilikleri veya sınırlamaları içerebilir,
(e) farklı amaçlara yönelik farklı maddeler hazırlayabilir,

(f) bildirimin yapıldığı veya yürürlüğe girdiği zamanda mevcut olan veya olmayan verilerle ilişkili olabilir.

(3) Dışişleri Bakanı tüzük uyarınca ilgili iletişim verilerinin saklanması hakkında farklı maddeler hazırlayabilir.

(4) Bu maddeler özellikle aşağıdakiler hakkında olabilir:

(a) Veri saklama bildirimi öncesi zorunluluklar,
(b) Veri saklama bildirimi kapsamında verilerin saklanması gereken azami süre,
(c) Veri saklama bildiriminin içeriği, ibraz edilmesi, yürürlüğe girmesi, incelenmesi, değişiklikleri ya da iptali,
(d) Bu kısma dayanarak saklanan verilere erişimin bütünlüğü, güvenliği ya da korunması, verilerin açıklanması veya ortadan kaldırılması,
(e) ilgili zorunluluk ve kısıtlamaların uygulanması veya bu zorunluluk veya kısıtlamalara uyumluluğun denetlenmesi,
(f) İlgili zorunluluk veya kısıtlamalar ya da ilgili yetkilerle ilgili uygulama ilkeleri,
(g) Kamu telekomünikasyon işletmecilerinin yaptığı harcamaların Dışişleri Bakanı tarafından (şartlı veya şartsız olarak) ilgili zorunluluk veya kısıtlamalara uyumlu bir şekilde ödenmesi,
(h) [2009 Veri Saklama Tüzüğü (EC Direktifi)]nin yürürlükten kalkması ve bu kısım sayesinde veri saklama işlemine geçilmesi.

(5) 3'üncü altbölümdeki tüzüğün ilgili verilerle ilgili açıkladığı gibi, (4)(b) altbölümü gereğince azami süre ilk günden itibaren 12 ayı geçmemelidir.

...'

30. DRIPA'nın 2'nci Kısmı 'ilgili iletişim verileri' ifadesi ile ilgili şu tanımı yapmaktadır: '[2009 Veri Saklama Tüzüğü (EC Direktifi)]'nün Programı'nda bahsedilen iletişim verileridir. Söz konusu veriler telekomünikasyon hizmeti verilirken kamu telekomünikasyon işletmecileri tarafından İngiltere'de üretilmiş ve işlenmiştir.'

RIPA (Araştırma Yetkileri Kanunu Tüzüğü)

31. 2000 tarihli Araştırma Yetkileri Kanunu Tüzüğü'nün ('RIPA') İkinci Bölümü'nün 'İletişim verilerinin yasal olarak elde edilmesi ve açıklanması' başlıklı 21(4)'üncü Kısmı aşağıdaki gibidir:

'Bu Bölüm'de "iletişim verileri" aşağıdaki anlamlara gelmektedir:

(a) Posta hizmeti veya telekomünikasyon sistemi vasıtasıyla iletilmek amacıyla bir haberleşmenin içerisinde yer alan veya haberleşmeye bağlanan (gönderici veya alıcı tarafından) tüm trafik verileri,
(b) Bir iletişimin içeriğini içinde barındırmayan bilgiler ((a) paragrafı kapsamına giren bilgiler dışında) ve herhangi bir kişinin;
(i) posta veya telekomünikasyon hizmetlerini kullanma şekli, veya
(ii) bir telekomünikasyon hizmetinin kişilere sağlanması veya kişilerce kullanılmasıyla bağlantılı olacak şekilde, herhangi bir telekomünikasyon sistemini kullanım şekliyle ilgili tüm bilgiler.

(c) posta hizmeti veya telekomünikasyon hizmeti veren bir kişinin hizmet verdiği kişilere ait elinde tuttuğu veya elde ettiği, (a) ve (b) paragrafları kapsamına girmeyen tüm bilgiler'.

32. C-698/15 sayılı Dava'nın referans listesinde 'kullanıcı konum verileri' yer alırken iletişimin içeriğine dair veri bulunmamaktadır.
33. Saklanan verilere erişime ilişkin RIPA'nın 22'nci Kısmı aşağıda verilmiştir:

'(1) Bu Bölümün amaçları doğrultusunda yetkilendirilen bir kişinin 2'nci alt kısımda belirtilen gerekçelere bakarak tüm iletişim verilerini elde etmenin gerekli olduğuna inandığı hallerde, bu kısım uygulanır.

(2) Eğer;

(a) ulusal güvenliğin menfaati,
(b) suçları önleme veya tespit etme yada düzensizliği önlemek,
(c) Birleşik Krallık'ın ekonomik refahı,
(d) Kamu güvenliğinin menfaati,
(e) Kamu sağlığının korunması,
(f) Bir hükümet birimine ödenecek her tür vergi, gümrük vergisi, harç, ödeme, katkı veya ücretin değerlendirilmesi veya toplanması,
(g) acil bir durumda, kişilerin ölmesini, yaralanmasını veya fiziksel, ruhsal sağlığına zarar gelmesini önlemek için ya da kişilerin fiziksel veya ruhsal sağlığına gelebilecek zararları hafifletmek için ya da
(h) Dışişleri Bakanı'nın emriyle bu alt kısmın amaçları doğrultusunda belirlenen herhangi bir amaç için gerekli olduğunda ((a)-(g) paragraflarında belirtilmiyor), alt kısımda belirtilen gerekçeler doğrultusunda iletişim verilerini elde etmek gereklidir.

….

(4) 5'inci alt kısım kapsamında, eğer yetkilendirilen kişi posta veya telekomünikasyon işletmecisinin iletişim verilerine ulaştığını, ulaşmış olabileceğini veya ulaşabileceğini düşünürse, o kişi posta veya telekomünikasyon işletmecisine bir uyarı göndererek,

(a) işletmeci verilere henüz sahip değilse, işletmecinin verileri elde etmesini ve
(b) her durumda, elindeki ya da elde edeceği tüm verileri açıklamasını gerekli görebilir.

(5) Eğer yetkilendirilen kişi söz konusu verinin izin verilen yöntemle, yetkilendirme veya uyarı yoluyla elde edilmesinin hedeflenen amaçla orantılı olduğuna inanmıyorsa, 3'üncü alt kısım uyarınca yetki vermez veya 4'üncü alt kısım uyarınca tebligat yapmaz. '

34. RIPA'nın 65'inci Kısmı uyarınca, verilerin uygun olmayan bir yolla elde edildiğine yönelik kanıt varsa, Araştırma Yetkileri Mahkemesi'ne (Birleşik Krallık) şikayet edilebilir.

2014 Veri Saklama Tüzüğü

35. DRIPA'ya dayanarak kabul edilen 2014 Veri Saklama Tüzüğü (2014 Tüzüğü) üç bölümden oluşmaktadır. İkinci Bölüm mevzuatın 2-14 sayıları arasındaki tüzükleri içermektedir. 'Veri saklama tebligatı' başlıklı 4'üncü Tüzük aşağıdadır:

'(1) Veri saklama tebligatı aşağıdakileri belirtmelidir:

(a) İlgili olduğu kamu telekomünikasyon işlemcisi (ya da işlemcilerin tanımı),
(b) Saklanması gereken ilgili iletişim verileri,
(c) Verilerin saklanacağı süre veya süreler,
(d) Verilerin saklanmasıyla ilgili diğer zorunluluk ve kısıtlamalar.

(2) Veri saklama tebligatı;

(a) Trafik verileri veya hizmet kullanımı verileri söz konusu olduğunda ilgili haberleşmenin gününden başlayarak,

(b) katılımcı verileri söz konusu olduğunda ilgili kişinin söz konusu telekomünikasyon hizmetini bıraktığı gün ya da (daha öncesinde) verilerin değiştirildiği günden başlayarak 12 ayı geçmeyecek şekilde verilerin saklanmasını zorunlu kılmalıdır.

…'

36. 2014 Yönetmeliği'nin 7'nci Tüzüğü 'Veri bütünlüğü ve güvenliği' başlığıyla aşağıdaki gibidir:

'(1) [DRIPA]'nın Birinci Kısmı uyarınca iletişim verilerini saklayan bir kamu telekomünikasyon işlemcisi:

(a) Diğer sistemlerdeki veriler ve söz konusu verilerin aynı bütünlüğe sahip olmasını ve aynı güvenlik ve korumaya tabi olmasını sağlamalıdır,
(b) uygun teknik ve kurumsal tedbirler yoluyla verilere yalnızca özel yetkilendirilmiş personelin erişebilmesini sağlamalıdır,
(c) uygun teknik ve kurumsal tedbirler alarak verilerin kazara veya yasalara aykırı bir şekilde yok edilmesini, kazara kaybedilmesi veya değiştirilmesini ya da yetki alınmadan veya yasalara uyulmadan saklanmasını, işlenmesini, erişilmesini veya açıklanmasını engellemelidir.

(2) [DRIPA]'nın Birinci Kısmı'na dayanarak iletişim verilerini saklayan bir kamu telekomünikasyon işlemcisi, ilgili Kısmın verilerin korunmasını yetkilendirmediği veya yasaların veri saklanmasına izin vermediği durumlarda, verileri yok etmelidir.

(3) Paragraf (2)'de bahsedilen verileri yok etme zorunluluğu, verilerin silinerek erişimin imkansız hale getirilmesi anlamına gelmektedir.

(4) İşlemcinin verilerin aylık veya daha kısa dönemler içinde silinmesini uygun görmesi ve bunun için ayarlama yapması yeterlidir.'

37. 2014 Tüzüğünün 8'inci Tüzüğü, 'Saklanan verilerin açıklanması' başlığıyla aşağıdaki gibidir:

'(1) Bir kamu telekomünikasyon işlemcisi, [DRIPA]'nın 1(6)(a) Kısmı kapsamına girmeyen açıklamaları engellemek amacıyla, [DRIPA]'nın Birinci Kısmına dayanarak saklanan verilere erişim kurallarını düzenleyen yeterli sayıda güvenlik sistemi (teknik ve kurumsal tedbirler dahil olmak üzere) oluşturmalıdır.

