



ÇAMURŞEN/TÜRKİYE KARARI: İNTERNET TRAFİK VERİLERİNİN SAKLANMASI VE SİSTEMATİK HAK İHLALLERİ

Dr. Ufuk YEŞİL



HAKKIMIZDA

Hollanda merkezli kurulan Justice Square Stichting, temel insan hakları ve yaşanan hak ihlalleri konularında farkındalık oluřturmak ve bu alanda m¼cadele etmek amaçlı kurulmuř bir sivil toplum kuruluřudur.

www.justicesquare.org

HAKKIMIZDA	2
ÖNSÖZ	5
Genel Olarak	6
1. İnternet Trafik Bilgilerinin ve HTS Kayıtlarının Saklanması ve İmhasına İlişkin Mevzuat	6
a) Türkiye Cumhuriyeti Anayasası	7
b) 6698 Sayılı Kişisel Verilerin Korunması Kanunu	7
c) 5809 Sayılı Elektronik Haberleşme Kanunu ve Bu Kanuna Dayanılarak Çıkarılan Yönetmelikler	10
d) Saklama Süresi ve Silme Yükümlülüğü Açısından	11
e) Bilgi Teknolojileri ve İletişim Kurumunun Yetkileri Açısından	14
f) 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve Bu Kanuna Dayanılarak Çıkarılan Yönetmelikler	17
g) 5237 sayılı Türk Ceza Kanunu	19
h) 5271 sayılı Ceza Muhakemesi Kanunu ve Bu Kanuna Dayanılarak Çıkarılan Yönetmelikler	20
2. HTS Kayıtları ve İnternet Trafik Bilgilerinin Kimin Tarafından Saklandığı Sorunsalı	22
a) Saklama Süresi Dolan Veriler Kimin Tarafından Saklandığı Hususunun Değerlendirilmesi	22
b) BTK'nın Veri Saklama Yetkisinin Değerlendirilmesi	25
c) Bilgi Teknolojileri ve İletişim Kurumunun Denetim Yükümlülüğü	32
3. Saklama Süresi Dolan Verilerin Delil Niteliği	34
4. Avrupa İnsan Hakları Mahkemesi'nin Konuya Yaklaşımı	36
a) Rotaru/Romanya Büyük Daire Kararı	36
b) Big Brother Watch ve Diğerleri/Birleşik Krallık Kararı	37
c) Benedik/Slovenya Kararı	37
d) Ekimdzhiev ve Diğerleri/Bulgaristan Kararı	38
e) Škoberne/Slovenya Kararı	39
f) Borislav Tonchev/Bulgaristan Kararı	40
g) Yalçınkaya/Türkiye Kararı	41
5. Çamurşen/Türkiye Kararı	42
a) Anayasa Mahkemesi'nin Ertan Erçiktı (3) Kararı	42

b) Çamurşen/Türkiye Kararı	44
c) Karara İlişkin Değerlendirme	45
d) Tazminat Yolunun Etkin Olduğu Yönündeki Tespitlere İlişkin	46
e) Çamurşen Başvurusundan Ayrılan Dosyayla İlgili AİHM'in Tavrı Ne Olacaktır? ..	57
f) AİHM Hangi Madde(ler) Kapsamında İnceleme Yapacak ve Karar Verecektir?	66

ÖNSÖZ

Bilişim teknolojilerindeki gelişmeler sonucunda geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi, daha önce birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezî olarak bir araya getirilebilmesi, verilerin veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle veriden yeni veriler üretme kapasitesinin artması, verilere erişim ve veri transferinin kolaylaşması, kişisel verilerin kıymetli bir varlık niteliği kazanması neticesinde özel sektör unsurlarınca oluşturulan risklerin daha yaygın ve önemli boyutlara ulaşması, terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır.

Belirtilen sebeplerle kişisel verilerin en üst seviyede korunması zorunlu olmakla birlikte bu hak mutlak ve sınırsız olmayıp Anayasa'nın 13. ve 20. maddeleri gereğince belirli koşullarda, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir. Anayasa'nın amir hükmü gereğince konuyla ilgili pek çok düzenleme yapılmıştır. Bu düzenlemelerden bazıları da kişisel veri niteliğindeki internet trafik verileri ve HTS kayıtlarının saklanması ve imhasına ilişkindir ve kanun ve yönetmeliklerde bu veri ve kayıtların saklanma ve imha prosedürleri ile denetim mekanizmalarına yer verilmiştir.

Ancak, tüm bunlara rağmen bilişim teknolojileri sektörünün düzenleyici ve denetleyici kurumu olan Bilgi Teknolojileri ve İletişim Kurumu (BTK), kendisine verilmiş bir yetki olamamasına ve bu konuda verilmiş mahkeme kararları bulunmamasına rağmen, internet trafik verilerini ve HTS kayıtlarını işletmecilerden istemekte, yıllarca saklamakta ve saklamaya devam etmektedir. Saklanma süresi geçmiş kayıtları mahkemelerin istemesi üzerine de bu kayıtları göndermiş ve hukuka aykırı hale gelen bu delillerle insanlar cezalandırılmıştır

Çalışmada, internet verileri ve HTS kayıtlarının saklanma usulüne ve konuyla ilgili Anayasa Mahkemesi tarafından verilen Ertan Erçıktı (3) ve bu karara atıfla AİHM'in verdiği Çamurşen/Türkiye kararının değerlendirmesine yer verilmiştir.

Stichting Justice Square bünyesinde hazırlanan bu çalışmanın faydalı olmasını dileriz.

19 Aralık 2024

Amsterdam

ÇAMURŞEN/TÜRKİYE KARARI: İNTERNET TRAFİK VERİLERİNİN SAKLANMASI VE SİSTEMATİK HAK İHLALLERİ

Genel Olarak

Elektronik ortamda işlenen suçların aydınlatılmasında internet bağlantısıyla ilgili kişi, yer ve zaman bilgisinin tespiti çok önemlidir. Bu tespitin yapılabilmesi için; kişilere tahsis edilen IP adresi, internet üzerinden sunulan hizmetin başlangıç ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve abone bilgilerine, diğer bir ifadeyle internet “*trafik bilgileri*” ne ihtiyaç vardır. Trafik bilgisi, bir internet kullanıcısının özel hayatı ile ilgili birçok detayı, kişisel tercihlerini, politik eğilimlerini, sağlık bilgilerini, ticari sırlarını ifşa edebilecek nitelikte kritik bilgiler içeren veri türüdür. Bu nedenle, trafik bilgileri ile bir kişinin hayatıyla ilgili neredeyse her detayın kolayca tespiti mümkündür. Dolayısıyla trafik bilgisinin kapsamına kişisel veriler de girer. Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri içerir. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlar. Ancak, söz konusu hak sınırsız değildir. Kişisel verilerin korunması hakkı veri sahibinin mutlak ve sınırsız bir veri hâkimiyetini mümkün kılmaz.

1. İnternet Trafik Bilgilerinin ve HTS Kayıtlarının Saklanması ve İmhasına İlişkin Mevzuat

Konu ile ilgili düzenlemeler genel olarak, Türkiye Cumhuriyeti Anayasası, 5809 sayılı Elektronik Haberleşme Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5237 sayılı Türk Ceza Kanunu (TCK), 5271 sayılı Ceza Muhakemesi Kanunu’nda (CMK) ve bu kanunlara dayanılarak çıkartılan yönetmelikle ile yapılmıştır.

a) Türkiye Cumhuriyeti Anayasası

Anayasa ile özel hayatın gizliliği güvence altına alınmış olup, herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz (Anayasa md. 20/1). Bunun yanı sıra; kişisel veriler için ayrı bir hüküm ile de güvence altına alınmıştır. Buna göre; herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir (Anayasa md. 20/3).

Anayasa ile deliller hakkında da bir güvence tanımlanmıştır. Bu düzenleye göre Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez (Anayasa md 38/6).

Yukarıda yer verilen iki düzenleme birlikte değerlendirildiğinde; kişisel veriler, ancak ve ancak kanunun öngördüğü hallerde veya kişinin açık rızasıyla işlenebilir ve hukuka aykırı olarak işlenen kişisel verilerin delil olarak kabul edilemez.

b) 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek (Kanun md. 1), kanunun kapsamı ise, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik ya da otomatik olmayan yollarla işleyen gerçek ve tüzel kişilerdir (Kanun md. 2).

Kişisel veri; *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde (Kanun md. 3/1-d), özel nitelikteki kişisel veri; *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler"* şeklinde (Kanun md. 6/1), kişisel verilerin işlenmesi ise; *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da*

kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem” şeklinde (Kanun md. 3/1-e) tanımlanmıştır.

Kanunun amacı ve kapsamı ile kanunda yer verilen kişisel veri ve kişisel verilerin işlenmesi tanımları hep birlikte değerlendirildiğinde; bir kişinin kimlerle, hangi sıklıkla, ne kadar konuştuğu, hangi internet sitelerine hangi sıklıkla girdiği gibi hususları ihtiva eden, bu bağlamda kullanıcısının özel hayatı ile ilgili birçok detayı, kişisel tercihlerini, politik eğilimlerini, sağlık bilgilerini, ticari sırlarını ifşa edebilecek nitelikte kritik bilgiler içeren trafik bilgilerinin kişisel veri niteliğinde olduğunda herhangi bir tereddüt bulunmamaktadır.

Kişisel veriler, ilgili kişinin açık rızası olmaksızın işlenemezler (Kanun md. 5/1). Kanunda yer verilen tanımdan da anlaşılacağı üzere, kaydetmek, depolamak, muhafaza etmek ve aktarmak da “işleme” kapsamındadır. Kişisel veriler, kanunda belirtilen şartları taşıdığı sürece işlenebilirler. Söz konusu şartlar kanunda aşağıdaki şekilde düzenlenmiştir (Kanun md. 5/2);

“a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

Yukarıda yer verilen düzenlemede yer alan “Kanunlarda açıkça öngörülmesi” şartında geçen “açıkça” ifadesi, büyük önem arz etmektedir. Nitekim, açık bir şekilde belirtilmeyen bir kanun metnine dayanılarak kişisel verilerin işlenebilmesi mümkün değildir.

İşlenen kişisel veriler, kanunda yer alan; “Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya

anonim hâle getirilir.” şeklindeki (Kanun md. 7/1) bir düzenleme ile koruma altına alınmıştır. Bu düzenlemeye göre hangi kanun gereğince işlenmiş olursa olsun, işlenmesini gerektiren sebeplerin ortadan kalkması halinde, işlenen kişisel veriler silinmeli, yok edilmeli veya anonim hale getirilmelidir. Düzenlemede geçem *“anonim hale getirme”* deyimini, kanunda *“kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi”* şeklinde (Kanun md. 3/1-b) düzenlenmiştir.

Kanunun uygulama esaslarının belirlenmesine yönelik çıkartılan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik¹ (*Silme Yönetmeliği*) ile imha; *“kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi”* şeklinde (Silme Yönetmeliği md 4/1-c), periyodik imha; *“kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi”* şeklinde (Silme Yönetmeliği md 4/1-ğ) tanımlanmıştır.

Silme Yönetmeliğine göre; kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir (Silme Yönetmeliği md. 10/1). Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir. Bu süre her halde 6 ayı geçemez. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir (Silme Yönetmeliği md. 11). Bu yükümlülüğü ihlal edenler, 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır (Kanun md. 17/2)

Sonuç olarak; kişisel veri niteliğinde olan HTS kayıtları ve internet trafik bilgileri, ancak Kanunda sayılan nedenlerle kaydedilebilir, saklanabilir, muhafaza edilebilir ve aktarılabilir. Söz konusu kanunda yer verilen sebeplerden olan *“kanunlarda açıkça öngörülmesi”* sebebi gereğince bu kişisel verilerin kaydedilmesi için, kanun lafzında vurgulandığı üzere, kanunda *“açıkça”* öngörülmesi şarttır. Bu bağlamda, kanunlarda geçen *“gibi bilgiler”, “her türlü bilgi”*

1 29/10/2017 tarihli ve 30224 sayılı Resmi Gazete

gibi muğlak ve belirli olmayan ifadeler, “açıkça öngörölme” koşulunu sağlamamaktadır. Bu nedenle, kanunlarda geçen kesin olmayan muğlak ifadeler kapsamında kişisel veri niteliğindeki bilgilerin işlenmesi hukuken mümkün değildir. Kanunda açık bir şekilde öngörülerek işlenen kişisel veriler dahi, yine kanunda öngörülen sebeplerin ortadan kalkması (saklama süresinin dolması gibi) durumunda, talep halinde veya her halde resen veri sorumlusu tarafından silinmesi gerekmektedir. Bu yükümlülüğün ihlali halinde, ihlali gerçekleştiren kişi, 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

c) 5809 Sayılı Elektronik Haberleşme Kanunu ve Bu Kanuna Dayanılarak Çıkarılan Yönetmelikler

Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir. Dolayısıyla, 5809 sayılı Kanun, elektronik haberleşme sistemlerinin uluslararası normlara uygun olması, bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, kişisel veri ve gizliliğin korunması, kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak ve izinsiz erişime karşı şebeke güvenliğinin sağlanması hususlarında tüketiciyi önce devlete, sonra da üçüncü kişilere karşı korumaktadır.

Kanunda; iletişim hizmeti veren işletmeci ile hizmet alan kullanıcı arasındaki sözleşmeye uygun olarak haberleşme hizmetinin sağlanması, korunması ve devamına ilişkin düzenlemelere yer verilmiştir.

5809 sayılı Elektronik Haberleşme Kanunu (md. 3/1-h) ile bu Kanun’a dayanılarak çıkarılan Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği² (*Yetkilendirme Yönetmeliği*) ve Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelikte³ (*Gizliliğin Korunması Yönetmeliği*) elektronik haberleşme kavramı; “elektiriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo,

2 28/5/2009 tarihli ve 27241 sayılı Resmi Gazete.

3 4/12/2020 tarihli ve 31324 sayılı Resmi Gazete.

telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması" şeklinde (Yetkilendirme Yönetmeliği md. 4/1-g), kullanıcılarına elektronik haberleşme hizmeti sunan veya elektronik haberleşme şebekesi sağlayıp alt yapısını işleten GSM firmaları ve bu şekilde yetkilendirilen şirketler "işletmeci" (Kanun md. 3/1-z, Yetkilendirme Yönetmeliği md. 4/1-o, Gizliliğin Korunması Yönetmeliği md. 4/1-d) ve aboneliği olup olmadığına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek ve tüzel kişi de "kullanıcı" (Kanun md. 3/1-cc, Yetkilendirme Yönetmeliği md. 4/1-s, Gizliliğin Korunması Yönetmeliği md. 4/1-ı) olarak tanımlanmıştır.

d) Saklama Süresi ve Silme Yükümlülüğü Açısından

Kanunda, veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere, verilerin yönetmelikle belirlenecek süre boyunca saklanacağı düzenlenmiştir (Kanun md. 51/10-c).

Kanunda bahsedilen "veri kategorileri" deyimini tanımlı ne kanunda ve ne de bu kanun kapsamında çıkartılan yönetmeliklerde bulunmamaktadır. Veri kategorileri, Gizliliğin Korunması Yönetmeliği ile yürürlükten kaldırılmış olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik⁴ ile düzenlenmiş olup, haberleşmenin sonlandırılacağı nokta,⁵ haberleşmenin türü⁶ ve haberleşmenin tarihi,

4 24/7/2012 tarihli ve 28363 sayılı Resmi Gazete

5 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin sonlandırıldığı/sonlandırılacağı numara veya numaralar, çağrı iletilme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi.