(2) [DRIPA]'nın Birinci Kısmı'na dayanarak iletişim verilerini saklayan bir kamu telekomünikasyon işlemcisi verilerin talep üzerine gecikmeden iletilmesini sağlamalı, verileri de buna dikkat ederek saklamalıdır.'

38. 2014 Tüzüğünün 'Bilişim Komiserinin Denetimi' başlıklı 9'uncu Tüzüğü şunu öngörür:

'Bilişim Komiseri, [DRIPA]'nın Birinci Kısmı'na dayanarak saklanan verilerin bütünlüğü, güvenliği veya yok edilmesine ilişkin olarak, bu Bölüm'de belirtilen zorunluluk veya kısıtlamalara uygunluk açısından denetim yapmalıdır.'

Uygulama İlkeleri

39. İletişim Verilerinin Elde Edilmesi ve Açıklanması Uygulama İlkeleri ('Uygulama İlkeleri'), 2.5-2.9 ve 2.36-2.45 arasındaki paragraflarda, iletişim verilerine erişimin gerekliliği ve orantılılığına ilişkin kılavuz ilkeler içermektedir. Sevk eden mahkemenin C-698/15 sayılı Dava'da açıkladığı gibi, bu ilkenin 3.72-3.77 paragrafları uyarınca, öncelikli veya gizli bilgilerle meşgul olan kişileri ilgilendiren iletişim verilerinin arandığı durumlarda, gereklilik ve orantılılık özellikle göz önünde bulundurulmalıdır.
40. Uygulama İlkeleri'nin 3.78-3.84'üncü paragrafları uyarınca, bir gazetecinin kaynağını bulmak amacıyla iletişim verilerine başvurulan özel davalarda mahkeme kararı gereklidir. İlkelerin 3.85-3.87'nci paragrafları uyarınca, yerel makamlarca erişim başvurusu yapıldığı zaman yargı onayı gereklidir. Avukat müvekkil gizliliği tarafından korunan ya da tıp doktorları, Milletvekilleri ya da diyanet işleri başkanlarına ait iletişim verilerine erişebilmek için mahkeme veya bağımsız bir organdan izin almaya gerek yoktur.
41. Uygulama İlkeleri'nin 7.1'inci paragrafı gereğince, RIPA hükümleri kapsamında elde edilen iletişim verileri, kopyaları, özetleri güvenli bir şekilde muamele görmeli ve korunmalıdır. Buna ek olarak, Veri Koruma Kanunu'nun gereklilikleri de bu verilerle birlikte yer almalıdır.
42. Uygulama İlkeleri'nin 7.18'inci paragrafı uyarınca, Birleşik Krallık'taki bir kamu makamı iletişim verilerini sınır aşırı makamlara açıklamayı gözden geçiriyorsa, bu makam, diğer hususlarla birlikte, verilerin yeterince korunup korunmayacağını değerlendirmelidir. Ancak, 7.22'nci paragrafta belirtilene göre, üçüncü ülke yeterli seviyede koruma sağlamasa dahi, yüksek kamu yararının söz konusu olduğu durumlarda veriler üçüncü ülkeye iletilebilmektedir. C-698/15 sayılı Dava'da sevk eden mahkemenin verdiği bilgiye göre, İçişleri Bakanı bazı verilerin mevzuat hükümlerinden muaf tutulmasını sağlayacak ulusal güvenlik sertifikası çıkartabilir.
43. İlkelerin 8.1'inci paragrafında, diğer hususlarla birlikte, RIPA Birinci Bölüm İkinci Kısım'da yer alan yetki ve görevlerin uygulanmasını bağımsız olarak denetleme görevi bulunan İletişim Tespiti Komiseri (Birleşik Krallık), RIPA tarafından oluşturulmuştur. İlkelerin 8.3'üncü paragrafında belirtildiği üzere, Komiser 'bir kişinin kasıtlı olarak veya düşüncesizlik sonucu oluşmuş bir başarısızlıktan olumsuz etkilendiğine karar verirse' o kişiyi yetkilerin yasaya aykırı kullanıldığı şüphesi hakkında bilgilendirebilir.

Asıl davadaki anlaşmazlıklar ve ön karar için sorulan sorular

C-203/15 sayılı Dava

44. 9 Nisan 2014'de, İsveç'te bulunan elektronik iletişim hizmeti sağlayıcısı Tele2 Sverige, PTS'e 8 Nisan 2014 tarihli *Dijital Haklar İrlanda ve Diğerleri* davası kararının ardından (C-293/12 ve C-594/12; *'Dijital Haklar* hükmü, EU:C:2014:238), 2006/24 sayılı Direktif'in geçersiz olduğunu, 14 Nisan 2014'den itibaren LEK'in kapsamında olan elektronik iletişim verilerini saklamayı bırakacağını ve bu tarihten önce saklanmış verileri sileceğini açıklamıştır.
45. 15 Nisan 2014'te Rikspolisstyrelsen, (İsveç Polis Teşkilatı) Tele2 Sverige'in ilgili veriyi kendisine göndermeyi durdurduğunu belirten bir şikayeti PTS'ye iletmiştir.
46. 29 Nisan 2014'de justitieminister (İsveç Adalet Bakanı) dava konusu İsveç mevzuatını *Dijital Haklar* hükmü ışığında incelemesi için özel bir raportör atamıştır. 13 Haziran 2014 tarihli ve 'Datalagring, EU-rätten och svensk rätt, Ds 2014:23' başlıklı bir raporda (Veri saklama, AB ve İsveç Hukuku; '2014 raporu') özel raportörün değerlendirmesine göre, LEK'in 16a-16f paragraflarında belirtildiği üzere, verilerin saklanmasına ilişkin ulusal

mevzuat AB Hukuku ya da Roma'da 4 Kasım 1950'de imzalanan Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşme'sine ('AİHM') aykırı değildi. Özel raportör, *Dijital Haklar* kararının genel ve gelişigüzel bir şekilde saklanmasının ilkesel açıdan kınanması gerektiği şeklinde yorumlanamayacağını açıklamıştır. Aynı şekilde raportöre göre *Dijital Haklar* kararı, mevzuatın orantılı sayılabilmesi için Mahkeme tarafından uyulması zorunlu bir takım kriterler oluşturulduğu anlamına gelmemelidir. Raportör, İsveç mevzuatının AB Hukuku ile uyumluluğunu değerlendirmek için veriye erişim, saklama süresi, verilerin korunması ve güvenliği hakkındaki hükümler ışığında veri saklama işleminin tüm boyutları ve bunun gibi tüm koşulların değerlendirilmesi gerektiğini düşünmüştür.

47. Buna dayanarak, 19 Haziran 2014'te PTS, Tele2 Sverige'in suçla mücadele amacıyla LEK kapsamındaki verileri altı ay süreliğine saklamadığını ve böylece ulusal mevzuattaki yükümlülüklerini ihlal ettiğini ifade etmiştir. PTS 27 Haziran 2014 sayılı emriyle, Tele2 Sverige'in 25 Temmuz 2014 öncesindeki verileri saklamasını istemiştir.
48. Tele2 Sverige, 2014 raporunun Dijital Haklar kararının yanlış yorumlanması sonucu oluştuğunu ve veri saklama yükümlülüğünün Şart'ta bulunan temel hakları ihlal ettiğini değerlendirmiş ve bu nedenle 27 Haziran 2014 emrine karşı Förvaltningsrätten i Stockholm (İdari Mahkeme, Stokholm) huzurunda dava açmıştır. Mahkeme 13 Ekim 2014 kararıyla davayı geri çevirdiği için Tele2 Sverige sevk eden mahkemenin huzurunda bu karara itiraz etmiştir.
49. Sevk eden mahkemenin görüşüne göre, İsveç mevzuatının AB Hukuku ile uyumluluğu 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı açısından değerlendirilmelidir. Bu direktif, trafik ve konum verilerinin iletişimin iletilmesi için gerekli olmadığı zaman silinmesi veya anonim hale getirilmesini öngören genel bir kural oluşturmaktadır. Ancak direktifin 15'inci maddesinin birinci paragrafı bu genel kurala istisna getirme hakkı doğurmakta ve böylece belirtilen özel gerekçelerden biri mevcut olduğunda, Üye Devletlerin verileri silme veya anonim hale getirme zorunluluğunu sınırlamalarına izin vermekte hatta verilerin saklanmasını mümkün kılmaktadır. Nitekim, AB hukuku bazı durumlarda elektronik iletişim verilerinin saklanmasına izin vermektedir.

50. Bunun aksine sevk eden mahkeme, elektronik iletişim verilerini örneğin asıl davada geçen verileri saklamak gibi genel ve gelişigüzel bir yükümlülüğün, *Dijital Haklar* kararı dikkate alınmak suretiyle Şart'ın 7'nci, 8'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı ile uyumlu olup olmadığını belirlemeye çalışmaktadır. Tarafların görüşleri bu konuda farklılık gösterdiği için Mahkeme, Tele2 Sverige'in de ifade ettiği gibi elektronik iletişim verilerinin genel ve gelişigüzel saklanması işleminin Şart'ın 7'nci ve 8'inci maddeleri ve 52'nci maddesinin birinci paragrafı ile çelişip çelişmediğini ya da 2014 Raporu'nda belirtildiği gibi veri saklama işleminin uyumluluğunu veriye erişim, verinin korunması ve güvenliği ve saklama süresi ile ilgili hükümler ışığında değerlendirilip değerlendirilmeyeceğine net bir şekilde karar vermelidir.
51. Bu şartlar altında the Kammarrätten i Stockholm (Stockholm İdari Temyiz Mahkemesi, İsveç) yürütmeyi durdurma kararı vermiş ve ön karar alınması için aşağıdaki soruları Mahkeme'ye iletmiştir:

'(1) Tüm kişileri, elektronik iletişim ve trafik verilerini kapsayan trafik verilerini ayrım, kısıtlama veya istisna olmaksızın suçla mücadele etmek amacıyla saklamak gibi genel bir yükümlülük ... Şart'ın 7'nci ve 8'inci maddeleri ve 52'nci maddelerinin birinci paragrafı dikkate alınmak suretiyle 2002/58/EC sayılı Direktif'in 15'inci maddesinin birinci paragrafıyla uyumlu mudur?