2) Elektronik posta ve internet telefonu ile ilgili olarak; elektronik posta alıcılarına ait kullanıcı kimliği, internet telefonu ile aranan alıcılara ait kullanıcı kimliği veya telefon numarası, internet telefonu veya elektronik posta alıcılarının adı ve adresi.

6 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; kullanılan elektronik haberleşme hizmeti. 2) Elektronik posta ve internet telefonu ile ilgili olarak; kullanılan internet hizmeti.

zamanı ve süresi⁷ ile haberleşmenin takibi ve kaynağı⁸ gibi hususların tanımlarına yer verilmiştir (Yürürlükten Kaldırılmış Gizliliğin Korunması Yönetmeliği md. 13/1).

Mülga olan Gizliliğin Korunması Yönetmeliğinde; tanımlanan bu veri kategorilerinin, haberleşmenin yapıldığı tarihten itibaren en fazla bir yıl, gerçekleşmeyen aramalara ilişkin kayıtların ise üç ay süreyle saklanabileceği belirtilmiştir (Yürürlükten Kaldırılmış Gizliliğin Korunması Yönetmeliği md. 14/1). Yürürlükte olan Gizliliğin Korunması Yönetmeliğinde ise veri kategorilerinin tanımı yapılmadığı gibi, **saklama süresi ile ilgili herhangi bir düzenleme de bulunmamaktadır**. Bunun yerine, yönetmeliğin birçok yerinde 6698 sayılı Kişisel Verilerin Korunması Kanununun ilgili maddelerine atıf yapılmakla yetinilmiştir. Son durumda, kanunda geçen “veri kategorileri” deyimini ne kanunda ne de yönetmeliklerde tanımlanmaması ve birçok yerde 6698 sayılı Kanuna atıfta bulunulması nedeniyle, 5809 sayılı Kanunun 51/10-c maddesinde yer verilen “veri kategorileri” deyiminden, 6698 sayılı Kanununda yapılan kişisel veri ve özel nitelikli kişisel veri ayrımının anlaşılması gerektiği kanaatindeyiz.

Yetkilendirme Yönetmeliğinin ilk halinde, “Trafik bilgilerinin muhafaza edilmesi: Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, kullanıcı sayısı, kimlik bilgileri ve görüşme süreleri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini, bir yıl süreyle muhafaza etmekle yükümlüdür.” düzenlemesi yer almakta iken 11/6/2016 tarihinde yapılan değişiklikten sonra “Trafik bilgilerinin muhafaza edilmesi: Erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, taraflara ilişkin IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı, kullanıcı sayısı ve abone kimlik bilgileri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini iki yıl süreyle; kullanıcı bilgilerini ise ilgili mevzuatta belirtilen zamanaşımı süresi boyunca muhafaza etmekle yükümlüdür” düzenlemesi yer almaktadır

7 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin başlangıç ile bitiş tarih ve zamanı.

2) İnternet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; internet erişimi ile ilgili oturum açma, kapatma tarihi ve zamanı, tahsis edilen dinamik veya statik internet protokol adresi, NAT kullanılan şebekelerde internet protokol adresi yanında port bilgisi, abone/kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili oturum açma ile kapatma tarihi ve zamanı.

8 1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere haberleşmenin başlatıldığı hatta ait telefon numarası, abonenin adı ve adresi, hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgiyi.

2) İnternet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, abonenin/kullanıcının adı ve adresini” ifade eder.

(Yetkilendirme Yönetmeliği md. 19/1-f). Görüleceği üzere, trafik bilgilerinin iki yıl saklanması öngören süre, 11/06/2016 tarihinde yapılan değişiklik öncesinde bir yıldır ve değişikliğe kadar erişim sağlayıcılar ve işletmeciler sadece *“kullanıcı sayısı, kimlik bilgileri, görüşme süreleri ve altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini”* saklamakla yükümlüdürler. Başka bir ifadeyle, değişiklikle yönetmeliğe eklenen *“IP adresi, port aralığı, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü ve aktarılan veri miktarı”* erişim sağlayıcıları ve telefon hizmeti sunan işletmeciler tarafından saklanamaz.

Yönetmeliğin ilk halindeki *“görüşmelere ait trafik bilgilerinin”* kapsamına değişiklik sonrası eklenen hususlar dahil edilemez. Zira, ne 5809 sayılı Kanunda ne de bu kanuna dayanılarak çıkarılan yönetmelikte trafik bilgisinin tanımına yer verilmemiştir ve yönetmeliğe sonradan eklenen hususların değişikliktan önceki dönem için de ilgililer aleyhine uygulanması mümkün değildir.

5809 sayılı Kanun gereğince trafik verilerinin gizliliği esas olup, ilgili mevzuat, yargı kararları ve ilgililerin rızası dışında bu verilerin kaydedilmesi, saklanması, kesilmesi ve takibi yasaktır (md. 51/2). Trafik bilgileri, kişisel verilerin işlenmesi usulüne tabidir ve ancak öngörülen amaçla bağlantılı, sınırlı ve ölçülü şekilde işlenip, işlendikleri amaç için gerekli olan süre kadar saklanabilir ve bu süre Yönetmeliklerde öngörülenden fazla olamaz (md. 51/1).

5809 sayılı Kanuna göre, iletişim bilgilerini içeren özel bilgiler, izinsiz ve yetkisiz olarak muhafaza edilemez (md. 56/1) ve bu yükümlülüğe aykırı hareket edenler bin günden beş bin güne kadar adli para cezasıyla cezalandırılır (md. 63/10). Yine, 5809 sayılı Kanuna dayanılarak çıkarılan Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nin,⁹ *“Kişisel Verilerin Korunmasına İlişkin İhlaller”* başlığı altındaki 13. maddesinin 1/a-2 bendinde, işletmecinin abonelerine/kullanıcılarına ait işlenen ve saklanan trafik verilerin ilgili mevzuatta öngörülen sürede tutma veya silme yükümlülüğünü yerine getirmemesi halinde bir önceki takvim yılındaki net satışların %3'ne kadar idari para cezası uygulanacağı hükme bağlanmıştır.

Sonuç olarak; bu kanun kapsamında toplanan trafik bilgileri, 11/6/2016 tarihinden önceki tüm veriler için 1 yıl (gerçekleşmeyen aramalar bakımından 3 ay), bu tarihten sonraki

9 15/02/2014 tarihli ve 28914 sayılı Resmi Gazete.

tüm veriler için ise 2 yıldır. Mevzuat, bu süreler geçtikten sonra ilgili kişisel veri niteliğinde olan trafik bilgilerinin, bir talebe bağlı olmaksızın, veri sorumlusu tarafından resen silinmesini zorunlu kılmıştır. Bunun yanı sıra, saklama ve silme yükümlülüğünü ihmal edenlere yaptırım uygulanacağı açık bir şekilde belirtmiştir. Aynı şekilde, süreyi aşan şekilde verilerin işlenmesi ile işletmeler eliyle kişilerin özel hayatına kanuni dayanağı olmayan bir müdahale gerçekleşmekte olup devletin bu şekilde kişilerin haklarının ihlal edilmesini önleme pozitif yükümlülüğü bulunmaktadır.

e) Bilgi Teknolojileri ve İletişim Kurumunun Yetkileri Açısından

Bilgi Teknolojileri ve İletişim Kurumunun (BTK) birçok görev ve yetkisi olmakla birlikte, bu başlık altında sadece HTS ile internet trafik bilgileri, bunların saklanma ve silinmesi ve denetim yükümlülüğü değerlendirilecektir.

5809 sayılı Kanununun 6. maddesinde BTK'nın görev ve yetkileri düzenlenmiştir. Bunlardan biri de elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmektir (Kanun md. 6/1-1).

Kanunun lafzında her ne kadar *“kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak”* denilmişse de kanundan anlaşılması gereken bu değildir. Nitekim bu maddenin gerekçesinde; *“Bu Kanunla Kurumun; elektronik haberleşme sektörü ile ilgili şikâyetleri inceleme yetkisi açıklığa kavuşturulmakta, şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi için ilgililerden bilgi ve belge toplama yetkisi verilmektedir.”* denilmektedir¹⁰. Gerekçeden de anlaşılacağı üzere, Kanun Koyucu, bu madde ile BTK'ya *“şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi”* ile sınırlı olmak üzere bilgi-belge almak ve gerekli kayıtları tutma yetkisi vermiştir. **BTK'nın sınırsız bir şekilde, her türlü bilgi ve belge almak, istemek ve kaydetmek yetkisi bulunmamaktadır.** Bu madde ile tanımlanan yetkisi, şikâyetleri incelemek

10 <https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d23/c026/tbmm23026138ss0255.pdf>

ve işletmeleri denetlemek hususlarıyla sınırlı olup **kişisel veri niteliğindeki trafik bilgilerini kaydetme, saklama, depolama, arşivleme ve paylaşma görev ve yetkisi bulunmamaktadır.**

Konuyla alakalı bir diğer yetki, Kanunun 60. maddesine 15/8/2016 tarihinde eklenen 12. fıkra ile şu şekilde düzenlenmiştir; *“Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkra da belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkra ya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir.”*

Söz konusu düzenlemeyi inceleyen Anayasa Mahkemesi;¹¹ kuralların anlam ve kapsamının belirlenmesinde yukarıda belirtilen kuralların bir bütün olarak göz önünde bulundurulması gerektiğini, **anılan maddede Kuruma siber güvenliği sağlama görevi verildikten sonra**, söz konusu hükmü izleyen fıkra da BTK’nın “...görevi kapsamında...” ilgili yerlerden bilgi, belge, veri ve kayıtları alabilmesinin, değerlendirmesini yapabilmesinin, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilmesinin, bunlarla irtibat kurabilmesinin ve bu kapsamda diğer gerekli önlemleri alabilmesinin veya aldırabilmesinin öngörüldüğünü; BTK’ya tanınan bu yetki ve imkânların, BTK’nın **siber güvenliğin sağlanması göreviyle sınırlı olduğunu**, öte yandan aynı maddenin devamında BTK’nın maddedeki görevleriyle ilgili taleplerinin yerine getirilmesinin zorunlu olduğu belirtilirken “...bu maddedeki görevleri ile ilgili...” ibaresine yer verilmesi ve siber güvenliğin sağlanması görevinin verildiği hükme atıfta bulunulması dava konusu kuralların yukarıda belirtilen anlam ve kapsamını teyit ettiğini söylemiştir (§ § 38-39).

Kararda da belirtildiği üzere; BTK’nın söz konusu yetki ve görevi, siber güvenliğin sağlanması görevi ile sınırlıdır. BTK, bu madde kapsamında kişisel veri niteliğinde olan

11 Anayasa Mahkemesinin 24/7/2019 T., 2017/16 E., 2019/64 K. sayılı kararı; <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2019/64?EsasNo=2017%2F16>

trafik bilgilerini kaydetme, ilgili kurum veya kuruluşlardan isteme, saklama ve arşivleme görev ve yetkisi bulunmamaktadır.

Öte yandan, kişisel veri niteliğinde olan trafik bilgilerinin 6698 sayılı Kanun ile korunduğu ve bu kanuna göre kişisel verilerin işlenmesi için kanunda “açıkça” öngörülmesi gerektiği gözetildiğinde, kanunlarda geçen “her türlü bilgi ve belge” ve “gibi bilgi ve belgeler” gibi ifadelerin kişisel veriler söz konusu olduğunda uygulanması mümkün değildir. Anayasanın 20. maddesinde (yukarıda incelenmiştir), kişisel verilerin ancak kanunlarla öngörülmesi halinde işlenebilmesi güvence altına alındığı için, yönetmelik veya başka bir düzenleyici işlem ile BTK’ya kişisel verileri toplama yetkisi ve görevi verilemez. Bu nedenlerle; BTK’nın, kişisel veri niteliğindeki trafik bilgilerini, kaydetme, saklama, depolama, arşivleme ve aktarma görev ve yetkisi yoktur.

BTK’nın kişisel veri niteliğindeki trafik bilgilerini, kaydetme, saklama, depolama, arşivleme ve aktarma görev ve yetkisinin olmasa da; birçok mevzuat hükmü gereğince, kişisel verilerin usulüne uygun saklanıp saklanmadığını, veri ihlallerinin olup olmadığını, söz konusu kişisel verilerin zamanından silinip silinmediğini denetleme görev ve yükümlülüğü bulunmaktadır.

5809 sayılı Kanuna göre BTK’nın; abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak (md 6/1-c), elektronik haberleşme sektöründe faaliyet gösterenlerin mevzuata uymasını denetlemek ve/veya denetlettirmek, konu ile ilgili usul ve esasları belirlemek, aykırılık halinde mevzuatın öngördüğü işlemleri yapmak ve yaptırımları uygulamak (md 6/1-s) görev ve yükümlülüğü bulunmaktadır. Gizliliğin Korunması Yönetmeliğinin 14. maddesinde, bu yönetmelikte belirlenen yükümlülüklerinin yerine getirilmemesi halinde Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği hükümlerinin uygulanacağı düzenlenmiştir.

5809 sayılı Kanuna göre, iletişim bilgilerini içeren özel bilgiler, izinsiz ve yetkisiz olarak muhafaza edilemez (md. 56/1) ve bu yükümlülüğe aykırı hareket edenler bin günden beş bin güne kadar adli para cezasıyla cezalandırılır (md. 63/10). Yine, 5809 sayılı Kanuna dayanılarak

ıkarılan Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliğinde,¹² işletmecinin abonelerine/kullanıcılarına ait işlenen ve saklanan trafik verilerin ilgili mevzuatta **öngörülen sürede tutma veya silme yükümlölüğünü yerine getirmemesi halinde idari para cezası uygulanacağı hükme bağlanmıştır (md. 13/1-a-2).**

BTK'nın kişisel veri niteliğinde olan trafik bilgilerinin usulüne uygun saklanıp saklanmadığını, bu verilerin zamanında silinip silinmediğini denetleme görev ve yetkisi yukarıda yer verilen düzenlemeler ile sınırlı değildir. Birçok mevzuat hükmünde BTK'ya benzer denetim görev sorumlulukları yüklenmiştir.

f) 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve Bu Kanuna Dayanılarak Çıkartılan Yönetmelikler

Kanunun amacı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlölük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir. İşbu Kanun ile dünyada yaşanan gelişmelere paralel olarak, ölkemizde de internet dahil hızla yaygınlaşan elektronik iletişim araçlarının sağladığı imkânların suiistimal edilmesi suretiyle işlenen suçlarla mücadele konusunda etkin ve doğru bir yapılanmayı mümkün kılabilcek özel bir kanun çıkartılması amaçlanmıştır¹³. Dolayısıyla bu Kanun, sadece internet ortamında yapılan yayınlara yönelik olup, özel kanun niteliğindedir. Kanunun uygulanmasına ilişkin usul ve esaslar için, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik¹⁴ (Uygulama Yönetmeliği) çıkartılmıştır.

Erişim kavramı, Kanun'da *“Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını”* şeklinde (Kanun md. 2/1-d) düzenlemiş iken Uygulama Yönetmeliğinde *“Herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını”* şeklinde (Uygulama Yönetmeliği md. 3/1-e) düzenlenmiştir. **Erişim sağlayıcı** kavramı; *“Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri”* şeklinde (Kanun md. 2/1-e, Uygulama

12 15/02/2014 tarihli ve 28914 sayılı Resmi Gazete.

13 <http://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c156/tbmm22156099ss1397.pdf>

14 30.11.2007 tarihli ve 26716 sayılı Resmi Gazete

Yönetmeliği 3/1-f) düzenlenmiştir. Söz konusu düzenleme gereğince, GSM operatörleri gibi internete erişme olanağı sağlayan her gerçek ve tüzel kişi, erişim sağlayıcısıdır.

Trafik bilgisi kavramı ise Kanun'da tanımlanmış olup iki kez önemli değişikliğe uğramıştır. Uygulama Yönetmeliği incelendiğinde ise; genel bir “trafik bilgisi” tanımının yapılmadığı, bunun yerine “erişim sağlayıcı trafik bilgisi”, “yer sağlayıcı trafik bilgisi” ve “vekil sunucu trafik bilgisi” olmak üzere üç ayrı kategoride tanımlama yapıldığı göze çarpmaktadır. Kanun ile yapılan tanımlamanın yönetmelik ile genişletildiği ve tanım kapsamında alınmayan hususların bu şekilde kapsama alındığı görülmektedir.

Kanunun ilk halinde, **trafik bilgisi**; “İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri” şeklinde tanımlanmışken, 01/03/2014 tarihinde yayımlanan 6527 sayılı Kanun¹⁵ ile ilgili madde “Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,” şeklinde değiştirilmiş, 31/7/2020 tarihinde yayımlanan 7253 sayılı Kanun¹⁶ ile de aynı maddede yer alan “IP adresi,” ibaresinden sonra gelmek üzere “port bilgisi,” ibaresi eklenmiştir.

IP bilgisi ile port bilgisi Kanunun ilk halinde trafik bilgisi kavramına kasıtlı olarak dahil edilmemiş, 2014 ve 2020 yılında yapılan iki değişiklik ile önce IP bilgisi, daha sonra ise port bilgisi, trafik bilgisi kapsamına alınmıştır. Sonuç olarak, trafik bilgileri kavramına, 01/3/2014 tarihinden önce IP adresi ile port bilgisi, 01/3/2014 ile 31/7/2020 tarih arasında ise port bilgisi dahil değildir. Kanun'da düzenlenen trafik bilgisi tanımı, Uygulama Yönetmeliği ile başka bir isim kullanılmak suretiyle genişletilmiş ve **erişim sağlayıcı trafik bilgisi** olarak şu şekilde tanımlanmıştır; “İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgiler” (Uygulama Yönetmeliği md. 3/1-g). Söz konusu düzenlemede yer alan “gibi bilgiler” ibaresi, Danıştay kararı¹⁷ ile iptal edilmiştir.

15 26.12.2024 tarihli ve 28928 sayılı Resmi Gazete

16 31.7.2020 tarihli ve 31202 sayılı Resmi Gazete

17 Danıştay Onüçüncü Dairesinin 12/12/2019 tarihli ve E.:2013/239; K.:2019/4266 sayılı kararı

Kanun ile erişim sağlayıcılarına birtakım yükümlülükler getirilmiş olup bunlardan biri trafik bilgilerini saklama yükümlülüğüdür. Kanun'a göre, erişim sağlayıcı, *"Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla"* yükümlüdür (Kanun md 6/1-b). Atıfta bulunulan yönetmeliğin ilk halinde bu süre, bir yıl olarak belirlenmişken (Uygulama Yönetmeliği md. 8/1-b) Danıştay Kararı ile ilgili fıkranın tamamı iptal edilmiştir. Halihazırda Uygulama Yönetmeliğinde, erişim sağlayıcının, trafik bilgilerini ne kadar süre ile saklayacağına ilişkin herhangi bir düzenleme bulunmamaktadır.

Kanun'da (md. 6/3), erişim sağlayıcının saklama yükümlülüklerini yerine getirmemesi halinde uygulanacak yaptırımlar; *"Birinci fıkranın (b), (c), (ç) (...) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkan tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir."* şeklinde düzenlenmiştir. Benzer düzenleme Uygulama Yönetmeliğinde de bulunmaktadır (md. 9/2). Söz konusu yaptırımın, trafik bilgilerinin süresinden fazla saklanamaması hususunda da uygulanacağı hususunda herhangi bir tereddüt yoktur. Nitekim, saklama süresi belirlenirken, trafik bilgilerinin saklanabileceği en fazla süre de belirlenmiştir.

g) 5237 sayılı Türk Ceza Kanunu

Kişisel verilerin hukuka aykırı şekilde ele geçirilmesi, kaydedilmesi ve silinmesi gereken verilerin silinmemesi 5237 sayılı Türk Ceza Kanunu'nda yaptırıma tabi tutulmuştur. Kanunun *"Kişisel verilerin kaydedilmesi"* kenar başlıklı 135. maddesinde; hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği ve kişisel verinin, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda verilecek cezanın yarı oranında artırılacağı düzenlenmiştir.

Kanunun, *"Verileri hukuka aykırı olarak verme veya ele geçirme"* kenar başlıklı 136. maddesinde; kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin iki yıldan dört yıla kadar hapis cezası ile cezalandırılacağı ve *"Verileri yok etmeme"* kenar başlıklı 138. maddesinde de; kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir

yıldan iki yıla kadar hapis cezası verileceği ve suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek cezanın bir kat artırılacağına yer verilmiştir. TCK'daki düzenlemelerden ve özellikle 138. maddeden de anlaşılacağı üzere, konuyla özel düzenleme yapılmış ve mevzuatta ön görülen sürelerin geçmesine rağmen verilerin yok edilememesi yaptırıma bağlanmıştır.

h) 5271 sayılı Ceza Muhakemesi Kanunu ve Bu Kanuna Dayanılarak Çıkarılan Yönetmelikler

5271 sayılı Ceza Muhakemesi Kanununun 135. maddesinde, bir soruşturma ve kovuşturma kapsamında iletişimin tespiti, dinlenilmesi ve kayda alınmasına dair düzenleme yer almaktadır. Bu maddede belirtilen “*iletişimin tespiti*” kavramı, kanunda tanımlanmamıştır. Bu kavram, kanuna dayanılarak çıkartılan Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelikte¹⁸ (İletişimin Tespiti Yönetmeliği) “*İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri*” şeklinde (İletişimin Tespiti Yönetmeliği md. 3/1-i) tanımlanmıştır. Bu tanıma göre; HTS ile internet trafik bilgileri de bu kapsamdadır.

Ceza Muhakemesi Kanununun 135. maddesinin 6. fıkrasında; “*şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti, soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır. Kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespiti imkân veren kodu ve tedbirin süresi belirtilir. (Ek cümleler: 24/11/2016-6763/26 md.) Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtlar derhâl imha edilir*” düzenlemesi yer almaktadır.

Anılan düzenleme gereğince, iletişimin tespiti ancak ve ancak soruşturma aşamasında, hakim, gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılabilir.

Ceza Muhakemesi Kanunu kapsamında yapılacak olan iletişim tespitinin nasıl yapılacağına ilişkin usul ve esasların düzenlenmesi amacıyla çıkartılan İletişimin Tespiti Yönetmeliği ile iletişimin tespiti amacıyla Bilgi Teknolojileri ve İletişim Kuruma (BTK) bir takım görev ve yetkiler verilmiştir. Bu yetkilerin bir kısmına aşağıda yer verilmiştir (md 17/1-a,b,c,d);

“a) 2559 sayılı Kanunun ek 7 nci maddesi, 2803 sayılı Kanunun ek 5 inci maddesi ve 2937 sayılı Kanunun 6 ncı maddesi uyarınca, telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik iş ve işlemleri tek bir merkezden yürütmek,

b) 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemleri tek bir merkezden yürütmek,

c) (a) ve (b) bentleri kapsamındaki taleplerin bu Yönetmeliğe ve diğer ilgili mevzuata uygun olup olmadığını incelemek ve gerektiğinde yetkili mercilere başvuruda bulunmak,

d) (a) ve (b) bentleri uyarınca gerçekleştirilen işlemler sonucunda elde edilen verileri ve bilgileri ilgisine göre Millî İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına, talep etmeleri halinde mahkemeye ve Cumhuriyet başsavcılıklarına iletmek”

Yukarıda yer verilen Kanun ve Yönetmelik metinlerinden de anlaşılacağı üzere, Anayasanın 22. maddesinin koruması altında olan ve **kişisel veri niteliğindeki trafik bilgilerinin BTK tarafından tutulup depolanabilmesi mümkün değildir**. Anayasanın 22 maddesinde kanunla öngörülmüş olma şartı ile 6698 sayılı Kişisel Verileri Koruma Kanununda kişisel verilerin, kanunla **“açıkça”** öngörülmüş olması şartının da sağlanmadığı göze çarpmaktadır. Dolayısıyla, yönetmelikte böyle bir yetki veya görev verilmiş olsaydı dahi uygulanabilmesi hukuken mümkün değildi. Zira Kanun ile BTK’ya böyle bir yetki veya görev verilmemiştir. BTK’nın bu konudaki yetkisi, telekomünikasyon sektöründeki düzenleyici kurum olması nedeniyle, yukarıda sayılan merciler arasında koordinasyonu sağlayıp, talep

edilen bilgilerin tek bir elden iletimini sağlamaktır. Yani **BTK “icracı” değil “aracı” bir kurumdur.**

2. HTS Kayıtları ve İnternet Trafik Bilgilerinin Kimin Tarafından Saklandığı Sorunsalı

İnternet trafik bilgileri ve HTS kayıtlarının elektronik haberleşmeye ilişkin olmaları nedeniyle 5809 sayılı Elektronik Haberleşme Kanunu ve bu Kanun’a dayanılarak çıkarılan yönetmelikler gereğince 11/6/2016 tarihine kadar **1 yıl**, sonrasında da **2 yıl** saklanabilmelerine rağmen, bu sürenin geçmesinden sonra dahi, Ceza Muhakemesi Kanununun 135. maddesinde yer alan iletişimin tespiti kararları doğrultusunda yargı mercilerine gönderildikleri görülmektedir.

Kanun ve Yönetmeliklerdeki açık düzenlemeye rağmen, kişisel veri niteliğindeki trafik bilgilerinin, saklanmaları gereken süreden daha fazla olacak şekilde kim ya da kimler tarafından saklandığı, ilgili verilerin neden silinmediği, yükümlülüklerini ihlal edenlerin denetlenip denetlenmediği ve son olarak kişisel verilerin kim tarafından yargı mercilerine gönderildiği hususu gündeme gelmektedir. Aşağıda bu hususlar, kategorize edilerek ayrı başlıklar halinde irdelenmiştir.

a) Saklama Süresi Dolan Veriler Kimin Tarafından Saklandığı Hususunun Değerlendirilmesi

Mevzuat hükümleri gereğince, kişisel veri niteliğinde olan trafik bilgilerinin, değişik Kanunlardaki tabiri ile “işletme”, “erişim sağlayıcı” ve “veri sorumlusu” sıfatıyla, bildiğimiz anlamda GSM ve internet operatörleri tarafından mevzuatta belirtilen süre boyunca saklama ve süre bitiminde silme yükümlülüğü bulunmaktadır. Bu sorumluluk, mevzuat ile sadece bu veri sorumlularına yüklenmiştir.

Söz konusu yükümlülüğün, erişim sağlayıcılar açısından belli bir külfete sebep olduğu, sistem bakımı, depolama alanı gibi sorunlar nedeniyle ilgili kişisel verileri süresinden fazla saklamak istemeyeceğinde şüphe yoktur. Nitekim, mevzuat gereğince amaçları dışında ilgili verileri de kullanamayacağından ve bu veriler ile ticari bir menfaat elde edilemeyeceğinden, söz konusu işletmelerin kişisel verileri süresinden fazla tutmasının kendilerine bir fayda sağlaması mümkün değildir. Nitekim, veri sorumlusu sıfatına haiz veri sorumluların tamamı,

kendi internet sitelerinde yayımlamak zorunda olduğu ve yayımladığı aydınlatma metnine göre, saklama süresi dolan kişisel verilerin silindiğini beyan etmektedirler¹⁹.

Nitekim, konuyla ilgili bir ağır ceza mahkemesi, dokuz farklı numaraya ilişkin bir yılı aşan sürelerdeki trafik bilgilerini Bilgi Teknolojileri Kurumu (BTK) yerine doğrudan GSM firmasından istemiş, istemi değerlendiren firma cevabi yazısında Gizliliğin Korunması Yönetmeliğinin 14/1. maddesini hatırlatarak; *“her ne kadar yazınızda “aynı IP numarasının başka kişilere tahsis edilip edilmediği, edilmiş ise bu kişilerin kimlikleri ve numaralarının her bir sanık yönünden gönderilmesi” istenmiş ise de, tespit edilen IP'lere ilişkin talebinize konu veriler şirketimiz sistemlerinde son bir yıl için saklandığından, sorgulanması istenen tarihlere ilişkin inceleme yapılması mümkün olmamıştır”*²⁰ demiştir. Yani **söz konusu veriler, saklama süresi boyunca erişim sağlayıcılar tarafından saklanmakta, saklama süresinin bitiminde ise silinmektedir.**

Erişim sağlayıcılar, söz konusu verileri süresinden fazla saklamıyorsa bu verilerin kimin tarafından saklandığı hususunun izahı önem taşımaktadır. Zira, ortada kişisel veri niteliğindeki trafik bilgilerinin süresinden fazla saklandığı ve yargı mercilerine gönderildiği gerçeği bulunmaktadır.

Mevzuat hükümlerine göre, Ceza Muhakemesi Kanununun 135. maddesi kapsamında verilen iletişimin tespitine yönelik kararların, aracı sıfatıyla BTK'ya, BTK'nın da aracı sıfatıyla veri sorumlusundan ilgili verileri alıp yargı mercilerine göndermesi gerekir. Somut durumda, veri sorumlusunun saklamadığını söylediği trafik bilgilerini, BTK'nın nasıl yargı mercilerine gönderdiği hususu izaha muhtaçtır. Nitekim, mevzuat hükümlerine göre, **ilgili trafik bilgilerini saklamak veri sorumlusunun yükümlülüğüdür ve BTK'nın bu konuda herhangi bir görev ve yetkisi bulunmamaktadır.**

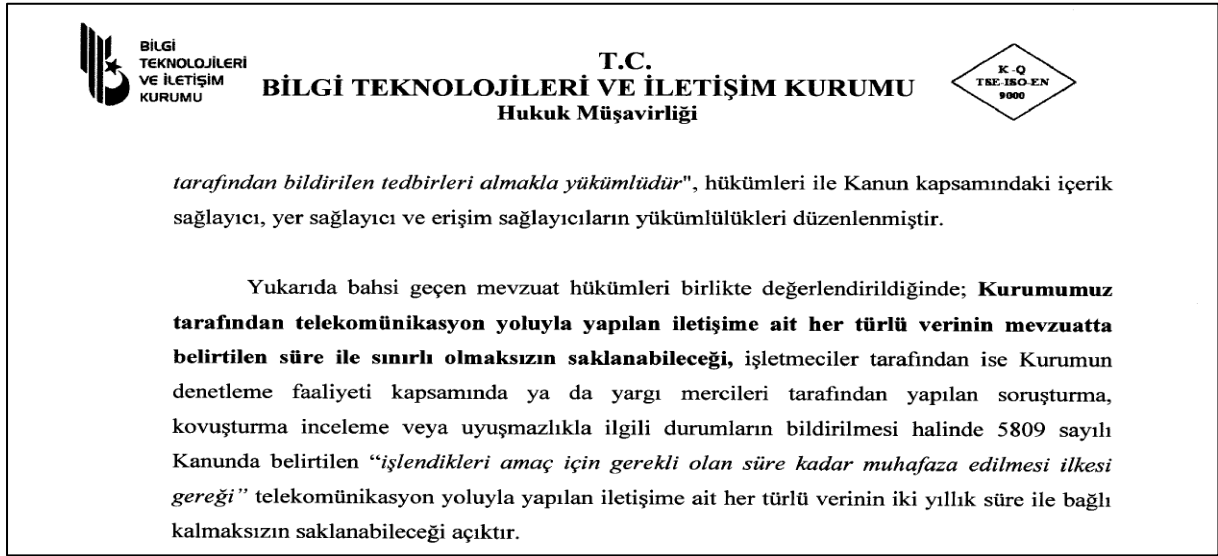
BTK tarafından, bu hususta kamuoyunu aydınlatan bir açıklama yapılmamaktadır. Fakat, konu ile alakalı veya benzer davalarda BTK'nın yaptığı savunmaların içeriğinde, söz konusu verileri kendisinin sakladığı ve yargı mercilerinden talep ettiğinde bu verileri derleyip yargı mercileriyle paylaştığına ilişkin ikrarları bulunmaktadır. Kullanıcı profillerinin çıkarılması amacıyla BTK tarafından alınan bir Kurul Kararına karşı açılan iptal davasında,

19 <https://www.turktelekom.com.tr/destek/gizlilik-guvenlik-ve-kvkk/aydinlatma-metinleri>

20 Turkcell GSM Firmasının 14/7/2017 tarihinde Ankara 15. Ağır Ceza Mahkemesine (2017/9 esas) gönderdiği müzekkere cevabı.