(2) Birinci sorunun cevabının olumsuz olması halinde,

(a) ulusal makamların saklanmış bilgiye erişimi [referans listesinin 19-36'ncı paragrafları arasında tanımlandığı] gibi belirlenirse,
(b) veri koruma ve veri güvenliği için gerekli olanlar [referans listesinin 38-43'üncü paragrafları arasında tanımlandığı] gibi düzenlenirse ve
(c) iletişimin sonlandığı günden başlayarak hesaplanmak üzere altı ay boyunca ilgili tüm veriler saklanır ve ardından [referans listesinin 37'nci paragrafında tanımlandığı] gibi silinirse buna rağmen veri saklamaya izin verilebilir mi?'

C-698/15 sayılı Dava

52. Sayın Watson, Brice ve Lewis Yüksek Adalet Mahkemesi (İngiltere & Galler) ve Queen's Bench Mahkemesi (İstinaf Mahkemesi) (Birleşik Krallık) huzurunda, DRIPA'nın Birinci Kısmı'nın yasallığı hakkında adli denetim başvurusunda bulunmuş ve diğer hususlarla birlikte, bu Kısmın Şart'ın 7'nci ve 8'inci maddeleri ile AİHS'nin 8'inci maddesine uygun olmadığı iddiasında bulunmuştur.
53. Yüksek Adalet Mahkemesi (İngiltere & Galler) ve Queen's Bench Mahkemesi (İstinaf Mahkemesi) 17 Temmuz 2015 tarihli kararıyla, *Dijital Haklar* kararının iletişim verilerini saklama ve bu verilere erişim hakkında Üye Devletlerin mevzuatlarına yönelik 'AB Hukuku'nun zorunlu gerekliliklerini' oluşturduğuna karar vermiştir. Yüksek Adalet Mahkemesi'ne göre, Mahkeme verdiği hükümde 2006/24 sayılı Direktif'in orantılılık ilkesiyle uyuşmadığına karar verdiği için, aynı hükümleri içeren ulusal mevzuatlar da aynı şekilde bu ilkeyle uyuşamaz. *Dijital Haklar* kararındaki mantıktan anlaşıldığı gibi, iletişim verilerinin saklanması için bir genel kurallar bütünü oluşturan mevzuat, Şart'ın 7'nci ve 8'inci maddelerinde garanti edilen hakları ihlal etmektedir. Bu mevzuat, veriye erişim konusunda ulusal hukukun tanımlayacağı ve yukarıdaki maddelerdeki hakları koruyacak yeterli teminat sağlayan kurallarla desteklenmediği sürece bir ihlal söz konusu olacaktır. Dolayısıyla DRIPA'nın Birinci Kısmı saklı veriye erişim ve verinin kullanımına dair açık ve belirgin kurallar koymamış ve veriye erişim bir mahkeme ya da bağımsız bir idari organın ön incelemesine tabi tutulmamıştır, bu nedenle de Şart'ın 7'nci ve 8'inci maddeleriyle uyumlu değildir.
54. İçişleri Bakanı, İstinaf Mahkemesi'ne (İngiltere & Galler) (Hukuk Birimi) (Birleşik Krallık) verilen hüküm aleyhinde temyiz başvurusunda bulunmuştur.
55. Mahkemeye göre, DRIPA'nın 1(1)'inci Kısmı İçişleri Bakanı'na, bir mahkeme veya bağımsız bir idari organdan onay gerekmeksizin, posta ve telekomünikasyon hizmetlerine ait tüm verilerin kamu telekomünikasyon işlemcileri tarafından en fazla 12 ay süreliğine saklanmasını gerektirecek genel bir rejim oluşturma yetkisi vermektedir. İçişleri Bakanı, Birleşik Krallık mevzuatında belirtilen amaçlara ulaşılması için gerekli ve orantılı olduğunu düşünmesi halinde bu gerekliliği kabul etmektedir. Bu veriler iletişimin içeriğini kapsamamasına rağmen iletişim hizmeti kullanıcılarının mahremiyetine büyük bir müdahale teşkil edebilir.
56. Sevk eden mahkeme, temyiz sürecinde iletilen ve ön karar talebiyle birlikte Mahkeme'ye göndermeye karar verdiği 20 Kasım 2015 tarihli kararı ve referans listesinde, veri saklamaya ilişkin ulusal kuralların 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının kapsamına girdiğini ve bu yüzden Şart'ın gerekliliklerine uygun olmak zorunda olduğunu düşünmektedir. Ancak, o direktifin 1'inci maddesinin üçüncü paragrafında bahsedildiği gibi AB yasama organı saklı verilere erişim kurallarını uyumlu hale getirmemiştir.

57. Sevk eden mahkeme *Dijital Haklar* kararının asıl davada bahsedilen konular üzerindeki etkisini göz önüne alarak, bu kararı doğuran davada Mahkeme'nin ulusal mevzuatları değil 2006/24 sayılı Direktif'in geçerliliğini değerlendirdiğini belirtmektedir. Diğer hususlarla birlikte veri saklama ve veriye erişim arasındaki yakın ilişki göz önüne alındığında, Direktif'in bazı teminatlar içermesi gerekliydi ve bununla birlikte, Direktif tarafından oluşturulan veri saklama rejiminin hukuki açıdan incelemesi yapılırken, *Dijital Haklar* kararının o verilere erişim kurallarını analiz etmesi gerekliydi. Dolayısıyla, Mahkeme verdiği kararda, ulusal mevzuata uygulanabilen ancak AB hukukunu uygulamayan veriye erişimle ilgili zorunluluklar koymayı amaçlamamıştı. İlaveten, mahkemenin muhakemesi 2006/24 sayılı Direktif'in belirlediği hedef ile oldukça bağlantılıydı. Ancak, ulusal mevzuat bu mevzuatın hedefleri ve bağlamı ışığında değerlendirilmelidir.
58. Ön karar için Mahkeme'ye soru iletme ihtiyacı ile ilgili olarak, sevk eden mahkeme, referans listesi çıkarıldığında diğer Üye Ülkelerdeki beşi son derece mahkemesi olan altı mahkeme tarafından *Dijital Haklar* kararı baz alınarak ulusal mevzuatın geçersizliğinin açıklandığını vurgulamıştır. Mahkemenin huzuruna çıkan davalarda hüküm vermek için cevabın gerekli olmasına rağmen iletilen sorulara verilen cevap açık değildir.
59. Bu şartlar altında, İstinaf Mahkemesi (İngiltere & Galler) (Hukuk Birimi) yürütmeyi durdurma kararı almış ve ön karar alınması için Mahkeme'ye aşağıdaki soruları iletmiştir:

'(1) [*Dijital Haklar* kararı] (özellikle 60-62 arasındaki paragraflar dahil) [Şart'ın] 7'nci ve 8'inci maddelerine uyum sağlamak amacıyla, ulusal mevzuatlar kapsamında saklanan verilere erişimi düzenleyen Üye Devletler iç hukukuna uygulanmak üzere AB hukuku yükümlülüklerini mi oluşturuyor?

(2) [*Dijital Haklar* kararı] [Şart'ın] 7'nci ve/veya 8'inci maddelerinin kapsamını Avrupa İnsan Hakları Mahkemesi içtihadında yer alan AİHS 8'inci maddesinin de ötesine mi taşıyor?'

Mahkeme süreci

60. Mahkeme Başkanı 1 Şubat 2016 tarihli *Davis ve Diğerleri* (C-698/15, yayımlanmadı, EU:C:2016:70) kararıyla C-698-15 sayılı Dava'nın Mahkeme İçtüzüğünün 105'inci maddesinin birinci paragrafındaki hızlandırılmış usul kapsamında incelenmesine karar vermiş, böylece İstinaf Mahkemesi'nin isteğini yerine getirmiştir.
61. Mahkeme Başkanı'nın 10 Mart 2016 tarihli kararıyla, C-203/15 ve C-698/15 sayılı davalar usul ve yargılamanın sözlü kısmının amaçları doğrultusunda birleştirilmiştir.

Ön karar için iletilen soruların değerlendirmesi

C-203/15 sayılı Dava'daki birinci soru

62. Şart'ın 52'nci maddesinin birinci paragrafı ve 7'nci ve 8'inci maddeleri ışığında okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının, asıl davada gündemde olan ve suçla mücadele edilmesini, tüm katılımcı ve kayıtlı kullanıcıların elektronik iletişim araçlarına ilişkin trafik ve konum verilerinin genel ve gelişigüzel bir şekilde saklanmasını öngören ulusal mevzuatı engelleyip engellemediğini, the Kammarrätten i Stockholm (İdari Temyiz Mahkemesi, Stockholm) C-203/15 sayılı Dava'daki ilk soruyla anlamaya çalışmaktadır**.**
63. Bu sorunun ortaya çıkma nedeni şudur: Asıl davadaki ulusal mevzuata aktarılması düşünülen 2006/24 sayılı Direktif, trafik ve konum verilerini saklama ve ulusal makamların verilere erişimini düzenlemesine rağmen *Dijital Haklar* kararı nedeniyle

hükümsüz ilan edilmiş ve bu durum tarafların *Dijital Haklar* kararının kapsamı ve mevzuata etkisi konusunda anlaşmazlığa varmasına rağmen gerçekleşmiştir.

64. İlk olarak asıl davadaki gibi bir ulusal mevzuatın AB hukuku kapsamına girip girmediği incelenmelidir.