Danıştay dava konusu Kurul kararı gereğince BTK'ya aktarılan abonelere ait kişisel veriler üzerinde, "veri işleme" yapıp yapılmadığı sormuş, davalı idarenin 05/08/2021 tarih ve 50218 sayılı ara karar cevabında, yetkili kurum ve kuruluşlar tarafından herhangi bir hukuki inceleme talebinde bulunulması durumunda, sorgulanmaya hazır olarak tutulmasını teminen ilgili sorgu sistemleri için işlendiği belirtilmiştir.

Kişisel veri niteliğinde olan trafik bilgilerinin süresinden fazla saklanmasıyla ilgili açılan başka bir davada ise;²¹ **BTK, telekomünikasyon yoluyla yapılan iletişime ait her türlü verinin mevzuatta belirtilen süre ile sınırlı olmaksızın saklama yetkisinin olduğunu iddia etmiş ve trafik bilgilerini saklamasını hukuka uygun görmüştür!** BTK'nın yaptığı savunmanın²² ilgili kısmının görseli aşağıda mevcuttur.



Görselden de anlaşılacağı üzere; BTK, nasıl elde ettiği belli olmayan trafik bilgilerini saklamakta, arşivlemekte ve talep olursa ilgili yerlere göndermektedir. Bu da yeterli değilmiş gibi söz konusu kişisel verileri sınırsız süreyle hem işletmeler hem de kendisi tarafından saklanabileceğini iddia etmektedir. Bu iddia aşağıda ayrıca değerlendirilmiştir.

21 İlgili dava dosyası Danıştay 13. Daire Başkanlığının 2020/997 esas sayılı dosyasında derdesttir.

22 Bilgi Teknolojileri ve İletişim Kurumu Hukuk Müşavirliğinin 04/3/2020 tarihli 53393206-641.04-16101 sayılı yazısı

b) BTK'nın Veri Saklama Yetkisinin Değerlendirilmesi

Saklama süresi dolan veriler, erişim sağlayıcı işletmeler tarafından saklanmadığına ve BTK tarafından bir şekilde yargı mercilerine gönderildiğine göre bu kişisel veriler BTK tarafından saklanmaktadır. Fakat mevzuat incelendiğinde, **BTK'nın kişisel veri niteliğinde olan trafik bilgilerini, erişim sağlayıcı olan işletmelerden isteyebileceğine, bu verileri saklayabileceğine, arşivleyebileceğine ve aktarabileceğine ilişkin bir yasal düzenleme yoktur.** Hal böyle iken, bu verilerin BTK'nın eline nasıl geçtiği hususunun izah edilmesinde zaruret vardır. Uygulamada, düzenleyici kurum olan BTK'nın ilgili verileri, kendi çıkarmış olduğu Gizli ibareli Kurul Kararları ile temin ettiği anlaşılmaktadır.

BTK'nın, zaman zaman erişim sağlayıcı olan işletmelere yazdığı yazılar ile işletmelerden kullanıcı profillerini çıkarmaya, kullanıcıların kişisel bilgilerini almaya ve daha da önemlisi kullanıcıların trafik bilgilerinin sürekli olarak BTK'ya aktarılmasına yönelik yazılar gönderdiği bilinmektedir. Bu yazılar **“GİZLİ”** ibareli olarak gönderilmekte ve kamuoyu ile paylaşılmamaktadır.

BTK'nın ilgili işletmelere gönderdiği yazılardan biri Bilgi Teknolojileri ve İletişim Kurumunun 15/12/2020 tarihli E-58415308-400-78040 ve *“İSS Trafik Log Deseni”* konulu yazısıdır²³. İlgili yazının ekinde ise *“İSS Trafik Deseni (13 sayfa)”* ve *“Dağıtım Listesi”* yer almaktadır.²⁴ **“GİZLİ”** ibareli yazı incelendiğinde; belli bir abone sayısından fazla abonesi olan işletmelerin, abone ve oturum kayıtlarının gönderilmesi amacıyla ek sunucu tedarik etmesi, diğerlerinin ise kurulu sunucularını kullanmaya devam etmeleri istenmiş ve ayrıca ekte yer alan teknik dokümana riayet edilmesi hususu ihtar edilmiştir.

Yazı da yer alan; *“Abone sayısı 20.000'in altında olan işletmeler ise trafik verisinin gönderimi için de hali hazırda abone ve oturum kayıtlarının gönderimi için kurulu uç sunucularını kullanmaya devam edecektir”* ifadesi önemlidir. Zira bu ifadeden, kişisel **bilgilerinin bu yazıdan önce de BTK'ya gönderildiği anlaşılmaktadır.** İlgili yazıda, regülasyon kurumu olan BTK'nın hangi

23 İlgili yazıya ve yazının eklerine, <https://www.turkiye.gov.tr/btk-ebys> adresindeki sayfada yer alan evrak doğrulama koduna “TVPEHQGS”, evrak sayısına ise “78040” yazılarak ve güvenlik resminde yer alan güvenlik kontrolü tamamlanarak ulaşılabilir. Ayrıca ilgili yazı, bu makalenin yayımlandığı tarihte https://static.bianet.org/system/uploads/1/files/attachments/000/003/655/original/%C4%B0SS_Trafik_Log_Deseni.pdf?1658407569 adresinde de yer almaktadır.

24 <https://www.drgokhangunes.com/genel/iss-trafik-logu-ve-teknik-detay-dokumani/>

yasal düzenlemeye istaneden bu bilgileri istediğine yer verilmemiştir. İlgili yazının ekinde yer alan dağıtım listesinde de 281 işletme bulunmaktadır.

BTK, ilgili yazıdan önce de bazı kişisel verilerin devamlı olarak kendisine gönderilmesini istese de bu istek gizli yapıldığı için ilgili yazılara ve yazı içeriklerine ulaşmak mümkün değildi. Ancak, yakın zamanda yazılan bir makalede,²⁵ yukarıda yer verilen 15/12/2020 tarihli yazıdan önce de 24/10/2018 tarihli bir başka yazıyla BTK'nın işletmelerden hangi bilgileri istediği ve bu yazı ve taleplerin ne anlama geldiğiyle ilgili şu hususlara yer verilmiştir; ²⁶

“BTK, 24.10.2018 tarih, 2018/DK-BSD-314 sayılı kurul kararını ve bu kararda değişiklik içeren; 16.04.2019 tarih 2019/DK-BSD/109 sayılı, 25.04.2019 tarihli 2019/DK-BSD/117 sayılı, 08.05.2019 tarih 2019/DK-BSD/131 sayılı kurul kararlarını almıştır. Söz konusu Kurul kararları, BTK'nın 5397 sayılı Kanun kapsamındaki önleyici istihbari amaçlı ve CMK kapsamındaki adli amaçlı iletişimin denetlenmesi görevlerini yerine getirme amacı gerekçesiyle, ISS, sabit telefon hizmeti, altyapı hizmeti, uydu haberleşme hizmeti, mobil uydu hizmeti sunan işletmecilerin abonelerinin kişisel ve ticari verilerinin detaylarını içerir “abone dosyalarının” BTK'ya aktarılması hususlarını içermektedir. 24.20.2018 tarih ve 2018/DK-BSD-314 sayılı kurul kararında yer alan abone teknik detay dokümanı, abone kişisel verilerini ve ticari verilerini içerir “abone dosyalarının” BTK'ya aktarımına ve abonelik süreçlerine ilişkin hükümler içermektedir. Şahıs aboneliklerinde; ad, soyad, kimlik numarası, detaylı adres bilgisi, anne kızlık soyadı, mesleği, doğum yeri ve tarihi, meslek kimliğinin seri numarası istenmekte, tüzel kişilerde; ticaret unvanı, mersis numarası, vergi kimlik numarası, kurum yetkilisinin unvanı, kimlik numarası, isim ve soy ismi, telefon numarası gibi veriler istenmektedir. Kurul kararı uyarınca verilerin bir kısmı abone hareket dosyaları olarak BTK'ya iletilecekken, aboneliklerin son durumunun da aylık rapor olarak gönderileceği ifade edilmiştir. Bu karar ile Türkiye'de telefon, internet aboneliği bulunan tüm kullanıcıların verileri kendilerinin bilgisi olmadan, açık rızası bulunmadan ve hiçbir sınırlama olmadan 2019 yılından bu yana BTK'ya aktarılmaktadır.”

25 Yorgancıoğlu, E., & Demircan, Y., T., (2023). Bilgi teknolojileri ve iletişim kurumu tarafından toplanan internet trafik verilerinin kişisel verilerin korunması hakkı bağlamında değerlendirilmesi. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 22(48), 1189- 1215. doi: 10.46928/iticusbe.1203350, Erişim adresi: <https://dergipark.org.tr/tr/pub/iticusbe/issue/81841/1203350>

26 Makalenin yazarı Elif Yorgancıoğlu, Ankara 3. İdare Mahkemesi 2022/314 E. sayılı dava dosyasında davacı işletmecinin vekilliği görevini yürütmektedir.

Makaleden de anlaşılacağı üzere, BTK 2018 yılında aldığı karar ile trafik bilgilerini de içeren kişisel verileri herhangi bir mahkeme kararı ve ayırım olmaksızın işletmelerden istemektedir. Bu husus, özellikle trafik verileri açısından endişe uyandırıcıdır.

BTK'nın 15/12/2020 tarihli "İSS Trafik Log Deseni" konulu yazısı ekinde yer alan 13 sayfalık teknik doküman incelendiğinde de;²⁷ dokümanın son sayfasında yer alan "Azami 1 saat olabilecek olan Trafik logu gönderim periyodu Kuruma yazılı olarak bildirilmeli," , "Yukarıda belirtilen alanlarda yer alan desen yapısına ve kısıtlamalara uygun olarak iletilmeyen verilerin BTK tarafından yapılan incelemeler neticesinde tespit edilmesi gerekli cezai işlemler başlatılacaktır." ve "İşletmeciler dosyalarını düzenli olarak göndermekle, gönderdikleri verilerin doğruluğunu ve bütünlüğünü sağlamakla yükümlüdürler" ifadeleri dikkat çekicidir. Bu ifadelerden anlaşılacağı üzere BTK, **en fazla bir saatlik periyotlarla tüm kullanıcıların trafik loglarını işletmelerden istemekte, trafik logu göndermenin zorunlu olduğunu belirtip, göndermeyen işletmelere ceza verileceğini ihtar etmektedir.** BTK'nın istediği veriler, teknik dokümanda detaylı olarak izah edilmiştir. Bu bilgiler arasında; kullanıcının, ismi-soyismi, IP no'su, özel köprü (port), gerçek IP, gerçek köprü, gerçek köprü başlangıcı, gerçek köprü bitiş bilgileri, trafiğin başlama zamanı, trafik süresi, hedef IP adresi ve portu, bağlantı uygulama için kurulduysa uygulamanın ismi, bir web sayfasına bağlantı gerçekleştirildiyse sayfanın adresi gibi kişinin haberleşme hürriyetine, özel hayatının gizliliğinin ihlali niteliğindeki kişisel verilerdir.

BTK'nın "İSS Trafik Log Deseni" konulu yazısına ilişkin Ankara idare mahkemesi nezdinde dava açılmış²⁸ dava kapsamında savunma yapan BTK, dava konusu işlemin varlığına dair herhangi bir itirazda bulunmamıştır. **BTK, kişisel veri niteliğindeki ve hatta bazı durumlarda özel nitelikli kişisel verileri en fazla bir saatlik periyotlar halinde işletmelerden cezai yaptırım tehdidiyle temin etmektedir.** BTK'nın söz konusu verilerle ne gibi işlemler yaptığı, verileri bozup bozmadığı, verileri kimlerle paylaştığı, kimlerin verilere erişim hakkına sahip olduğu ve verilerin doğruluğunu ve bütünlüğünü nasıl sağladığı gibi hususların cevabı bulunmamaktadır. Nitekim, bu konuda herhangi bir yasal mevzuat

27 <https://www.drgokhangunes.com/genel/iss-trafik-logu-ve-teknik-detay-dokumani/>

28 Ankara 3. İdare Mahkemesinin 2022/314 esas sayılı dosyasında derdesttir.

olmadığı gibi konu hakkında idare tarafından çıkartılmış bir düzenleyici işlem de yoktur. Bu haliyle, Anayasa ve yasalarla korunan değerler, BTK uygulamaları ile ihlal edilmektedir.

Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği, bu sınırlamaların Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı belirtilmiştir. Anayasa'nın 20. maddesinin ilk fıkrasında, herkesin özel hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı belirtilmiş; son fıkrasında da herkesin kişisel verilerinin korunmasını isteme hakkına sahip olduğu ve kişisel verilerin ancak kanunda öngörülen hallerde veya açık rızanın mevcut olması durumunda işleneceği güvence altına alınmıştır.

Anayasa'nın 22. maddesinde öngörülen haberleşme özgürlüğü, kişinin kesintiye uğramadan ve sansür edilmeden başkalarıyla iletişim kurma hakkıdır. Bu özgürlük, çok daha geniş bir alanı kaplayan *“özel hayatın”* bir yönünü oluşturur. Dolayısıyla *“haberleşmenin gizliliği”* kavramı, özel hayatın gizliliği kavramı içinde yer alır.

Özel hayatın korunması her şeyden önce özel hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Kişinin özel hayatında yaşananların yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini isteme hakkı, kişinin temel haklarından biridir ve bu niteliği nedeniyle insan haklarına ilişkin beyanname ve sözleşmelerde yer almış, tüm demokratik ülkelerin mevzuatlarında açıkça belirlenen istisnalar dışında devlete, topluma ve diğer kişilere karşı korunmuştur.

Bilişim teknolojilerindeki gelişmeler sonucunda geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi, daha önce birbirinden ilişkisiz şekilde tutulan verilerin merkezî olarak bir araya getirilebilmesi, verilerin veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkânlarla analize tabi tutulmak suretiyle veriden yeni veriler üretme kapasitesinin artması, verilere erişim ve veri transferinin kolaylaşması, kişisel verilerin ticari işletmeler kıymetli bir varlık niteliği kazanması neticesinde özel sektör unsurlarınca oluşturulan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır.

Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, kişiye ilişkin bütün bilgileri ifade eder. Bu bağlamda, adı-soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, görüntü ve ses kayıtları, IP adresi, e-posta adresi, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Buna göre; **trafik bilgilerinin, kişisel veri niteliğinde olduğunda kuşku bulunmamaktadır.**

Anayasa Mahkemesi tarafından, BTK'nın kişisel veri niteliğindeki trafik bilgilerini işletmelerden alabilme hakkının olmadığına ilişkin birçok yorumu ve bu konudaki kanunların ilgili maddelerini iptal ettiği birçok kararı bulunmaktadır. Bu kararlardan birinde Anayasa Mahkemesi, 5809 sayılı Kanun'un Bilgi Teknolojileri ve İletişim Kurumunun işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden elektronik haberleşmeyle ilgili olarak, ihtiyaç duyacağı her türlü bilgi ve belgeyi alabilmesini öngören 6. maddesinin (1) numaralı fıkrasının (1) bendi incelenmiş²⁹ ve şu tespitte bulunulmuştur;

“İptali istenen ibare ile Kuruma verilen ‘işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi alma yetkisi’nin, Kurumun kuruluş amacı ve faaliyet alanında yer alan elektronik haberleşme sektörü ile ilgili şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi amacıyla sınırlı olarak kullanılabileceği, ayrıca Kurumun abone, kullanıcı, tüketici ve son kullanıcıların kişisel bilgilerinin gizliliğini ve işletmecilerin ticari sırlarını korumakla görevli olduğu dikkate alındığında, iptali istenen ibare ile Kuruma gerçek ya da tüzel kişilerden özel hayatın gizliliğini ya da haberleşme özgürlüğünü ihlal eden bilgi ve belgeleri alma konusunda yetki verildiği söylenemez. Bu nedenle iptali istenen kuralın özel hayatın gizliliği hakkını ve haberleşme özgürlüğünü sınırlayan bir yönü bulunmamaktadır.”

Görüldüğü üzere, elektronik haberleşme sektörü ile ilgili şikâyetleri değerlendirme ve denetim işlevlerini gerektiği gibi yerine getirebilmesi amacıyla sınırlı olarak kullanılmak üzere BTK'ya kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden elektronik haberleşmeyle ilgili olarak, ihtiyaç duyacağı her türlü bilgi ve belgeyi alabilme yetkisi verilmiştir. Sınırlı olarak verilen bu yetkinin, tüm abonelere ait kişisel verileri kapsayacak şekilde sınırsız olarak

29 Anayasa Mahkemesinin 2/6/2011 tarihli 2008/115 esas ve 2011/86 sayılı kararı

kullanmasına özel hayatın gizliliğini ve haberleşme özgürlüğünü ihlal edeceği için izin verilmemiştir.

Benzer şekilde; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlemesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 3. maddesinin 4. fıkrasında yer alan; *"Trafik bilgisi, Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden temin edilir. Hakim tarafından karar verilmesi hallerinde ilgili mercilere verilir."* düzenlemesi Anayasa Mahkemesi tarafından;³⁰ *"...Trafik bilgisi adı altında temin edilecek olan bilgiler Anayasa ile teminat altına alınan iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü, kişisel verilerin korunması gibi birçok temel hakla doğrudan ilgili olup bu bilgilerin TİB (yeni ismi ile BTK) tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olması temel hak ve özgürlüklerin doğrudan ihlaline sebebiyet vermektedir. Anayasa'nın 13. ve 20. maddelerinde yer alan güvencelere rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın amaç, gerekçe, kapsam ve sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle, dava konusu kural Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır"* gerekçesiyle iptal edilmiştir.

Aynı şekilde Anayasa Mahkemesi, 5651 sayılı Kanunun 5/5. maddesinde yer alan; *"Yer sağlayıcı, Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla yükümlüdür"* ifadesi ile erişim sağlayıcıların; *"Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla"* yükümlü olduklarını belirten 6/1-d maddesindeki ifadeyi; *"...bu çerçevede iptali istenilen kurallarda, TİB'in (BTK) hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB'de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamaktadır. Kurallar bu yönleriyle belirli ve öngörülebilir değildirler. Anayasa'da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin konu, amaç ve kapsam bakımından yeterli sınırlamaya tabi kılınmaksızın koşulsuz olarak TİB'e verilmesine imkân tanımakta, böylece kişiler idareye karşı korumasız hale getirilmektedirler. Dolayısıyla*

30 Anayasa Mahkemesinin 2/10/2014 tarihli 2014/149 esas ve 2014/151 sayılı kararı

iptali istenilen kurallar, belirli ve öngörülebilir olmadığından kişilerin kişisel verilerin korunması hakkını ölçüsüzce sınırlandırmakta ve Anayasa'nın 20. maddesine aykırılık teşkil etmektedir. Açıklanan nedenlerle kurallar, Anayasa'nın 2., 13. ve 20. maddelerine aykırıdır” diyerek iptal etmiştir.³¹

Görüldüğü üzere, aboneye ait trafik bilgisinin, idarece, işletmecilerden temin edilmesine yönelik, kanuni düzenlemeler, Anayasa Mahkemesince iptal edilmiştir. Hali hazırda, bu konuda herhangi bir kanun hükmü de bulunmamaktadır. Kanunla verilmeyen yetkinin, daha açık bir ifadeyle, **BTK'ya sektörün düzenlenmesi amacıyla verilen genel yetkinin, ikincil mevzuat ile genişletilmesi ve bu kapsamda kişisel veri niteliğindeki trafik bilgilerinin toplanması mümkün değildir.**

Bununla birlikte, 5809 sayılı Kanun'un 12. maddesinin (2) numaralı fıkrasının (d) bendi ile abonelere ait kişisel verilerin ve gizliliğinin korunması görevi işletmecilere; işletmeciler tarafından abonelere ait kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin düzenlemeleri ve denetlemeleri yapmak görevi de BTK'ya verilmiştir. Dolayısıyla işletmeciler, kişisel bilgileri ve belgeleri abonelerden isteyebilecekler, trafik bilgilerini kanunda öngörülen süre boyunca saklayacaklardır. Kanun koyucu, abonelere ait kişisel bilgileri ve belgeleri koruma görevini de işletmecilere vermiştir. **İşletmecilerin, korumakla yükümlü olduğu abonelerine ait kişisel verileri BTK ile paylaşabileceklerine dair kanuni bir düzenleme yoktur. BTK, işletmecilerde bulunan kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik gereken tedbirleri almak adına işletmecilere yükümlülükler getirmek ve bunun için düzenlemeler yapmakla mükelleftir.**

Her ne kadar, özel yaşam hakkı belirli koşullarda ve demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olmamak üzere kanunla sınırlanabilir ise de; BTK'nın, hakkında herhangi bir adli süreç veya talep bulunmayan abonelere ilişkin kişisel verilere sınırsız bir şekilde ulaşabiliyor, **bu verileri hiçbir güvence olmaksızın sınırsız süreyle saklayabiliyor ve arşivleyebiliyor olması, kişilerin özel hayatlarına müdahale etme anlamına gelir ki somut durumda gerçekleşen budur.**

Anayasanın 20. maddesinin 3. fıkrası gereğince, kişisel verilerin ancak kanunda öngörülen hallerde saklanabileceğinin düzenlenmesi, yine Anayasanın 13. maddesi gereğince,

31 AYM'nin 08/12/2015 T., 2014/87 E., 2015/112 K. sayılı kararı.

temel hak ve hürriyetlerin Anayasanın ilgili maddelerinde yer verilen sebeplerle sınırlı olmak kaydıyla özüne dokunulmaksızın ancak kanunla sınırlandırılabilirliğinin güvence altına alınması, 6698 sayılı Kişisel Verileri Koruma Kanununun 5/2-a ve 6/3-b fıkraları gereğince, kişisel verilerin ancak kanunda “açıkça” öngörülmüş olması koşulunu içermesi nedenleriyle, **Kanunda açık bir şekilde yer verilmeyen şekilde kişisel verilerin saklanması mümkün değildir. Bu bağlamda mevzuat hükümleri incelendiğinde, kişisel veri niteliğindeki kişisel verilerin BTK tarafından işlenebileceğine ilişkin kanunun “açıkça” verdiği bir yetki bulunmamaktadır.**

BTK’nın yetki ve sorumluluklarına yer verilen Kanun ve Yönetmelik metinlerinden de anlaşılacağı üzere, **Anayasa’nın 22. maddesinin koruması altında olan ve kişisel veri niteliğindeki trafik bilgilerinin BTK tarafından tutulup depolanabilmesi mümkün değildir.** Zira BTK’ya böyle bir yetki verilememiştir ve **BTK’nın bu konudaki yetkisi, telekomünikasyon sektöründeki düzenleyici kurum olması nedeniyle, yukarıda sayılan merciler arasında koordinasyonu sağlayıp, talep edilen bilgilerin tek bir elden iletimini sağlamaktır.** Yani **BTK “icracı” değil “aracı” bir kurumdur.**

Yapılan açıklamalardan da anlaşılacağı üzere, Kanun ve Yönetmeliklerde BTK’nın sınırsız şekilde ve herhangi şarta bağlı olmadan talep ettiği bilgileri erişim sağlayıcılardan isteyebileceğine ilişkin bir hüküm yoktur. Böyle bir yetkisi olmayan BTK’nın, Anayasa’nın 22. maddesi gereğince ancak hâkim kararıyla ulaşılabilecek trafik bilgilerini, erişim sağlayıcılardan doğrudan isteyebilmesi ve bu bilgileri depolayıp, saklama süresi geçtikten sonra da ilgili mercilere gönderebilmesi mümkün değildir. Buna rağmen, BTK, kişisel veri niteliğindeki trafik bilgilerinin düzenli olarak kendisine gönderilmesini dikte etmekte bu kapsamda elde ettiği trafik bilgileri sınırsız bir süre boyunca keyfi bir şekilde saklamakta, gelen verileri süzüp anlamlı tablolar oluşturup paylaşmaktadır.

c) Bilgi Teknolojileri ve İletişim Kurumunun Denetim Yükümlülüğü

BTK’nın kişisel veri niteliğindeki bilgileri toplama, depolama, saklama ve arşivleme yetki ve görevi olmasa da; Kanun Koyucu ve yürütmenin zaman zaman bu konuda düzenleme yaptıkları görülmektedir. Ancak, bu kanuni düzenlemelerin tamamı Anayasa Mahkemesi tarafından Anayasaya aykırı bulunarak, yönetmelikle yapılan düzenlemelerde Danıştay tarafından iptal edilmiştir. Halihazırda BTK’nın kişisel veri niteliğindeki bilgileri, herhangi bir

mahkeme kararı olmaksızın, erişim sağlayıcı olan işletmelerden alabileceğine ilişkin bir hüküm bulunmamasına rağmen BTK, kendi çıkarttığı kurul kararları ve zorlama yorumlarla işletmelerden kişisel verileri istemekte, bu hususta işletmeleri cezai yaptırım uygulamakla tehdit edip verileri temin etmekte ve sınırsız süre ve hiçbir koşula uymaksızın kullanmaktadır.

Bu konuda BTK'nın sorumluluğu, işletmeleri kullanıcıların kişisel verilerini gerektiği gibi koruyup korumadığı, ilgili verileri rıza olmaksızın başka yerlere aktarıp aktarmadığı hususlarında denetlemek ve gerekli önlemleri almaktır. BTK'nın konuyla ilgili yükümlülüklerine biri 5651 sayılı Yasanın 6/3. maddesinde düzenlemiştir. Düzenlemede, saklama süresine ilişkin olan maddeye atıf yapılmış ve bu maddeye aykırılık halinde işletmeye ceza verileceği belirtilmiştir. Aynı şekilde BTK'ya 5809 sayılı Yasanın 6/1-c maddesinde; *“abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak”* görevi verilmiştir. Anılan düzenlemeler gereğince BTK'nın işletmeleri denetlemesi ve süresi geçtiği için silinmeyen veriler nedeniyle işletmelere yaptırım uygulaması gerekmektedir. **Buna rağmen BTK, bu denetleme yükümlülüğünü ihmal etmekte ve daha kötüsü süresi geçtiği halde silinmeyen verileri, kendisi depolamakta ve işlemekte ve islediği verileri başka kurum ve kuruluşlarla da paylaşmaktadır.**

Uygulamada BTK, söz konusu denetim görev sorumluluklarını yerine getirmek bir yana, Anayasa ve yasalara açıkça aykırı olmasına, Anayasa mahkemesi ve Danıştay kararlarında böyle bir yetki ve görevinin olmadığı açıkça belirtilmesine rağmen, kişisel verileri işletmelerden almakta ve kendisi bu verileri işlemektedir. Bu bağlamda, söz konusu kişisel verileri isteyen BTK ve verileri gönderen işletmeler bu hukuka aykırılıktan sorumludurlar. Kanunlara göre bu konudaki hukuka aykırılığı gidermek ve gerektiğinde yaptırım uygulamak BTK'nın görevi olmasına rağmen, hukuka aykırılıkların doğrudan kendisinden kaynaklanması ve işletmeleri yaptırım tehdidiyle hukuksuzluğa zorlaması nedeniyle konu ile alakalı hiçbir işlem yapılamamaktadır. Kısaca, BTK kişisel veri niteliğinde olan internet trafik bilgilerinin ve HTS kayıtlarının süresinden fazla saklanmasıyla ilgili denetim görev ve yükümlülüğünü ihmal etmektedir.

3. Saklama Süresi Dolan Verilerin Delil Niteliği

Bir hususun ceza hukuku açısından delil olarak kabul edilebilmesi için, o hususun kanunlara uygun elde edilmesi şarttır. Nitekim, Anayasanın 38. maddesinin 6. fıkrasında kanuna aykırı olarak elde edilmiş bulguların delil olarak kabul edilemeyeceğine, CMK'nın 206. maddesinin 2. fıkrasında delillerin kanuna aykırı elde edilmesi halinde reddolunacağına ve yine CMK'nın 217. maddesinin 2. fıkrasında da yüklenen suçun hukuka uygun elde edilmiş delillerle ispat edileceğine ilişkin hükümler bulunmaktadır.

Mevzuat gereğince, iletişimin tespitine yönelik hukuka uygun bir karar verildiğinde, ilgili kararın bir üst yazı ile birlikte, yargı mercilerince aracı kurum olan BTK'ya gönderilmesi, BTK'nın ise ilgili yazının şekil açısından hukuka uygunluğunu incelemesi ve gerektiğinde ilgili mercilerle iletişime geçmesi gerekir. Buradaki inceleme, sadece usuli bir inceleme olup BTK'nın mahkeme kararlarını denetleme hakkı ve yetkisi yoktur. BTK'nın görevi, yazı ekinde kararın olup olmadığını, kararın içeriğinde şekil bakımından unutulmuş bir şey bulunup bulunmadığını (tespit tarihlerinin başlangıcı, bitişi, tespit yapılacak numara ve kişiye ilişkin bilgiler gibi) incelemek ve eksiklik görürse ilgili merciye irtibata geçmektir. Şayet böyle bir eksiklik yoksa ilgili işletmeden verileri alacak ve yargı mercine gönderecektir.