2002/58 sayılı Direktif'in kapsamı

65. Yazılı gözlemlerini Mahkeme'ye sunan Üye Devletler, trafik ve konum verilerinin saklanması ve verilere ulusal makamlarca erişilmesi hakkındaki ve suçlarla mücadele amacı taşıyan ulusal mevzuatın 2002/58 sayılı Direktif kapsamında olup olmadığı ve kapsamında ise ne ölçüde kapsamı içinde yer aldığı konusunda fikir ayrılığı yaşamaktadır. Belçika, Danimarka, Almanya ve Estonya Hükümetleri, İrlanda ve Hollanda Hükümeti bu soruya evet cevabını verirken, Çek Hükümeti mevzuatın asıl hedefinin suçla mücadele olduğunu belirterek hayır cevabını vermiştir. Birleşik Krallık ise, yalnızca verilerin saklanmasına ilişkin mevzuatın Direktif'in kapsamına girdiğini, yetkili ulusal kolluk makamlarının bu verilere erişimini düzenleyen mevzuatın Direktif kapsamında yer almadığını belirtmiştir.
66. Komisyon C-203/15 sayılı Dava'da Mahkeme'ye gönderdiği yazılı gözlemlerinde söz konusu ulusal mevzuatın 2002/58 sayılı Direktif'in kapsamına girdiğini belirtirken, C-698/15 sayılı Dava'daki yazılı gözlemlerinde yalnızca veri saklamaya ilişkin ulusal kuralların o direktifin kapsamına girdiğini ancak ulusal makamların bu verilere erişimine ilişkin kuralların bu kapsama girmediğini ifade etmiştir. Ancak Komisyon'a göre, ulusal makamların verilere erişimine ilişkin kurallar elektronik iletişim hizmeti sağlayıcılarının sakladığı verileri düzenleyen ulusal mevzuatın Şart'ın 7'nci ve 8'inci maddelerindeki temel haklara orantılı bir müdahale teşkil edip etmediğini belirlemek için dikkate alınmalıdır.
67. Bu bağlamda, 2002/58 sayılı Direktif'in kapsamını değerlendirirken diğer hususlarla birlikte o direktifin genel yapısının da dikkate alınması gereklidir.
68. 2002/58 sayılı Direktif'in birinci maddesinin birinci paragrafına göre, direktif diğer hususlarla birlikte temel hak ve özgürlüklerin eşit seviyede korunmasını ve özellikle, elektronik iletişim sektöründe kişisel verilerin işlenmesiyle ilgili mahremiyet ve gizlilik hakkını sağlamak için gerekli olan ulusal hukuk hükümlerinin uyumlu hale getirilmesini öngörmektedir.
69. Direktif'in birinci maddesinin üçüncü paragrafı, ceza hukuku, kamu güvenliği, savunma, devlet güvenliği alanlarındaki devlet faaliyetleri gibi ve devlet güvenlik işleri söz konusu olduğunda (kıyaslayarak bkz; 95/46 sayılı Direktif'in üçüncü maddesinin ikinci paragrafının birinci bendine istinaden, 6 Kasım 2003 tarihli karar, *Lindqvist*, C-101/01, EU:C:2003:596, 43'üncü paragraf ve 16 Aralık 2008 tarihli, *Satakunnan Markkinapörssi ve Satamedia*, C-73/07, EU:C:2008:727, 41'inci paragraf) devletin ekonomik refahı dahil olmak üzere bazı alanlarda 'devlet faaliyetlerini' kendi kapsamından çıkarmaktadır.

70. 2002/58 sayılı Direktif'in üçüncü maddesi, Avrupa Birliği kamuya açık iletişim ağlarında ve veri toplama ve tespit cihazlarını destekleyen ağlarda mevcut olan kamuya açık elektronik iletişim hizmetlerinin verilmesiyle bağlantılı olan kişisel veri işleme sürecinde direktifin uygulanması gerektiğinden söz eder ('elektronik iletişim hizmetleri'). Sonuç olarak, direktifin bu tür hizmet sağlayıcılarının yürüttüğü faaliyetleri düzenlediği göz önüne alınmalıdır.
71. 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafına göre, belirtilen şartlara tabi olmak kaydıyla, Üye Devletler '[o direktifin] 5'inci, 6'ncı maddeleri, 8'inci maddesinin 1'inci, 2'nci, 3'üncü ve 4'üncü paragraflarının ve 9'uncu maddesinin öngördüğü hak ve yükümlülüklerin kapsamını sınırlayan yasama tedbirleri' alabilirler. O direktifin 15'inci maddesinin birinci paragrafının ikinci cümlesi Üye Devletlerin kabul edebileceği tedbirlere örnek teşkil eden ve 'veri saklanmasını öngören' tedbirleri açıklar.
72. Aslında, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafında atıf yapılan yasama tedbirleri Devlet veya Devlet makamlarının faaliyetlerini ilgilendirmektedir ve kişilerin aktif olduğu alanlarla ilgisizdir (bkz, buna ilişkin 29 Ocak 2008 tarihli karar *Promusicae*, C-275/06, EU:C:2008:54, 51'inci paragraf). Ayrıca, hükümdeki tedbirlerin taşıdığı; milli güvenliğin korunması, savunma ve kamu güvenliği, cezai eylemlerin veya elektronik iletişim sistemlerinin izinsiz kullanılmasının önlenmesi, soruşturulması, tespiti ve kovuşturulması vb. hedefler direktifin 1'inci maddesinin üçüncü paragrafındaki faaliyet hedefleriyle büyük ölçüde örtüşmektedir.
73. Ancak, 2002/58 sayılı Direktif'in genel yapısı göz önüne alındığında, bu kararın önceki paragrafında tanımlanan faktörler 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafında bahsedilen yasama tedbirlerinin bu direktif kapsamından çıkartıldığı sonucunu doğurmaz, çünkü aksi halde bu hüküm herhangi bir amaçtan yoksun olurdu. Nitekim, 15'inci maddenin birinci paragrafına göre, suçla mücadele etmek amacıyla verilerin saklanması gibi bu maddedeki ulusal tedbirler direktifin kapsamına girmektedir. Çünkü bu madde Üye Devletlere yalnızca direktifteki şartların yerine getirilmesi şartıyla bu tedbirleri kabul etme izni vermektedir.
74. Buna ilaveten 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafında bahsedilen yasama tedbirleri bu hükümdeki amaçlar doğrultusunda elektronik iletişim hizmetleri sağlayıcılarının faaliyetlerini yönetir. Aynı şekilde direktifin 3'üncü maddesi ile birlikte okunan 15'inci maddenin birinci paragrafı yasama tedbirlerinin o direktif kapsamında olduğu şeklinde yorumlanmalıdır.
75. Bu direktifin kapsamı, asıl davada sağlayıcıların trafik ve konum verilerini saklamalarını gerektiren tedbir gibi bir yasama tedbiri kabul etmeye kadar uzanmaktadır. Çünkü bunu yapmak kişisel verilerin sağlayıcılar tarafından işlenmesini de içine alır.
76. Direktifin kapsamı aynı zamanda asıl davada olduğu gibi elektronik iletişim hizmeti sağlayıcılarının sakladığı verilere ulusal makamlar tarafından erişilmesiyle ilgili bir yasama tedbirini içine alır.
77. 2002/58 sayılı Direktif'in 5'inci maddesinin birinci paragrafında garanti edilen elektronik iletişimin ve ilgili trafik verilerinin gizliliğinin korunması ifadesi özel kişi, organ ya da devlet organı fark etmeksizin kullanıcılar dışındaki tüm kişiler tarafından alınan tedbirlere uygulanır. Direktifin 21'inci gerekçesinde doğrulandığı gibi, direktif elektronik iletişimin gizliliğini sağlayabilmek için 'iletişimle ilgili tüm veriler' dahil olmak üzere, haberleşmeye izinsiz erişimi önlemeyi amaçlamaktadır.
78. Bu şartlar altında eğer bir yasama tedbiri sırasında bir Üye Devlet, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafına dayanarak, bu hükmün amaçları doğrultusunda ve belirtilen şartları taşımak kaydıyla, elektronik iletişim hizmeti sağlayıcılarından ulusal makamlara saklı verilere erişim izni vermesini istediğinde, bu

tedbir kişisel verilerin sağlayıcılar tarafından işleme sokulmasını ilgilendirir ve bu süreç direktifin kapsamına girer.

79. Buna ek olarak, veriler gerekli olduğunda yalnızca yetkili ulusal makamların erişebilmesi için saklandığından dolayı, verilerin saklanmasını öngören ulusal mevzuat, ilke olarak, yetkili ulusal makamların elektronik iletişim hizmetleri sağlayıcıları tarafından saklanan verilere erişmesine ilişkin hükümlerin oluşturulmasını zorunlu kılar.
80. 2002/58 sayılı Direktif'in 15'inci maddesinin (1b) sayılı paragrafı bu yorumu desteklemektedir. Bu maddeye göre, kullanıcı kişisel verilerine erişim taleplerine cevap verirken sağlayıcılar tarafından ulusal usuller oluşturulmalıdır. Bu usuller direktifin 15'inci maddesinin birinci maddesi uyarınca ulusal hukuk hükümleri baz alınarak oluşturulmalıdır.
81. Yukarıda bahsedilenlerden anlaşılacağı gibi, C-203/15 ve C-698/15 sayılı davalarda bahsedildiği gibi ulusal mevzuat 2002/58 sayılı Direktif'in kapsamına girmektedir.