Ancak, uygulamada mevzuatın aksine hareket edilmekte ve trafik bilgileri mahkemece iletişimin tespitine karar verilmeden önce işletmelerden toplanmaktadır. Esasında BTK'nın yaptığı işlemin *“iletişimin tespiti”* dir. Zira, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmeliğin 3. maddesinin i bendinde yapılan tanıma göre **iletişimin tespiti**; *“iletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri”* ifade eder. Ancak, trafik verilerini kaydetip isleme ve yasal süresi boyunca saklama işletmelerin yükümlülüğündedir ve BTK'ya bu konuda kanunla verilmiş bir yetki yoktur.

Bir idari kurum olan BTK'nın yasal zorunluluk nedeniyle trafik verilerini elinde bulundurulmuş işletmelerden alması, *“diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler”* kapsamında değerlendirilmelidir. Zira, ilgili trafik verilerinin BTK tarafından alınmasıyla birlikte ceza

hukuku anlamında iletişim tespit edilmiş olur. Bu durumda, mahkeme kararı olmadan iletişim tespit edilmesi nedeniyle trafik verileri hukuka aykırı hale gelir ve bu şekilde elde edilen trafik verileri yargılamalarda kullanılamaz.

Öte yandan, Anayasanın 20. maddesinin 3. fıkrası gereğince kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Detaylıca açıklandığı üzere, ilgili trafik bilgilerinin BTK tarafından işleneceğine ilişkin herhangi bir yasa maddesi yoktur. Burada bahsedilen **“işleme”** tabiri 6698 sayılı yasada; *“kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi”* ifade edeceği şeklinde (md. 3/1-e) tanımlandığından ve işleme kapsamına **“elde etme”, “depolama”, “muhafaza etme”, “yeniden düzenleme”, “devralma”,** gibi işlemler de girdiğinden, BTK’nın söz konusu işleminin de **“işleme”** olduğunda şüphe yoktur. **BTK’nın bu verileri herhangi bir mahkeme kararı olmadan işleme yetkisi ve görevi olmamasına rağmen, veri sorumlusu işletmelerden elde edip saklamakta, anlamlı tablolara dönüştürüp işlemekte, başka kurumlarla paylaşmakta ve dolayısıyla hukuka aykırı olarak işlemektedir. Hukuka aykırı hale gelen bu verilerin yargılamada kullanılabilmesi mümkün değildir.**

Ayrıca, hukuka aykırı bir şekilde BTK tarafından elde edilen trafik bilgilerinin BTK tarafından nasıl korunduğu, yani güvenilirliklerinin nasıl sağlandığına ilişkin herhangi bir düzenlememe ve güvence de yoktur. Verileri toplama, saklama ve arşivleme yetkisi olmayan BTK’nın, verilerin korunmasına yönelik güvencelerin olması da mümkün değildir. Zira BTK’ya karşı açılan davalarda BTK; **kanunun kişisel verilerin korunmasına yönelik getirdiği yükümlülöklere tabi olmadığını, söz konusu verileri herhangi bir sınırlamaya tabi olmaksızın istediğı koşullarda istediğı süre boyunca saklayabileceğini belirtmektedir.** Bu da, söz konusu trafik verilerinin güvenilirliğini ortadan kaldırmaktadır. Zira, yargı mercileri tarafından verilen iletişimin tespitine yönelik kararlara cevaben BTK; *“...belirtilen tarih aralığında ilgili işletmeler tarafından kurumumuza elektronik ortamda gönderilen kayıtlar esas alınarak hazırlanmış ve ekte sunulmuştur”* demektedir. Bu ifadelerden; ilgili verilerin BTK’nın ilgili işletmeden aldığı kayıtlar üzerinde gerçekleştirdiğı **“hazırlama”** faaliyeti sonucu

oluşturulduğu ve bu nedenle orijinal veriler olmadığı anlaşılmaktadır. Veri bütünlüğü bozulan, başka bir deyişle ham olmayan verilerin delil olarak kullanılması mümkün değildir.

Yapılan bu açıklamalar sadece ilgili verilerin temin ediliş şekliyle ilgili hukuka aykırılıklara ilişkindir. Saklama süresi geçtiği halde silinmeyen trafik verileri ise esasında hukuken var olmaması gereken ve hatta var olmasının cezai ve hukuki yaptırıma bağlandığı verilerdir. Söz konusu veriler, saklama süresinin dolmasıyla birlikte delil niteliğini kaybederler.

4. Avrupa İnsan Hakları Mahkemesi'nin Konuya Yaklaşımı

Avrupa İnsan Hakları Mahkemesi (AİHM), internet trafik verileri, HTS kayıtlarının ya da kişisel veri niteliğindeki bilgilerin saklanması ve imhasıyla ilgili başvuruları, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. maddesi, yani özel yaşam ve aile hayatına saygı hakkı kapsamında incelemektedir ve bu konuda verdiği çok sayıda kararı vardır.

a) Rotaru/Romanya Büyük Daire Kararı

AİHM kararına konu Rotaru/Romanya başvurusunda başvuru, Romanya İstihbarat Teşkilatının (RİT) kendisi hakkında bazıları yanlış ve iftira niteliğinde olan kişisel bilgiler içeren bir dosya tuttuğunu ve kullandığını iddia etmiştir. AİHM, idareye verilen gizli yetkinin kullanıldığı durumlarda keyfilik riskinin daha da arttığını, iletişimin denetlenmesiyle ilgili idareye tanınan kontrolsüz yetkinin denetime açık olmamasının hukuk devleti ilkesiyle bağdaşmadığını ve söz konusu yetkinin kapsamının ve nasıl kullanılacağına açıkça gösterilmesi gerektiğini belirtmiş,³² ancak, başvuruya konu olayda; ulusal hukukta başvuruçunun özel yaşamıyla ilgili bilgilerin RİT tarafından toplanıp kayıt altına alınmasına ve gizli dosyalarda arşivlemesine izin verilmesine rağmen, bu yetkinin kullanımını kısıtlayan bir düzenlemeye, kayıt altına alınacak bilginin türüne, tedbirin uygulanacağı kişi kategorilerine, elde edilen bilgilerin ne kadar saklanacağına ve hangi şartlarda bu tedbire başvurulacağına yer verilmediğini, ayrıca bu yetkinin keyfi şekilde kullanılmasını engelleyecek herhangi bir güvence ve denetimin öngörülmediğini ve takdir yetkisinin

32 AİHM'in Malone/Birleşik Krallık Kararı, B. No:8691/79, 02/8/1984.

kullanımıyla ilgili de bir netlik bulunmadığını belirterek, öngörülen tedbirin “*yasaya uygunluk*” şartını karşılamadığını ve bu nedenle de başvurucunun 8. maddedeki haklarının ihlal edildiğini hükme bağlamıştır.³³

b) Big Brother Watch ve Diğerleri/Birleşik Krallık Kararı

AİHM, Birleşik Krallık İstihbarat Teşkilatına İstihbarat Yetkilerinin Düzenlenmesine Dair Kanun’la verilen, kitlelerin istihbari amaçla toplu dinlenilmesi ve internet servis sağlayıcılarından iletişim bilgilerinin toplu şekilde alınmasına ilişkin yetkiyi, bilgilerin elde edilmesi, filtrelenip ayıklanmasında kullanılan arama kriterleri başta olmak üzere, arama ve seçme süreçlerinde bağımsız denetim mekanizmalarının yetersiz olması, ayrıca inceleme için seçilecek iletişim bilgilerinin kişilerin özel hayatına ilişkin olmasına rağmen bunların ayıklanması aşamasında uygulanan gerçek bir güvencenin bulunmaması ve bilgilere erişim öncesinde bir mahkeme ya da bağımsız idari merci denetiminin öngörülememesi nedeniyle AİHS’in 8. maddesine aykırı bulmuştur.³⁴

c) Benedik/Slovenya Kararı

AİHM kararına konu bir başka olay şöyle gerçekleşmiştir; Slovenya Anayasası’nda iletişimin gizliliğinin bir sonucu olarak, kişilerin iletişim ve kimlik bilgilerinin (internet trafik bilgisi) yalnızca mahkeme kararıyla temin edilebileceği hükme bağlanmış, ancak ceza muhakemesi kanununda adli soruşturma kapsamında polisin hâkim kararına gerek olmadan ilgililerin internet trafik bilgilerini internet servis sağlayıcılardan isteyebileceği düzenlenmiştir. Bir soruşturma kapsamında hâkim kararı olmadan trafik bilgileri polis tarafından elde edilen ve bu bilgilere istinaden tutuklanan bir kişi AİHM’e başvurmuş ve başvurusunda; trafik bilgilerinin mahkeme kararı olmadan elde edildiğini, iletişim bilgileriyle ilgili gizlilik hakkından feragat etmediğini ve bu bilgilerin de özel hayat kavramı kapsamında korunması gerektiğini, iç hukuktaki belirsizlik nedeniyle özel hayatına yapılan müdahaleye karşı kendisine yeterli güvence sağlanmadığını, başvurusuna konu olayda Anayasa

33 AİHM’in Rotaru/Romanya Büyük Daire Kararı, B.No: 23841/95, 04/5/2000, § 56-63.

34 AİHM’in Big Brother Watch ve Diğerleri/Birleşik Krallık Kararı, B. No: 58170/13, 62322/14 ve 24960/15, 13/9/2018, § 465-468.

hükümlerinin uygulanması gerektiğini, zira Anayasa’da iletişim bilgilerinin ancak mahkeme kararıyla verilebileceğinin düzenlendiğini ve bu hususlara uyulmayarak özel yaşam hakkının ihlal edildiğini öne sürmüştür.

AIHM başvuruyla ilgili verdiği kararında, IP adresleriyle ilgili abone bilgilerinin verilmesinin mahkeme kararına tabi olduğunu ve polisin basit bir yazılı talebiyle elde edilemeyeceğini, polise bu bilgileri alma yetkisi veren yasanın dayanağının şekli netlikten yoksun olduğunu, 8. madde ile ilgili keyfi müdahalelere karşı yeterli koruma sağlanmadığını ve başvurucunun özel hayatına saygı hakkına yapılan müdahalenin Sözleşme’nin 8. maddesinin ihlali sonucunu doğurduğunu belirtmiştir.³⁵

d) Ekimdzhiev ve Diğerleri/Bulgaristan Kararı

AIHM, Ekimdzhiev ve Diğerleri/Bulgaristan kararında; Bulgaristan hukukundaki gizli izleme, iletişim verilerinin saklanması ve erişimi için keyfiliğe ve kötüye kullanıma karşı yetersiz yasal güvenceler sağlanması nedeniyle başvuruçuların özel yaşam ve aile hayatının korunması hakkının ihlaline karar vermiştir.³⁶

AIHM’e göre iletişim verilerinin saklanmasını ve daha sonra yetkililerin bu verilere erişimini düzenleyen yasalar, 2015 yılında ABAD’ın Dijital Haklar İrlanda ve Diğerleri davasındaki kararının ardından Anayasa Mahkemesi bunları inceledikten sonra önemli ölçüde iyileştirilmiş olsa da kanunlar, pratikte uygulandığı şekliyle hala, aşağıdaki açılardan Sözleşme’nin 8. maddesi uyarınca gerekli olan keyfilik ve kötüye kullanıma karşı asgari güvencelerden yoksundur:

(a) Yetkilendirme prosedürü, yetkili makamlar tarafından saklanan iletişim verilerine yalnızca “demokratik bir toplumda gerekli olduğunda” erişilmesini sağlamaya yeterli görünmemektedir.

(b) Cezai kovuşturma sırasında yetkililer tarafından erişilen verilerin yok edilmesi için net zaman sınırları belirlenmemiştir.

35 AIHM’in Benedik/Slovenya Kararı, B.No: 62357/14, 24/04/2018, § 128 vd.

36 AIHM’İN Ekimdzhiev ve Diğerleri/Bulgaristan Kararı, B. No: 70078/12, 11/04/2022.

(c) Yetkililer tarafından erişilen iletişim **verilerinin saklanması, erişilmesi, incelenmesi, kullanılması, iletilmesi ve imha edilmesi konusunda kamuya açık kurallar mevcut değildir.**

(d) Denetim sistemi, mevcut düzeni ile kötüye kullanımı etkin bir şekilde kontrol etmek için yeterli görünmemektedir.

(e) Hâlihazırda yürürlükte olan bildirim düzenlemeleri çok dardır ve

(f) Etkili bir hukuk yolunun bulunmadığı görülmektedir.

Sonuç olarak, bu yasalar “*Yasa niteliği*” şartını tam olarak karşılamamaktadır ve Bulgaristan'daki iletişim verilerinin tutulması ve bunlara erişilmesi sisteminin gerektirdiği “*müdahaleyi*” “*demokratik bir toplumda gerekli*” kriterinin kapsamında tutmaktan uzaktır. Dolayısıyla, Sözleşme'nin 8. maddesi bu açıdan da ihlal edilmiştir” (§ § 420- 421).

e) Škoberne/Slovenya Kararı

Karara konu olayda; rüşvet suçundan yürütülen bir soruşturmada ulusal mahkeme, eski bir hakim olan başvuruçunun kullandığı telefona ilişkin iletişim kayıtlarının hizmet sağlayıcılarından istenmesine karar vermiştir. Hizmet sağlayıcıları, mahkemenin talebindeki daha uzun dönem yerine, sadece yasal olarak bu bilgileri **tutmak zorunda oldukları 14 aylık** süreye ilişkin verileri mahkemeye göndermişlerdir. Başvurucu, bu bilgilere dayanılarak mahkum edilmiştir.³⁷

Başvuruçunun özel hayatına müdahale teşkil eden iletişim verilerinin tutulmasının ulusal hukukta yasal bir temelinin bulunduğu ve verilerin bir mahkeme kararına dayanarak alındığında tartışma yoktur (§ 130). Ancak AİHM, yer bilgisinin, iletişim kurulan kişilerin, iletişim örgüsünün belirlenmesi yoluyla kişilerin özel hayatını ilgilendiren bilgilerin sistematik biçimde toplanması ve saklanması temel haklara geniş kapsamlı ve özellikle ciddi bir müdahale oluşturduğunu belirtmiştir (§ 134).

AİHM'e göre, ilgili yasada iletişim bilgilerin hangi amaçlar için tutulduğu belirtilmekle birlikte, bu tedbirin kapsamının ve uygulanışının çerçevesini çizen hükümler yoktur. Tedbirin “*demokratik bir toplumda gerekli olanla*” sınırlı kalmasını sağlayacak hükümlerin veya mekanizmaların bulunmaması AİHS'in 8. maddesiyle bağdaşmamakta ve **bilgilerin tutulma**

37 AİHM'in Škoberne/Slovenya Kararı, B. No: 19920/20, 15/5/2024.

süresinin kayda değer bir süre olan 14 ayla sınırlandırılması da bu sonucu değiştirmemektedir (§ 139).