Şart'ın 7'nci, 8'inci, 11'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının yorumlanması

82. 2002/58 sayılı Direktif'in birinci maddesinin ikinci paragrafına göre, bu direktif hükümlerinin 95/46 sayılı Direktif'i 'daha ayrıntılı anlattığı ve tamamladığına' dikkat edilmelidir. 2'nci gerekçede belirtildiği gibi, 2002/58 sayılı Direktif, özellikle Şart'ın 7'nci ve 8'inci maddelerindeki haklara tamamen saygı duyulmasını amaçlar. Bu bağlamda, 2002/58 sayılı Direktif'i oluşturan, kişisel verilerin işlenmesi ve elektronik iletişim sektörünün gizliliğinin korunmasına ilişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktif Önerisinin açıklayıcı memorandumunda belirtildiği gibi (COM(2000) 385 final), AB Yasama meclisi 'kullanılan teknolojiye bakılmaksızın, elektronik iletişim hizmetlerinin tümü için yüksek seviyede kişisel veri ve gizlilik korumasının sürdürülmesi' için çalışmıştır.
83. Bu bağlamda, yeni teknolojilerin çıkması ve otomatik depolama ve veri işlemenin artan kapasitesi sonucunda, elektronik iletişim hizmetleri kullanıcılarının kişisel veri ve gizliliklerine yönelik bazı riskler oluşmaktadır. 2002/58 sayılı Direktif'in özellikle 6'ncı ve 7'nci gerekçelerinden anlaşılacağı gibi Direktif bu risklere karşı koruma sağlamayı amaçlayan bazı özel hükümler içermektedir.
84. Direktif'in 5'inci maddesinin birinci paragrafına göre, Üye Devletler ulusal mevzuatları yoluyla kamu iletişim ağı ve kamu elektronik iletişim hizmetleriyle yürütülen yazışmaların gizliliğini ve ilgili trafik verilerinin gizliliğini sağlamak zorundadır.
85. 2002/58 sayılı Direktif'in 5'inci maddesinin birinci paragrafının ikinci cümlesinde açıklandığı gibi, diğer hususlarla birlikte, iletişimin gizliliği ilkesi genel bir kural olarak; kullanıcılar dışındaki kişilerin ilgili kullanıcıların rızası olmadan elektronik iletişime ilişkin trafik verilerini depolama hakkı olmadığını ifade eder. Yalnızca 15'inci maddenin birinci paragrafı uyarınca yasal olarak yetkilendirilen kişiler için ve haberleşmenin iletilmesi için gereken teknik depolama hususunda istisnalar vardır (bkz, 29 Ocak 2008 tarihli karar, *Promusicae*, C-275/06, EU:C:2008:54, 47'nci paragraf).
86. Aynı şekilde, 2002/58 sayılı Direktif'in 22'nci ve 26'ncı gerekçelerinde doğrulandığı gibi, direktifin 6'ncı maddesi gereğince, trafik verilerinin işlenmesi ve depolanması yalnızca gerekli olduğu ölçüde ve faturalama, hizmet pazarlaması ve katma değer hizmetlerinin sağlanması için gereken süre içinde onaylanır (bkz, 29 Ocak 2008 tarihli karar, *Promusicae*, C-275/06, EU:C:2008:54, 47'nci ve 48'inci paragraflar). Hizmetler, yalnızca faturaya yasal yolla itiraz etme süresi ya da ödeme yapılması için yasal süreç başlatma süresinin sonuna kadar faturalandırılabilir. Bu süre geçtiğinde, işlenen ve depolanan veriler silinmeli veya anonim hale getirilmelidir. Direktif'in 9'uncu maddesinin birinci paragrafı, trafik verileri hariç konum verilerinin bazı şartlara tabi olduğunu

belirtmektedir. Yalnızca veriler anonim hale geldikten sonra veya kullanıcı ya da katılımcı rızası alındıktan sonra veri işlemi yapılabilir.

87. 2002/58 sayılı Direktif'in 5'inci, 6'ncı maddesi ve 9'uncu maddesinin birinci paragrafı iletişimin ve ilgili verilerin gizliliğini sağlamayı, kötüye kullanım risklerini en aza indirmeyi amaçlamaktadır. Bu maddelerin kapsamı direktifin aşağıda yer alan 30'uncu gerekçesi ışığında değerlendirilmelidir: 'Elektronik iletişim ağları ve hizmetlerinin temin edilmesini sağlayan sistemler kişisel verilere olan ihtiyacı en aza indirmek için tasarlanmalıdır'.
88. Aslında, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı, Üye Devletlere direktifin 5'inci maddesi birinci paragrafında belirtilen kişisel verilerin gizliliğini sağlama ilkesine ve 6'ncı ve 9'uncu maddelerdeki diğer yükümlülüklere bazı istisnalar getirme imkanı tanımıştır (bkz, 29 Ocak 2008 tarihli karar, *Promusicae*, C-275/06, EU:C:2008:54, 50'nci paragraf).
89. Ancak, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı uyarınca Üye Devletler iletişim ve ilgili trafik verilerinin gizliliği ilkesinin kapsamını sınırlama imkanına sahip olduğundan dolayı, bu hüküm Mahkeme'nin yerleşik içtihadı gereğince kesin surette yorumlanmalıdır (kıyaslayarak bkz, 22 Kasım 2012 tarihli karar, *Probst*, C-119/12, EU:C:2012:748, 23'üncü paragraf). Bu nedenle bu hüküm, 2002/58 sayılı Direktif'in 5'inci maddesinin anlamsız hale gelmemesi halinde, söz konusu ilkeye ve özellikle bu maddedeki veri depolama yasağına getirilen istisnaların kurallaşmasına izin veremez.
90. Bu bağlamda şuna dikkat edilmelidir: 2002/58 sayılı Direktif'in 15'inci madde birinci paragraf ve birinci cümlesinde, yasal tedbirlerin amaçladığı ve iletişimin ve ilgili trafik verilerinin gizliliği ilkesine istisna teşkil eden hedefler, 'milli güvenliği (Devlet güvenliği), savunmayı, kamu güvenliğini, ceza gerektiren suçların veya elektronik iletişim sisteminin izinsiz kullanımının önlenmesi, soruşturulması, tespiti ve kovuşturulmasını güvence altına almalıdır' ya da bu hedefler 2002/58 sayılı Direktif'in 15'inci madde, birinci paragrafı birinci cümlesinin (bkz, 29 Ocak 2008 tarihli karar, *Promusicae*, C-275/06, EU:C:2008:54, 53'üncü paragraf) atıf yaptığı 95/46 sayılı Direktif'in 13'üncü maddesi birinci paragrafında bahsedilen diğer hedeflerden biri olmalıdır. Bu hedefler listesi, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının ikinci cümlesinden anlaşılacağı gibi geniş kapsamlıdır ve yasama tedbirlerinin 15'inci maddenin birinci paragrafının birinci cümlesindeki "gerekçeler" baz alınarak doğrulanması gerektiğini ifade eder. Aynı şekilde, Üye Devletler önceki hükümde listelenmeyen amaçları taşıyan tedbirleri kabul edemez.

91. Buna ek olarak, 2002/58 sayılı Direktif'in 15'inci maddesi birinci paragrafı üçüncü cümlesi uyarınca, '15'inci madde birinci paragrafta atıfta bulunulan tüm tedbirler, Şart'ın garantilediği genel ilkeler ve temel hakları içine alan 6'ncı maddenin birinci ve ikinci paragraflarında atıf yapılan tedbirler de dahil olmak üzere, Avrupa Birliği Hukukunun genel ilkelerine riayet etmelidir. Dolayısıyla, 2002/58 sayılı Direktif'in 15'inci maddesi birinci paragrafı, Şart'ın garanti altına aldığı temel haklar doğrultusunda yorumlanmalıdır (kıyaslayarak bkz, 95/46 sayılı Direktif'le ilişkili olan 20 Mayıs 2002 tarihli karar, *Österreichischer Rundfunk ve Diğerleri*, C-465/00, C-138/01 ve C-139/01, EU:C:2003:294, 68'inci paragraf; 13 Mayıs 2014 tarihli karar, *Google Spain ve Google*, C 131/12, EU:C:2014:317, 68'inci paragraf, ve 6 Ekim 2015 tarihli karar, *Schrems*, C 362/14, EU:C:2015:650, 38'inci paragraf).

92. Bu bağlamda, elektronik iletişim hizmetleri sağlayıcılarına asıl davadaki gibi ulusal mevzuat tarafından getirilen trafik verisini saklama ve gerektiğinde yetkili ulusal

makamlarla paylaşma yükümlülüğü, ön karar başvurusu için sorulan sorularda açıklanan Şart'ın 7'nci ve 8'inci maddelerine ve Şart'ın 11'inci maddesinde garantilenen ifade özgürlüğüne uyum konusunda sorular yaratmaktadır (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin olarak *Dijital Haklar* kararının 25'inci ve 70'inci paragrafları).

93. Bundan ötürü, Şart'ın 7'nci maddesinde garantilenen özel hayatın gizliliği ve 8'inci maddesinde garantilenen kişisel verileri koruma hakkının önemi, Mahkeme'nin içtihadından anlaşıldığı üzere (bkz, 6 Ekim 2015 tarihli karar, *Schrems*, C-362/14, EU:C:2015:650, 39'uncu paragraf ve atıfta bulunulan içtihat), 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafını yorumlarken dikkate alınmalıdır. Her demokratik toplumun özel bir önem atfettiği ifade özgürlüğü hakkı için de aynı durum söz konusudur. Şart'ın 11'inci maddesinde garanti edilen bu temel hak çoğulcu, demokratik bir toplumun temel yapıtaşlarından birini oluşturur ve ABA'nın (Avrupa Birliği Anlaşması) 2'nci maddesi kapsamında Birliğin üzerine kurulu olduğu değerlerden biridir (bkz, 12 Haziran 2003 tarihli karar, *Schmidberger*, C-112/00, EU:C:2003:333, 79'uncu paragraf, ve 6 Eylül 2011 tarihli karar, *Patriciello*, C-163/10, EU:C:2011:543, 31'inci paragraf).
94. Bu bağlamda, Şart'ın 52'nci maddesinin birinci paragrafı kapsamında, Şart'ta tanınan hak ve özgürlüklerin kullanılması sırasında yapılacak kısıtlamaların kanunlar tarafından öngörülmesi ve bu hak ve özgürlüklerin esasına saygılı olması gerektiği hatırlanmalıdır. Orantılılık ilkesi dikkate alındığında, bu hak ve özgürlüklerin kullanımı, yalnızca gerekli görüldüğünde ve Avrupa Birliği'nin toplumun menfaati için kabul ettiği hedefleri gerçekleştirmesi ve diğer kişilerin hak ve özgürlüklerini koruma ihtiyacını karşılaması halinde kısıtlanabilir (15 Şubat 2016 tarihli karar, *N.*, C-601/15 PPU, EU:C:2016:84, 50'nci paragraf).

95. Son konuya istinaden, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının birinci cümlesi uyarınca, Üye Devletler, bu hükümde belirtilen hedefleri dikkate alarak, 'demokratik bir toplumda gerekli, uygun ve orantılı olması' halinde, iletişim ve ilgili trafik verilerinin gizliliği ilkesine istisna teşkil eden bir tedbir kabul edebilir. Direktif'in 11'inci gerekçesi, bu tarz bir tedbirin niyetlenen amaçla 'kesinlikle' uyumlu olması gerektiğini ifade eder. Özellikle verilerin saklanması hususunda, direktifin 15'inci maddesinin birinci paragrafının ikinci cümlesi, verilerin 'kısıtlı süre için' saklanması ve direktifin 15'inci maddesinin birinci paragrafının birinci cümlesindeki hedeflerden biri tarafından haklı görülmesi gerektiğini belirtir.

96. Mahkeme'nin yerleşik içtihadında da orantılılık ilkesinden önemle bahsedilmektedir. Özel hayata saygı gösterilmesi hakkının AB düzeyinde korunması, kişisel verilerin korunmasına yönelik kısıtlama ve derogasyonların ancak kesin surette gereklilik oluşması halinde uygulanmasını gerektirir (16 Aralık 2008 tarihli karar, *Satakunnan Markkinapörssi ve Satamedia*, C-73/07, EU:C:2008:727, 56'ncı paragraf; 9 Kasım 2010 tarihli karar, *Volker und Markus Schecke ve Eifert*, C-92/09 ve C-93/09, EU:C:2010:662, 77'nci paragraf; *Dijital Haklar* kararı, 52'nci paragraf, ve 6 Ekim 2015 tarihli karar, *Schrems*, C-362/14, EU:C:2015:650, 92'nci paragraf).

97. C-203/15 sayılı davada olduğu gibi ulusal mevzuatın bu şartları taşıyıp taşımadığı konusunda ise, mevzuat tüm kayıtlı kullanıcı ve katılımcıların elektronik iletişim araçlarıyla ilgili bütün trafik ve konum verilerinin genel ve gelişigüzel olarak saklanmasını öngörür. Buna ek olarak, mevzuat elektronik iletişim hizmetleri sağlayıcılarına bu verileri sistematik, devamlı ve istisnasız olarak saklama yükümlülüğü getirir. Referans listesinde belirtildiği gibi, mevzuatın kapsamına giren veri kategorileri,

esas olarak 2006/24 sayılı Direktif'in saklanmasını gerekli gördüğü verilerle örtüşmektedir.

98. Elektronik iletişim hizmeti sağlayıcılarının saklaması gereken veriler sayesinde bir iletişimin kaynağını ve varış noktasını takip etmek, tespit etmek, iletişimin tarih, saat, süre ve türünü tespit etmek, kullanıcıların iletişim aracını belirlemek ve mobil iletişim aracının konumunu belirlemek mümkündür. Bu veriler, diğer hususlarla birlikte, katılımcı veya kayıtlı kullanıcının adı ve adresini, arayan kişinin telefon numarasını, aranan numarayı ve internet hizmetleri için IP adresini içerir. Bu veriler sayesinde, özellikle katılımcı veya kayıtlı kullanıcının iletişime geçtiği kişiyi tespit etmek ve haberleşmenin zamanını ve yerini belirlemek mümkündür. Buna ilaveten, bu veriler kullanılarak katılımcı veya kayıtlı kullanıcının kişilerle belirli bir süre içinde ne sıklıkta iletişime geçtiğini öğrenmek de mümkündür (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 26'ncı paragraf).

99. Bu verilerin tamamı sayesinde şahısların kişisel verilerine erişildiğinde, bu kişilerin günlük alışkanlıkları, daimi veya geçici ikametgahları, günlük veya diğer eylemleri, faaliyetleri, sosyal ilişkileri ve bulundukları sosyal çevreler gibi özel hayatlarını ilgilendiren konularda oldukça kesin sonuçlara ulaşmak mümkündür (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar kararı*, 27'nci paragraf). Özellikle bu veriler, Başsavcının Görüşü'nün 253, 254 ve 257-259 sayılı maddelerinde görüldüğü gibi, ilgili kişilerin bir profilini oluşturma imkanı sunacak ve iletişimin içeriği kadar hassas bilgilere erişilmesini sağlayacaktır.

100. Mevzuatın Şart'ın 7'nci ve 8'inci maddelerindeki temel haklara yaptığı bu müdahale büyük etkiler doğurmakla birlikte oldukça ciddi kabul edilmesi gereken bir müdahaledir. Katılımcı veya kayıtlı kullanıcının bilgisi olmadan verilerin saklanması sonucunda ilgili kişiler kendi özel hayatlarının sürekli bir gözetim altında olduğunu hissedebilir (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 37'nci paragraf).

101. Bu mevzuatın iletişimin içeriğini saklama izni vermediği ve bu yüzden bu hakların esasına (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 39'uncu paragraf) zarar vermediği durumlarda bile, trafik ve konum verileri elektronik iletişim araçlarının kullanımı üzerinde ve akabinde kullanıcıların Şart'ın 11'inci maddesiyle garantilenen ifade özgürlüğünü kullanma hakkı üzerinde bir etki oluşturabilir (karşılaştırarak bkz 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 28'inci paragraf).

102. Ulusal mevzuat uyarınca ve suçla mücadele amacıyla trafik ve konum verilerinin saklanması sonucunda söz konusu temel haklara yapılan müdahalenin ciddiyeti dikkate alındığında, sadece ağır suçla mücadele şeklinde belirtilen hedef bu tür bir tedbiri haklı göstermektedir (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 60'ıncı paragraf).

103. Buna ilaveten, organize suç ve terör gibi ağır suçlarla mücadelenin etkin bir şekilde yürütülmesi büyük ölçüde modern soruşturma tekniklerinin kullanımına bağlı olsa da, toplumsal yarar doğuracak bu tür bir hedef ne kadar öncelikli olursa olsun, tüm trafik ve konum verilerinin genel ve gelişigüzel olarak saklı tutulmasını öngören bir ulusal mevzuatı haklı gösteremez (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 51'inci paragraf).

104. Bu bağlamda öncelikle, bu mevzuat mevcut kararın 97'nci paragrafında tanımlanan özellikleri ışığında, 2002/58 sayılı Direktif'in oluşturduğu sisteme göre veri saklamanın istisna teşkil etmesine rağmen, trafik ve konum verilerini saklamayı bir kural haline getirmektedir.

105. İkinci olarak, asıl davada geçen ulusal mevzuat genelleme yaparak tüm katılımcı, kayıtlı kullanıcı, elektronik iletişim aracı ve trafik verilerini kapsamakta dolayısıyla hedeflenen amaca yönelik bir ayrım, sınırlama veya istisna uygulamamaktadır. Mevzuat elektronik iletişim hizmetlerini kullanan tüm kişileri etkilemekte ve dolaylı olarak dahi ceza muhakemesine gereklilik oluşturmayan kişileri içine almaktadır. Dolayısıyla, kişilerin davranışlarının ağır ceza gerektiren suçlarla dolaylı veya uzaktan bağlantısı olabileceğini varsaymak için hiçbir kanıt bulunmamasına rağmen mevzuat bu kişilere de uygulanmaktadır. Ayrıca hiçbir istisna getirmediği için iç hukuk uyarınca yazışmaları mesleki gizlilik arz eden kişilere de uygulanmaktadır (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı , 57'nci ve 58'inci paragraflar).

106. Bu mevzuata göre, saklanması gereken veriler ve kamu güvenliği tehdidi arasında bir ilişki olmasına gerek yoktur. Özellikle bu mevzuat, belli bir zamana ve/veya belli bir coğrafi bölgeye ait olan ve/veya bir şekilde ağır bir suça karışmış olan bir grupla ilgili verilerin (i) saklanmasıyla sınırlı değildir. Ayrıca mevzuat, saklanan veriler yoluyla, diğer sebeplerle suçla mücadeleye katkıda bulunan kişilerin verileriyle de (ii) sınırlı değildir (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 59'uncu paragraf).

107. Dolayısıyla, asıl davada geçen ulusal mevzuat, Şart'ın 7'nci, 8'inci, 11'inci maddesi ve 52'nci maddesinin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı uyarınca, kesin surette gerekli olan sınırların dışına çıkmaktadır ve demokratik bir toplumda haklı gösterilemez.

108. Ancak, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı Şart'ın 52'nci maddesi birinci paragrafı ve 7'nci, 8'inci ve 11'inci maddeleri dikkate alınarak okunduğunda, bir Üye Devletin, önleyici bir tedbir olarak, ağır suçla mücadele amacıyla, hedeflenen trafik ve konum verilerini saklamayı öngören mevzuatı kabul etmesini engellemez. Saklanacak verinin kategorileri, kullanılan iletişim aracı, ilgili kişiler ve kabul edilmiş veri saklama süresi açısından veri saklama işleminin kesinlikle gereklilik arz etmesi şartı vardır.

109. Mevcut kararın önceki paragrafında belirtilen gereklilikleri yerine getirmek amacıyla, ulusal mevzuat ilk olarak bu tür bir veri saklama tedbirinin kapsamı ve uygulanmasını düzenleyen açık ve kesin kurallar koymalıdır ve bu kurallar asgari düzeyde teminatlar oluşturarak verileri saklanan kişilere bu verilerin kötüye kullanılmasına karşı etkili koruma oluşturacak yeterli garanti vermelidir. Bu mevzuat, özellikle, veri saklama tedbirinin, hangi durumlarda ve hangi şartlar alında önleyici tedbir olarak kabul edilebileceğini belirtmeli ve bu tedbirin kesin surette gereklilik arz etmesini sağlamalıdır (kıyaslayarak bkz, 2006/24 sayılı Direktife ilişkin, *Dijital Haklar* kararı, 54'üncü paragraf ve belirtilen içtihat).