Mahkemeye göre, iletişim verilerinin tutulmasının 8. maddeye aykırı olduğu durumlarda; bu bilgilere yetkili makamlarca erişilmesi, sonrasında işlenmesi ve saklanması bu maddeyle bağdaşmaz (§ 144). AİHM, başvurunun iletişim verilerinin tutulmasına temel oluşturan yasadaki ilgili hükümlerinin “*yasallık niteliği*” şartını karşılamadığını ve başvurunun 8. madde haklarına müdahaleyi “*demokratik bir toplumda gerekli olanla*” sınırlandıramadığını belirterek; söz konusu iletişim verilerinin tutulmasının, onlara erişilmesinin ve bilgilerin işlenmesinin 8. maddeyi ihlal ettiğine karar vermiştir (§ 147).

f) Borislav Tonchev/Bulgaristan Kararı

Başvuruya konu olayda veri sahibi başvuru, Temmuz 2004’te Bulgaristan’da Ceza İnfaz Kurumu Genel Müdürlüğü’nde gardiyan olarak işe başlamıştır ve bu işe başlayabilmek için adli sicil kaydının temiz olması gerekmektedir. Ancak, başvuru iş başvurusu yaptığı dönem ile işe alınması arasında alkollü araç kullandığı için idari ceza almıştır. Başvuru; 2012 yılında Adalet Bakanlığındaki başka bir pozisyon için başvurmuş, fakat adli sicil kaydına işlenen bu ceza nedeniyle hem başvurusu reddedilmiş hem mevcut işinden çıkarılmıştır.³⁸

Başvuru, adli sicil kaydının **beş yıllık saklama süresine** tabi olduğunu ve süre dolduktan sonra silinmesi gerektiğini belirterek, meslekten çıkarılmasının hukuka aykırı olduğunu belirterek dava açmıştır. Ancak, açtığı dava reddedilmiş, üst mahkeme de bu kararı onamıştır. Başvuru, bunun üzerine Adalet Bakanlığı’nın verilerini yasa dışı işlediğini belirterek Bulgaristan veri koruma otoritesine (CPDP) şikayette bulunmuştur. CPDP, başvuru hakkı bulmuş ve adli sicil verileri beş yıldan fazla saklandığı için para cezası vermiştir. Ancak, bu karar daha sonra iptal edilmiştir.

Başvuru, bu karar üzerine AİHM’e başvurmuş ve verilerinin yasa dışı işlendiğini iddia etmiştir. Mahkeme, verilerin saklanmasıyla ilgili düzenlemelerdeki belirsizlik ve verilerin ne zaman silinmeleri gerektiğine ilişkin bir düzenlemenin bulunmaması nedeniyle yeterince öngörülebilir olmadığını ve bu durumun AİHS’in 8/2 maddesini ihlal ettiğini tespit etmiştir.

38 AİHM’in Borislav Tonchev/Bulgaristan Kararı, B. No: 40519/15, 16/7/2024.

Bulgaristan Adalet Bakanlığı, verilerin süresiz saklanması gerektiğini savunurken, CPDP bu verilerin kayıt kartlarıyla birlikte silinmesi gerektiğini belirtmiştir. AİHM, düzenlemelerdeki belirsizlikleri öngörülebilirlik ilkesine aykırı bulmuştur (§ 130 vd.)

g) Yalçınkaya/Türkiye Kararı

Karara konu olayda başvuru, cezalandırılmasına gerekçe yapılan Bylock haberleşme uygulamasına ilişkin verilerin Milli İstihbarat Teşkilatı (MİT) tarafından bir mahkeme kararı olmaksızın ve ilgili yasal çerçeveyi ihlal ederek toplandığı ve kullanıldığından ve internet trafik verilerinin (CGNAT) BTK tarafından yasal süre sınırı dışında tutulduğundan şikâyetçi olmuştur.³⁹

AİHM, konuyla ilgili Hükümete şu soruları yöneltmiştir; özellikle başvurunun bahse konu verilerin, saklanmaları için kanunda belirtilen azami sürenin ötesine geçen bilgileri içerdiği iddiası dikkate alındığında; başvurunun telefonuna ve internet trafik kayıtlarına ilişkin BTK tarafından sağlanan veriler, ilgili ulusal hukuka uygun şekilde saklanmış ve ortaya konulmuş mudur? İlgili kanunda ve uygulamada, keyfi müdahale ve kötüye kullanıma karşı hangi güvenceler bulunmaktadır?

Başvuruda AİHS'in 6, 7 ve 11. maddelerinden ihlal bulan AİHM, başvurunun şikâyetinin özünde, hukuka aykırı bir eylem sebebiyle özel hayatına yapılan müdahaleden ziyade hukuka aykırı olarak ele geçirildiği iddia edilen Bylock ve internet trafik verilerine dayanılarak mahkûm edilmesinin yer aldığını belirtmiştir (§ 371).

AİHM'e göre, başvurunun 8. maddeye bakan yönü başvurunun kendisi tarafından da tali bir mesele olarak değerlendirilmiştir. Bu durum başvurunun söz konusu delile dayanılarak mahkûm edilmesinin adilliğine yönelik ulusal mahkemeler ve AİHM nezdindeki argümanlarının da anlaşılmaktadır. Yine, Bylock ve internet trafik verileriyle ilgili özel hayata ilişkin hususlar, büyük ölçüde bu delillerin ceza yargılamasında kullanılmasıyla ilgili ileri sürülmüştür (§ 372).

AİHM, başvuran tarafından hukuka aykırı delillere dayanılarak mahkûm edilmesine ilişkin Sözleşme'nin 8. maddesi kapsamında ileri sürdüğü hususların Sözleşme'nin 6 § 1

39 AİHM'in Yüksel Yalçınkaya/Türkiye kararı, 15669/20, 26/9/2023.

maddesi kapsamında incelendiğini ve bu maddeden ihlal verdiğini belirterek, bu şikâyetlerin Sözleşme'nin 8. maddesi açısından kabul edilebilirlik ve esas yönünden ayrı ayrı incelenmesine gerek olmadığına karar vermiştir (§ 373).

5. Çamurşen/Türkiye Kararı

AIHM'in Türkiye ile ilgili verdiği yakın tarihli bir kararı Çamurşen Türkiye başvurusuna ilişkindir. AIHM, başvuruyu AYM'nin Ertan Erçıktı (3) kararına atıfla, yani iç hukuk yollarının tüketilmediğini belirterek kabul edilmez bulmuştur. AYM kararına yapılan vurgu ve aynı gerekçelerle başvurunun reddi nedeniyle, öncelikle AYM kararına ilişkin değerlendirmelere yer verilmesinin uygun olacağı düşünülmüştür.

a) Anayasa Mahkemesi'nin Ertan Erçıktı (3) Kararı

Karara konu olayda başvuru, internet trafik bilgilerinin mevzuatta belirlenen süreden fazla tutulması ve bu bilgilerin ilgili mahkemeye gönderilmesi nedeniyle BTK ve ilgili üç şirket hakkında suç duyurusunda bulunmuştur. Yapılan soruşturma sonunda başsavcılık; başvuru hakkındaki soruşturmanın 2014'te başladığı ve 2015 yılı içinde çeşitli zamanlarda bilgilerin temin edildiği, şirketler için bir yıllık saklama yükümlülüğü olmasına rağmen BTK için böyle bir süre sınırlaması olmadığı ve şirketlerin bilgileri silmesi ya da yok etmesine ilişkin bir yükümlülük ve yaptırım öngörülmediğini belirterek kovuşturmaya yer olmadığına karar vermiştir. Bu kararın kesinleşmesi üzere başvuru AYM'ye bireysel başvuruda bulunmuş; konunun önemini gözetken özenli bir soruşturma yapılmadan ve yeterli gerekçe sunulmadan şikâyeti reddedildiği için özel hayata saygı ve kişisel verilerin korunmasını isteme ile adil yargılanma haklarının ihlal edildiğini ileri sürmüştür.⁴⁰

Başvurucuya göre; BTK internet trafik bilgilerini kendi bünyesinde tutmamakta, soruşturma veya kovuşturma sürecinde talep hâlinde erişim sağlayıcı şirketlerden temin ederek ilgili makama göndermekte ve mevzuata göre erişim sağlayıcı şirketler bu bilgileri en fazla iki yıl saklayabilmektedirler. Yargılandığı mahkemenin talebi üzerine kullandığı cep telefonu numarasına ilişkin 2014-2015 yıllarına ait internet trafik bilgilerini BTK'nın 4/7/2017

40 Başvuru No: 2018/14040, 30/6/2021. <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/14040>

tarihinde göndermesinin, ticari amaçla kurulmuş şirketlerin ilgili mevzuatta belirtilen süreler geçmiş olsa bile hukuka aykırı olarak internet trafik bilgilerini tutmaya devam ettiklerini gösterdiğini belirtmiştir.

Başvurucu, kişisel verilerin ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebileceğini, kendisine ait verilerin depolanmasına ilişkin rızasının olmadığını ve mevzuata göre şirketlerin kişisel verileri süresiz olarak saklama yetkilerinin bulunmadığını söylemiştir. Başvurucuya göre asıl sorun, insanların kişisel verilerinin özel şirketlerce depolanmaya devam edilmesidir ve bu başvuru, üçüncü kişilerin cezalandırılması amacına değil, durum tespitine yöneliktir. Ayrıca, bu ciddi sorunun tazminat davasıyla çözülmesi de mümkün değildir.

AYM, başvurunun amacının hak ihlalinin tespiti, kişisel zararının giderimi ve faillerin cezalandırılması olduğunu ve şikâyet konusu fiilin erişim sağlayıcı şirketler ve BTK'nın kurumsal faaliyet niteliğindeki işlemlerinden kaynaklandığını vurgulamıştır. Aynı şekilde, ceza yargılamasında kasıtlı veya ihmali bir eylem tespit edilmedikçe kurum ve şirket çalışanlarının bireysel olarak ceza sorumluluğundan söz edilemeyeceğini ve kurumsal sorumluluğun da ceza yargılamasına konu olamayacağını belirtmiştir.

AYM'ye göre, başvurunun iddia ettiği kişisel zararların ceza yargılamasıyla giderilmesi mümkün değildir ve idare ve hukuk mahkemeleri bu tür iddiaları inceleme ve hukuka aykırılık veya hak ihlali tespit etme yetkisine sahiptir. Hukuka aykırı bir eylem tespit edildiğinde, kişisel zararların tazmini için manevi tazminata hükmedilebilir. Tazminat yolu hem bireysel hem de kurumsal sorumluluğa dayanılabilir ve hâkim tazminat yanında ek giderim ve tedbire de karar verebilir. AYM, örnek gösterdiği kararlardan; benzer iddiaların hem hukuk hem de idare mahkemelerinde esastan incelendiğini, tarafların yargılamaya etkin bir şekilde katılımı sağladıklarını ve ilk derece mahkemelerinin kararlarının kanun yolu incelemelerine tabi olduğunu belirtmiştir.

AYM, Borçlar Kanunu'nun 58 ve İdari Yargılama Usul Kanunu'nun 11 ve 12. maddelerine göre açılacak tazminat davalarının ceza yargılamasına göre başvurunun amacına daha uygun ve makul bir başarı şansı sunduğu sonucuna varmıştır. Başvurunun tazminat yolunun etkisiz olduğuna dair somut bir iddiasının olmadığını da belirten Mahkeme,

başvurunun başvuru yollarının tüketilmemesi nedeniyle kabul edilemez olduğuna karar verilmiştir.

b) Çamurşen/Türkiye Kararı

Başvurusu AYM tarafından kabul edilmez bulunan başvuru, internet trafik verilerinin öngörülen yasal süreden fazla tutulmasının ve bu verilerin BTK aracılığıyla ceza yargılaması amacıyla ilk derece mahkemesine iletilmesinin özel hayata saygı hakkını ihlal ettiği iddiasıyla AİHS'in 8. maddesi uyarınca şikâyetle bulunmuştur. Başvurucu ayrıca AİHS'in 13. maddesine dayanarak etkili bir iç hukuk yolundan mahrum bırakıldığını da belirtmiştir.⁴¹

AİHM, AYM tarafından yorumlandığı ve uygulandığı üzere, başvuruçunun gibi şikâyetler için en etkili yolun idare ve hukuk mahkemeleri önündeki tazminat yolları olduğunu kaydetmektedir. Mahkeme, Anayasa Mahkemesi tarafından Ertan Erçıktı (3) kararında açıklığa kavuşturulduğu üzere, **benzer meseleleri dile getiren davalarda idare ve hukuk mahkemelerinin yargılamaya etkin şekilde katılabilmiş olan taraflar tarafından öne sürülen iddiaların esasını kapsamlı biçimde incelediğini ve ilk derece mahkemelerinin kararlarının üst mahkemelerin denetimine tabi olduğunu ayrıca kaydetmektedir.** Mahkeme, görevinin ikincil niteliğine önem vererek, bahsedilen yollarla bağlantılı olarak ulusal mahkemeler tarafından gerçekleştirilen incelemenin herhangi bir şekilde sınırlı olacağına ya da açıkça başarısızlığa mahkûm olduğuna işaret eden hiçbir şeyin bulunmadığı görüşündedir. Mahkeme böylelikle, yukarıda belirtilen yollarının etkililiğinden şüphe etmek veya başvuruçuya herhangi bir başarı ihtimali sunamayacaklarına hükmetmek için hiçbir neden görmemektedir (§ 24).

Bu nedenle AİHM, başvuruçunun 2577 sayılı Kanun'un 12. maddesinde ve 6098 sayılı Kanun'un 58. maddesinde düzenlenen idare ve hukuk mahkemeleri önündeki tazmin yollarından yararlanmadığı için iç hukuk yollarını tüketmek için kendisinden beklenebilecek her şeyi yaptığının kabul edilemeyeceğini düşünmektedir (§ 26). Ancak Mahkeme, daha sonrası için bu yolların etkin olup olmadığının incelenmesi seçeneğini açık tutmuştur (§ 27).

41 B. No: 42883/19, 12/11/2024

Sonuç olarak Mahkeme, Hükümetin itirazını kabul ederek AİHS'in 8. maddesi kapsamında yapılan şikâyeti, AİHS'in 35. maddesinin 1. ve 4. fıkraları gereğince iç hukuk yollarının tüketilmemiş olması nedeniyle reddetmiştir.

c) Karara İlişkin Değerlendirme

Çamurşen/Türkiye başvurusu bir grup başvurudur ve aşağıdaki tablodan da anlaşılacağı üzere bu grupta Çamurşen dışında altı başvuru daha bulunmaktadır.⁴² Ancak AİHM, Çamurşen'in başvurusunu ayrıarak reddetmiş, diğer başvurularla ilgili bir karar vermemiştir.

AİHM Başvuru No	Başvuran	Kullanılan İç Hukuk Yolu	AYM Başvuru Tarihi	AYM Karar Tarihi	Kararı Veren AYM Birimi	AYM Karar Gereçesi
42883/19	Metin Çamursen	Savcılık suç duyurusu	7 Ağustos 2018	21 Haziran 2019	3. Komisyon 1. Bölüm	İç hukuk yolunun tüketilmemesi nedeniyle başvurunun reddi
23236/20	Serkan Uslu	Savcılık suç duyurusu	14 Haziran 2019	11 Haziran 2020	3. Komisyon 2. Bölüm	Dayanaktan yoksun/ihlal edilen hak yok
16296/20	Sadık Yayla	Savcılık suç duyurusu	19 Kasım 2018	3 Aralık 2019	3. Komisyon 2. Bölüm	Dayanaktan yoksun/ihlal edilen hak yok
23143/20	Hüseyin Akbulut	Savcılık suç duyurusu	5 Kasım 2018	12 Kasım 2019	1. Komisyon 1. Bölüm	Dayanaktan yoksun/ihlal edilen hak yok
22308/20	Gökhan Yaman	Savcılık suç duyurusu	21 Haziran 2019	9 Temmuz 2019	3. Komisyon 1. Bölüm	Dayanaktan yoksun/ihlal edilen hak yok
16165/20	Hüsmen Koçak	Savcılık suç duyurusu üzerine AYM başvurusu yapılmış. Bilahare 18 Haziran 2019 da idari yargıda tam yargı davası açmış, BiM idare mahkemesi kararını 19 Aralık 2020'de kesin olarak onamıştır.	11 Mart 2019	27 Şubat 2020	2. Komisyon 2. Bölüm	Dayanaktan yoksun/ihlal edilen hak yok
44197/19	Duran Denizci	Savcılık suç duyurusu	24 Haziran 2018	9 Temmuz 2019	3. Komisyon 1. Bölüm	Özel hayat ve adil yargılanma hakkı kapsamında başvuru yapılmış. Özel hayat hakkına ilişkin iddiaların açıkça dayanaktan yoksun olması, adil yargılanma hakkına ilişkin iddialarının da konu bakımından yetkisizliği nedeniyle başvurunun reddine karar vermiştir.