110. İkinci olarak, suçla mücadele bağlamında, önleyici bir tedbir olarak trafik ve konum verilerini saklama yetkisi veren ulusal mevzuatın yerine getirmesi gereken maddi hukuk şartları hususunda, veri saklamanın kesin surette gerekli olan hususların sınırlarını aşmamasını sağlamak gerekecekse, yukarıda belirtilen şartlar ağır suçu önleme, soruşturma, tespit etme ve kovuşturma amaçları doğrultusunda alınan önlemlerin niteliğine göre değişiklik gösterirken, verilerin saklanması nesnel ölçütlere uymaya devam

etmelidir ki bu da saklanması gereken veriler ve takip edilen hedef arasında bir bağlantı kurmaktadır. Özellikle, bu şartların pratikte tedbirin kapsamını ve böylelikle etkilenen halkı sınırlaması için getirildiğinin ortaya konulması gereklidir.

111. Bu tür bir tedbire halk açısından sınırlama getirilmesi ve muhtemelen bundan etkilenecek durumlar hususunda, ulusal mevzuat, ağır ceza gerektiren suçlarla dolaylı da olsa bağlantısı olabilecek kişiyi tespit etmeye yarayan ve bir şekilde, ağır suçla mücadeleye veya kamu güvenliğine karşı ciddi bir tehlikeyi önlemeye imkan veren tarafsız bir kanıta dayanmalıdır. Yetkili ulusal makamın tarafsız bir delile dayanarak bir veya birden çok coğrafi bölgede söz konusu eylemlerin hazırlığının yapılma veya yürütülme riskinin yüksek olduğunu düşündüğü yerlerde bu sınırlamalar konabilir.

112. Yukarıda bahsedilenler dikkate alındığında, C-203/15 sayılı davanın ilk sorusunun cevabı şu şekilde yorumlanmalıdır: Şart'ın 7'nci, 8'inci, 11'inci maddelerinin ve 52'nci maddenin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı, suçla mücadele etmek amacıyla, tüm katılımcı ve kayıtlı kullanıcıların elektronik iletişim araçlarıyla ilgili tüm trafik ve konum verilerinin genel ve ayrımsız bir şekilde saklanmasını öngören ulusal mevzuatı engellemektedir.

C-203/15 sayılı davanın ikinci sorusu ve C-698/15 sayılı davanın birinci sorusu

113. Öncelikle dikkat edilmesi gereken nokta şudur: Kammarrätten i Stockholm (İdari Temyiz Mahkemesi, Stokholm) sadece o davanın birinci sorusuna verilen cevabın olumsuz olması ihtimaline karşı C-203/15 sayılı Dava'da ikinci soruyu sormuştur. Ancak, bu kararın 108-111'inci paragraflarında belirtildiği gibi, ikinci soru veri saklamanın genelleştirilmesi veya hedeflenmesinden bağımsız olarak ortaya çıkmaktadır. Bu nedenle mahkeme C-203/15 sayılı Dava'nın ikinci sorusuyla, elektronik iletişim hizmeti sağlayıcılarına yüklenen veri saklama yükümlülüğünün kapsamından bağımsız olarak sorulan birinci soruyu (C-698/15 sayılı dava) birlikte cevaplandırmalıdır.

114. C-203/15 sayılı davanın ikinci sorusunu ve C-698/15 sayılı davanın birinci sorusunu soran sevk eden mahkemeler, suçla mücadele bağlamında veriye erişim amacının ağır suçla mücadeleyle sınırlı olmadığı, erişimin bir mahkeme veya bağımsız bir idari makamın ön denetimine tabi olmadığı ve ilgili verinin Avrupa Birliği içerisinde saklanmasının zorunlu olmadığı hallerde; Şart'ın 7'nci, 8'inci maddelerinin ve 52'nci maddesinin birinci fıkrası dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafının, özünde, trafik ve konum verilerinin korunmasını ve güvenliğini, özellikle yetkili ulusal makamların saklanmış verilere erişimini düzenleyen ulusal mevzuatı engelleyip engellemediğini tespit etmeye çalışmaktadır.

115. Elektronik iletişimin gizliliği ilkesine istisna teşkil eden ulusal mevzuatı gerekçelendirebilen hedefler hususunda, bu kararın 90'ıncı ve 102'nci paragraflarında belirtildiği gibi 2002/58 sayılı Direktifin 15'inci maddesinin birinci paragrafının birinci cümlesinde açıklanan hedefler listesinin geniş kapsamlı olması nedeniyle, saklanmış veriye erişim gerçekçi bir şekilde ve kesin surette bu hedeflerden biriyle uyumlu olmalıdır. Ayrıca, bu mevzuat tarafından hedeflenenin, erişim nedeniyle temel haklara yapılan müdahalenin ciddiyeti ile orantılı olması gerektiği için, ceza gerektiren suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması hususunda sadece ağır suçla mücadele şeklindeki hedef saklanmış veriye erişimi gerekçelendirebilmektedir.

116. Orantılılık ilkesiyle uyum değerlendirildiğinde, elektronik iletişim hizmetleri sağlayıcılarının ulusal makamlara saklı veriye erişim verirken uyulması gereken şartları düzenleyen ulusal mevzuat, bu kararın 95'inci ve 96'ncı paragraflarında belirtilenler

uyarınca, bu tür bir erişimin kesin surette gerekli olan hususların sınırlarını aşmamasını sağlamalıdır.

117. Buna ilaveten, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafında atıfta bulunulan yasama tedbirlerinin, direktifin 11'inci gerekçesi uyarınca 'yeterli sayıda teminata tabi olması' gerektiğinden, bu kararın 109'uncu paragrafında yazılı içtihat uyarınca veri saklama tedbiri, elektronik iletişim hizmeti sağlayıcılarının hangi durumlarda ve şartlar altında yetkili ulusal makamlara erişim izni vermesi gerektiğini açıklayan açık ve kesin kurallar düzenlemelidir. Aynı şekilde, bu türden bir tedbir hukuken iç hukuk içerisinde bağlayıcı olmalıdır.

118. Yetkili ulusal makamların saklanmış verilere erişimini kesin surette gerekli olan hususlarla sınırlamak için, ulusal hukuk elektronik iletişim hizmeti sağlayıcılarının hangi şartlar altında erişim izni vermesi gerektiğini belirlemelidir. Ancak, ilgili ulusal mevzuat, bu erişimin 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafında atıfta bulunulan hedeflerden birini içermesini öngörmekle sınırlanamaz. Ulusal mevzuat, yetkili ulusal makamların saklanmış verilere erişimini belirleyen maddi ve usuli şartları da düzenlemelidir (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin olarak, *Dijital Haklar* kararı, 61'inci paragraf).

119. Aynı şekilde, amaçlanan hedefle dolaylı da olsa herhangi bir bağının olmasına bakılmaksızın, saklanmış olan tüm verilere genel bir erişim olması kesin surette gerekli hususların sınırları içinde kalındığını göstermediğinden dolayı, ilgili ulusal mevzuat yetkili ulusal makamların hangi durumlar ve şartlar altında katılımcı veya kayıtlı kullanıcı verilerine erişebileceğini belirlemek için nesnel ölçütlere dayanmalıdır. Bu bağlamda, genel bir kural olarak, suçla mücadeleyle ilgili olmak suretiyle, sadece ağır bir suç planladığından, işlemekte olduğundan veya işlediğinden ya da bu türden bir suça bir şekilde karıştığından şüphelenilen kişilerin verilerine erişim izni verilebilir. (kıyaslayarak bkz, AİHM, 4 Aralık 2015, *Zakharov/Russia*, CE:AİHS:2015:1204JUD004714306, § 260). Ancak milli güvenlik, milli savunma veya kamu güvenliği menfaatlerinin büyük ölçüde terör eylemi tehdidi altında olması gibi özel durumlarda, verilerin bu gibi eylemlerle mücadelede etkili bir katkı sağlayacağını öne süren nesnel kanıtların varlığı halinde, diğer kişilerin verilerine de erişim sağlanabilir.

120. Bu şartlara uygulama aşamasında bütünüyle saygı duyulmasını sağlamak için yetkili ulusal makamların saklanmış verilere erişiminin, genel bir kural olarak, geçerli bir aciliyet hali dışında, bir mahkeme veya bağımsız idari bir organ tarafından bir ön denetime tabi olması gereklidir. İlaveten o mahkeme veya organ yetkili ulusal makamların, suçun önlenmesi, tespiti veya kovuşturulması usulleri çerçevesinde, diğer hususlarla birlikte sunulan gerekçeli talebi üzerine karar vermelidir (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, Dijital Haklar kararı, 62'nci paragraf; ayrıca kıyaslayarak bkz, AİHS'nin 8'inci maddesine ilişkin, AİHM, 12 Ocak 2016, Szabó ve Vissy/ Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 ve 80).

121. Aynı şekilde, yetkili ulusal makamların saklanmış veriye erişim hakkı aldığını etkilenen kişilere bildirmesinin makamların yürüttüğü soruşturmaları tehlikeye atmayacağı anlaşıldığı anda, etkilenen kişiler uygulanabilir ulusal usuller uyarınca bu konuda bilgilendirilir. Bu bildiri aslında etkilenen kişilerin hakları ihlal edildiğinde, diğer hususlarla birlikte 95/46 sayılı Direktif'in 22'nci maddesi dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin ikinci paragrafında açıkça öngörüldüğü gibi, hukuk yoluna başvurma hakkını kullanabilmesini sağlamak adına gereklidir (kıyaslayarak bkz, 7 Mayıs 2009 tarihli, *Rijkeboer kararı*, C-553/07, EU:C:2009:293, 52'nci paragraf, ve 6 Ekim 2015, *Schrems kararı*, C-362/14, EU:C:2015:650, 95'inci paragraf).

122. Elektronik iletişim hizmetleri sağlayıcıları tarafından saklanan verilerin güvenliği ve korumasına ilişkin kurallar hususunda, 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı, Üye Devletlerin bu direktifin 4'üncü maddesinin birinci paragrafına ve 1a paragrafına istisna getirmesine izin vermemektedir. Bu hükümler saklı verilerin kötüye kullanım tehlikesine ve her tür yasa dışı erişime karşı etkili bir şekilde korunmasını sağlamak için sağlayıcıların uygun teknik ve örgütsel önlemler almalarını gerektirmektedir. Saklı verilerin miktarı, hassasiyeti ve yasadışı erişim riski dikkate alındığında, verilerin tam bütünlüğünü ve gizliliğini sağlamak için elektronik iletişim hizmetleri sağlayıcıları uygun teknik ve örgütsel tedbirler yoluyla oldukça yüksek bir koruma ve güvenliği garantilemelidir.Özellikle, ulusal mevzuat saklanmış verilerin Avrupa Birliği içine kalmasını ve veri saklama süreci sona erdiğinde geri çevrilmez bir şekilde bu verilerin ortadan kalkmasını sağlamalıdır (kıyaslayarak bkz, 2006/24 sayılı Direktif'e ilişkin, *Dijital Haklar* kararı, 66-68 arasındaki paragraflar).

123. Her durumda, Üye Devletler kişisel verilerin işlenmesi ile ilgili olarak kişilerin korunmasının AB hukukunda garantilenen koruma seviyesiyle uyumunu bağımsız bir makamın denetlemesini sağlamalıdır. Bu kontrol Şart'ın 8'inci maddesinin üçüncü paragrafı tarafından açıkça gerekli görülmektedir ve Mahkeme'nin yerleşik içtihadı uyarınca kişisel verilerin saklanması alanında kişilerin korunmasına saygının temel bir unsurunu oluşturmaktadır. Durum böyle olmasaydı verileri saklanan kişiler Şart'ın 8'inci maddesinin birinci ve üçüncü paragrafında garantilendiği gibi ulusal denetim makamları önünde verilerinin korunmasını talep etme hakkından yoksun kalırdı (bkz, bu hususta, Dijital Haklar kararı, 68'inci paragraf, ve 6 Ekim 2015 tarihli karar, Schrems, C 362/14, EU:C:2015:650, 41-58 arasındaki paragraflar).

124. Bu kararın 115-123 arasındaki paragraflarında açıklandığı gibi, Şart'ın 7'nci, 8'inci ve 11'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafından kaynaklanan yetkili ulusal makamların saklı verilere erişimi ile verilerin güvenliği ve koruma seviyesi hakkındaki yükümlülüklerin asıl davada söz konusu ulusal mevzuat tarafından yerine getirilip getirilmediğini ve bu yükümlülüklerin ne kadarının yerine getirildiğini belirlemek sevk eden mahkemelerin görevidir.

125. Yukarıdakiler göz önüne alındığında, C-203/15 sayılı Dava'nın ikinci sorusuna ve C-698/15 sayılı Dava'nın birinci sorusuna verilecek yanıt şudur: Suçla mücadele bağlamında veriye erişim amacının ağır suçla mücadeleyle sınırlı olmadığı, erişimin bir mahkeme veya bağımsız bir idari makamın ön denetimine tabi olmadığı ve ilgili verinin Avrupa Birliği içerisinde saklanmasının zorunlu olmadığı hallerde; Şart'ın 7'nci, 8'inci ve 11'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı, trafik ve konum verilerinin korunmasını ve güvenliğini, özellikle de yetkili ulusal makamların saklı veriye erişimini düzenleyen ulusal mevzuatı engellediği şeklinde yorumlanmalıdır.

C-698/15 sayılı Dava'nın ikinci sorusu

126. C-698/15 sayılı Dava'nın ikinci sorusuyla Temyiz Mahkemesi'nin (İngiltere & Galler) (Hukuk Birimi) aslında açıklığa kavuşturmak istediği konu *Dijital Haklar* kararında Mahkeme'nin Şart'ın 7'nci ve/veya 8'inci maddelerini AİHS'nin 8'inci maddesine AİHM tarafından verilen kapsamı genişletmek üzere yorumlayıp yorumlamadığıdır.

127. Öncelikle, ABA'nın 6'ncı maddesinin üçüncü paragrafı, AİHS'nin tanıdığı temel hakların AB hukukunun genel esaslarını oluşturduğunu kabul ederken; AİHS'nin Avrupa Birliği kabul etmediği sürece AB hukuku bünyesinde resmi olarak yer alan yasal bir belge olmadığını hatırlamak gereklidir (bkz,bu konuya ilişkin, 15 Şubat 2016 tarihli karar, *N.*, C-601/15 PPU, EU:C:2016:84, 45 'inci paragraf ve söz konusu içtihat).

128. Aynı şekilde, bu davada bahsi geçen 2002/58 sayılı Direktif' yalnızca Şart'ın garantilediği temel haklar ışığında yorumlanmalıdır (bkz, bu konuya ilişkin, 15 Şubat 2016 tarihli karar, *N.*, C-601/15 PPU, EU:C:2016:84, 46'ncı paragraf ve söz konusu içtihat).

129. Buna ilaveten, Şart'ın 52'nci maddesindeki açıklama, bu maddenin üçüncü paragrafının Şart ve AİHS arasında gerekli olan tutarlılığı 'Birlik hukukunun ve Avrupa Birliği Adalet Divanı'nın özerkliğini olumsuz etkilemeden' sağlamayı amaçladığını ifade etmektedir (15 Şubat 2016 kararı, *N.*, C-601/15 PPU, EU:C:2016:84, 47'nci paragraf). Özellikle Şart'ın 52'nci maddesinin üçüncü paragrafının ikinci cümlesinde açıkça belirtildiği gibi, 52'nci maddenin üçüncü paragrafının birinci cümlesi Birlik Hukukunun AİHS'den daha kapsamlı bir koruma sağlamasına engel olmamaktadır. Son olarak, Şart'ın 8'inci maddesi Şart'ın 7'nci maddesindekinden tamamen farklı olan bir temel hakla ilgilidir ve AİHS'de bir eşdeğeri yoktur.

130. Ancak Mahkeme'nin yerleşik içtihadı uyarınca, ön karar başvurusunun yapılma nedeni genel veya varsayımsal sorularla ilgili tavsiye niteliğinde görüşlerin paylaşılması değil AB hukukunu ilgilendiren bir uyuşmazlığın etkili bir şekilde çözülmesini sağlamaktır (bkz, buna ilişkin, 24 Nisan 2012 tarihli karar, *Kamberaj*, C-571/10, EU:C:2012:233, 41'inci paragraf; 26 Şubat 2013 tarihli karar, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, 42'nci paragraf, ve 27 Şubat 2014 tarihli karar, *Pohotovosť*, C-470/12, EU:C:2014:101 29'uncu paragraf).

131. Bu davada özellikle mevcut kararın 128'inci ve 129'uncu paragraflarındaki hususlar ışığında, Şart'ın 7'nci ve 8'inci maddelerinin verdiği korumanın AİHS 8'inci maddesinde garantilenen hususlardan daha geniş olup olmadığı sorusu, C-698/15 sayılı Dava'daki uyuşmazlığın nedenini oluşturan 2002/58 sayılı Direktif'in Şart'ı dikkate alarak yorumlanmasını etkileyecek ölçüde değildir.

132. Dolayısıyla, C-698/15 sayılı Dava'daki ikinci soruya verilecek cevabın, uyuşmazlığın ilgili kanun dikkate alınarak çözümü için gerekli AB hukuku noktalarının yorumlanmasını sağlamadığı görülmektedir.

133. Bu açıklamaya dayanılarak C-698/15 sayılı Dava'daki ikinci soru kabul edilemez.

Harcamalar

134. Asıl davanın tarafları için bu dava işlemleri ulusal mahkemeler önündeki derdest işlemlerin bir bölümü olduğundan harcamalar konusunu da bu mahkemeler değerlendirir. Tarafların harcamaları dışında Mahkeme'ye görüş sunulurken yapılan harcamalar geri alınamaz.

Bu gerekçelerle, Mahkeme (Büyük Daire) aşağıdaki hükmü verir:

1. **2009/136/EC sayılı 25 Kasım 2009 tarihli Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi ile değişik Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 2002/58/EC sayılı 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'nin (Mahremiyet ve elektronik iletişime ilişkin Direktif) 15'inci maddesinin birinci paragrafı; Avrupa Birliği Temel Haklar Şartı'nın 7'nci, 8'inci, 11'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak, tüm katılımcı ve kayıtlı kullanıcıların bütün elektronik iletişim araçlarıyla ilgili trafik ve konum verilerini, suçla mücadele amacıyla, genel ve ayrımcı bir şekilde saklamayı öngören ulusal mevzuatı engellediği şeklinde yorumlanmalıdır.**

2. **2009/136 sayılı Direktif'le değişik ve Temel Haklar Şartı'nın 7'nci, 8'inci ve 11'inci maddeleri ve 52'nci maddesinin birinci paragrafı dikkate alınarak okunan 2002/58 sayılı Direktif'in 15'inci maddesinin birinci paragrafı; suçla mücadele bağlamında veriye erişim amacının ağır suçla mücadeleyle sınırlı olmadığı, erişimin bir mahkeme veya bağımsız bir idari makamın ön denetimine tabi olmadığı ve ilgili verinin Avrupa Birliği içerisinde saklanmasının zorunlu olmadığı hallerde; trafik ve konum verilerinin korunmasını ve güvenliğini, özellikle de yetkili ulusal makamların saklı verilere erişmesini düzenleyen ulusal mevzuatı engellediği şeklinde yorumlanmalıdır.**
3. **Temyiz Mahkemesi'nin (İngiltere & Galler) (Hukuk Birimi) yönelttiği ikinci soru kabul edilemez.**

Lenaerts	Tizzano	Silva de Lapuerta
von Danwitz	Da Cruz Vilaça	Juhász
Vilaras	Borg Barthet	Malenovský
Levits	Bonichot	Arabadjiev
Rodin	Biltgen	Lycourgos

Karar 21 Aralık 2016 tarihinde Lüksemburg'da açık celsede verilmiştir.

A. Calot Escobar K. Lenaerts

Kayıt Memuru Başkan

(*) Dava İngilizce ve İsveççe dillerinde yazılmıştır.