42 <https://hudoc.echr.coe.int/eng?i=001-209418>

AIHM'in Çamurşen başvurusuyla birleştirerek grup yaptığı diğer altı dosyada da başvuranlar önce savcılığa suç duyurusunda bulunup ardından verilen takipsizlik kararı üzerine AYM'ye müracaat etmişlerdir (başvuranlardan biri ayrıca idari yargı yolunu da tüketmiştir). AYM ise bu altı başvuruyu Çamurşen başvurusundan farklı olarak, **"iç hukuk yollarının tüketilmemesi"** nedeniyle değil, **"esastan"**, yani **ihlal edilen bir hak olmadığı gerekçesiyle** kabul edilmez bulmuştur.

d) Tazminat Yolunun Etkin Olduğu Yönündeki Tespitlere İlişkin

AYM gibi AIHM'e göre de başvuru, idare ya da hukuk mahkemelerinde tazminat davası açması gerekirken açmamış ve bu yolu tüketmediği için başvurusu kabul edilmez bulunmuştur. Zira, AYM kararında örnek gösterilen mahkeme kararlarında başvuru konusuyla ilgili benzer iddialar hem hukuk hem de idare mahkemeleri tarafından esasa girilerek ayrıntılı şekilde incelenmiş, tarafların iddia ve savunmalarıyla yargılamaya etkin bir şekilde katılmaları sağlanmış ve ayrıca ilk derece mahkemelerinin kararlarının kanun yolu incelemelerine tabi olduğu görülmüştür. Yani, başvuru, idare mahkemeleri nezdinde etkin şekilde işleyen bir hukuk yolu mevcuttur.

Acaba durum gerçekten böyle midir? AYM'nin örnek gösterdiği üç idari yargı ve bir hukuk mahkemesi kararının hiçbirinde tazminata hükmedilmemiş ve davalar reddedilmiştir. Ayrıca, bu kararların hiçbirinde davacıların şikayetinın esasını oluşturan internet trafik verilerinin saklanma süresinden daha fazla saklandığına ilişkin değerlendirme yapılmamıştır. Etkili olduğu ve tüketilmesi gerektiği belirtilen tazminat yoluna başvuru neticesinde verilen dava ret gerekçeleri şunlardır; telekomünikasyon yoluyla yapılan iletişime ait verilerin adli soruşturma ve kovuşturmalarda Cumhuriyet başsavcılıkları ile mahkemeler tarafından istenilmesi halinde davalı idare tarafından bu taleplerin yerine getirilebilmesi için saklanması yasal zorunluluktur,⁴³ davaya konu olayda tazmini gereken herhangi bir zararın varlığından söz edilemez⁴⁴ ve davalının hukuka aykırı ve kusurlu bir eylemi bulunmadığından sorumlu

43 Ankara 13. İdare Mahkemesinin 14/2/2020 T., 2018/2355 E., 2020/426 K. sayılı kararı.

44 Ankara 2. İdare Mahkemesinin 19/2/2019 T., 2019/1169 E., 2019/2537 K. sayılı kararı.

tutulmasının söz konusu olamaz. Zira davalı BTK, sadece Ağır Ceza Mahkemesi tarafından istenen bilgileri gizli olarak mahkemeye göndermiştir.⁴⁵

Hem AYM, hem de AİHM kararında dikkat çeken bir husus, benzer nitelikte açılan davalarda tazminata hükmedilmese de; *“ilk derece mahkemelerinin kararlarının kanun yolu incelemelerine tabi olduğunu”* hatırlatılması olmuştur. Bu sayede ilk derece mahkemelerinde lehe bir karar çıkmasa da belki istinaf ya da temyiz aşamasında tazminata hükmedilebileceğini belirterek, ihtimal üzerine işlemeyen bir yol etkili bulunmuştur.

Yaptığımız araştırma neticesinde bu konuda lehe verilmiş bir karara rastlamadığımız gibi AYM’nin emsal gösterdiği karar sayısında çok daha fazla aleyhe karara ulaştığımızı belirtmek isteriz. Bu kararlar; *“AYM ve AİHM’in ilk derece mahkemeleri tazminata hükmetmese de istinaf ya da temyiz merci hükmedebilir”* düşüncesinin doğru olmadığını da ortaya koymaktadır. Şöyle ki; AYM’nin emsal gösterdiği kararlardan biri Ankara 2. İdare Mahkemesi tarafından verilmiştir. Bu kararda mahkeme; *“davalı kurumun denetim faaliyetlerini yerine getirme noktasında herhangi bir hizmet kusurunun bulunmadığı açık olup, davacı hakkında Tekirdağ 2. Ağır Ceza Mahkemesince yürütülen ceza yargılamasında, işletmeci (GSM operatörü) tarafından CGNAT kayıtlarının hatalı olarak oluşturulduğuna dair herhangi bir tespitin de bulunmadığı, aksine davacının FETÖ/PDY terör örgütünün örgüt içi kriptolu haberleşme sistemi olarak kullanılan ByLock programına girdiğinin tespit edilmesi sonucunda mahkumiyetine hükmedildiği dikkate alındığında, olayda tazmini gereken herhangi bir zararın varlığından söz edilemeyeceği”* ni belirterek davayı reddetmiştir.⁴⁶ Bu kararın istinaf incelemesini yapan Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesi de istinaf başvurusuna konu idare mahkemesi kararının usul ve hukuka uygun olduğunu ve kaldırılmasını gerektiren bir neden bulunmadığını belirterek **kesin olarak** istinaf başvurusunu reddetmiştir.⁴⁷

AYM’nin tazminat yolunun etkin olduğuna ilişkin örnek verdiği bir başka karara konu olayda davacı, şahsına ait HTS kayıtları, GPRS kayıtları, GSM görüşme kayıtları gibi verilerin yargılanmakta olduğu mahkemeye sunulduğundan bahisle BTK aleyhine hukuka aykırı eylemde bulunulduğu iddiasıyla Ankara 12. İdare Mahkemesinde dava açmıştır. Ankara 12.

45 İstanbul Anadolu 7. Asliye Hukuk Mahkemesinin 15/10/2020 T., 2017/454 E., 2020/212 K. sayılı kararı.

46 Ankara 2. İdare Mahkemesinin 19/2/2019 T., 2019/1169 E., 2019/2537 K. sayılı kararı.

47 Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesinin 30/12/2020 T., 2020/627 E., 2020/1744 K. sayılı kararı.

İdare Mahkemesi; “*uyuşmazlık konusu tazminat talebine esas olan ve silinmesi istenilen kayıtların; ceza hukukunda delil olarak kullanıldığı ve tespit niteliğinde olduğu, idari bir işlem niteliğinde olmadığı ve idari davaya konu edilemeyeceğinden buna bağlı olarak istenen tazminat talebinin de esasının incelenme olanağı bulunmadığı*” gerekçesiyle davanın incelenmeksizin reddine karar vermiştir.⁴⁸

Davacı tarafından istinaf yoluna başvurulması üzerine, Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesi; “*davacı tarafından kişisel verilerinin yasal hükümlere aykırı olarak süresi dışında saklandığı, zamanında silinmemesinin hizmet kusuru oluşturduğu iddialarıyla görülmekte olan davanın açıldığı, dolayısıyla bu işlemler nedeniyle Anayasanın ilgili hükmü ve 2577 sayılı Kanun çerçevesinde tam yargı davası açılmasına engel bulunmadığı anlaşıldığından, İdare Mahkemesince işin esasının incelenerek bir karar verilmesi gerekirken, davanın incelenmeksizin reddi yolunda verilen kararda hukuki isabet bulunmamaktadır*”⁴⁹ diyerek kararın kaldırılmasına ve dava dosyasının yeniden bir karar verilmek üzere mahkemesine gönderilmesine karar vermiştir. Ankara 12. İdare Mahkemesi tarafından yeniden görülen davada bu kez davanın reddine karar verilmiştir.⁵⁰ Davacı tarafından istinaf yoluna başvurulması sonucunda, Ankara Bölge İdare Mahkemesi istinaf başvurusunun reddine **kesin olarak** karar verilmiştir.⁵¹ Yani, AYM ve AİHM’in etkili dedikleri tazminat yoluyla ilgili idare mahkemesi ve istinaf, bu işlemin idari davaya konu dahi olamayacağını ve buna bağlı olarak istenen tazminat talebinin esasının incelenme olanağının da bulunmadığını belirtmişlerdir. Mahkemelerin esasını bile incelemedikleri tazminat yolunun etkili olmadığı izahtan varestedir.

AYM’nin emsal gösterdiği kararlardan bir diğeri olan Ankara 13. İdare Mahkemesi kararının⁵² istinaf incelemesini yapan Ankara Bölge İdare Mahkemesi 10. İdari Dava Dairesi; idare mahkemesinin kararının usul ve hukuka uygun olup kaldırılmasını gerektiren bir neden bulunmadığını belirterek **kesin olarak** onanmasına karar vermiştir.⁵³

48 Ankara 12. İdare Mahkemesinin 13/02/2020 T., 2019/1908 E., 2020/238 K. sayılı kararı.

49 Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesinin 25/6/2020 T., 2020/753 E., 2020/627 K. sayılı kararı.

50 Ankara 12. İdare Mahkemesinin 24/12/2020 T., 2020/1651 E., 2020/2229 K. sayılı kararı.

51 Ankara Bölge İdare Mahkemesinin 18/02/2021 T., 2021/198 E., 2021/222 K. sayılı kararı.

52 Ankara 13. İdare Mahkemesinin 14/2/2020 T., 2018/2355 E., 2020/426 K. sayılı kararı.

53 Ankara Bölge İdare Mahkemesi 10. İdari Dava Dairesinin 11/11/2020 T., 2020/1787 E., 2020/2310 K. sayılı kararı.

Konuyla ilgili açılan bir başka davada Ankara 16. İdare Mahkemesi; “...olayda; yukarıda yer verilen mevzuat uyarınca ilgililerin haklarını ihlal eden bir idari işlem dolayısıyla iptal davası yanında tam yargı davası açabilecekleri açık olmakla birlikte; bakılmakta olan davada iptali istenen HTS kayıtlarının idari davaya konu olabilecek bir işlem niteliğinde bulunmadığından, buna bağlı olarak istenen tazminat talebinin 2577 sayılı İdari Yargılama Usul Kanununun 2. ve 12. maddeleri kapsamında yapılmış bir tazminat istemi olarak nitelendirilemeyeceği sonucuna varıldığından, davanın bu kısmının da esasını inceleme olanağı bulunmamaktadır”⁵⁴ diyerek, başvuruya konu olayın iptal davası yanında tam yargı davasına da konu olamayacağını belirterek reddetmiştir. Bu dosyanın istinaf incelemesini yapan Ankara Bölge İdare Mahkemesi 8. İdari Dava Dairesi; idare mahkemesinin kararının usul ve hukuka uygun olduğunu ve istinaf başvurusunun kabulünü gerektiren bir neden bulunmadığını belirterek **kesin olarak** istinaf başvurusunun reddine karar vermiştir.⁵⁵

Anakara 2. İdare Mahkemesi tarafından verilen bir başka karara konu olayda davacı; ceza mahkumiyetinde esas alınan Bylock isimli haberleşme programına dair verileri içerir HTS kayıtlarının iptali ile maddi kayıplarının hesaplanmasını ve 2.000.000.000,00 TL tazminat ödenmesi istemiştir. Ankara 2. İdare Mahkemesi, **bu davayı bir önceki karardaki gerekçenin (16. İdare Mahkemesinin) aynısıyla**, yani; “olayda; yukarıda yer verilen mevzuat uyarınca ilgililerin haklarını ihlal eden bir idari işlem dolayısıyla iptal davası yanında tam yargı davası açabilecekleri açık olmakla birlikte; bakılmakta olan davada iptali istenen HTS kayıtlarının idari davaya konu olabilecek bir işlem niteliğinde olmadığından, buna bağlı olarak istenen tazminat talebinin 2577 sayılı idari Yargılama Usulü Kanununun 2. ve 12. maddeleri kapsamında yapılmış bir tazminat istemi olarak nitelendirilemeyeceği sonucuna varıldığından, davanın bu kısmının da esasını inceleme olanağı bulunmamaktadır” diyerek reddetmiştir.⁵⁶ İki farklı mahkemenin farklı tarihlerde verdikleri ret kararlarının gerekçelerinin noktası ve virgülüne kadar aynı olması dikkat çekici bir husustur.

54 Ankara 16. İdare Mahkemesinin 29/3/2018 T., 2018/612 E., 2018/768 K. sayılı kararı.

55 Ankara Bölge İdare Mahkemesi 8. İdari Dava Dairesinin 08/10/2018 T., 2018/1320 E., 2018/1198 K. sayılı kararı.

56 Ankara 2. İdare Mahkemesinin 12/4/2019 T., 2019/628 E., 2019/782 K. sayılı kararı.

Bu ilginç durum sadece bu iki mahkemeye özgü de değildir. Zira konuyla ilgili açılmış davaları reddeden Ankara 3.⁵⁷ 12.⁵⁸ ve 23. İdare⁵⁹ Mahkemelerinin ret gerekçeleri birebir aynıdır. Her üç davanın ret gerekçesi şöyledir; “İdarenin hukuki sorumluluğundan söz edilebilmesi için ortada bir zararın bulunması ve bunun idareye yüklenebilen bir işlem veya eylemden doğması, başka bir deyişle zararlar idari faaliyet arasında uygun illiyet bağının bulunması gerektiği, idarenin sorumluluğu hizmet kusuru ve kusursuz sorumluluk ilkelerine dayandığı, ister hizmet kusuru, isterse kusursuz sorumluluk ilkelerine dayandırılınsın, idarenin tazmin borcunun doğabilmesi için bir zararın mevcudiyeti, zarara yol açan eylemin veya işlemin idareye yüklenebilir nitelikte olması ve zarar ile eylem veya işlem arasında illiyet bağının bulunması zorunlu kıldığı, bu şartlardan birinin yokluğu idarenin sorumluluğunu ortadan kaldıracaktır. Diğer bir ifadeyle, ortada bir zarar yoksa veya meydana gelen zararın idari eylem veya işlemle ilgisi bulunmuyorsa, idari faaliyet zararın gerçek nedenini, illiyetini teşkil etmiyorsa, arada illiyet bağı mevcut değilse veya zarara yol açan eylem veya işlem idareye yüklenebilir nitelikte değilse, idarenin sorumluluğu ortadan kalkmaktadır.

Uyuşmazlıkta, yukarıda aktarımı yapılan mevzuat hükümlerinin dava konusu olayla birlikte değerlendirilmesinden, telekomünikasyon yoluyla yapılan iletişime ait verilerin adli soruşturma ve kovuşturmalarda Cumhuriyet Başsavcılıkları ile Mahkemeler tarafından istenilmesi halinde davalı idare tarafından bu taleplerin yerine getirilebilmesi için saklanması yasal zorunluluk olduğu anlaşılmaktadır.

Bu durumda, yasaların uygulanmasından kaynaklanan dava konusu olayda, davalı idareye atfedilebilecek bir hizmet kusurunun bulunmadığı, yine somut olayda davalı idarenin kusursuz sorumluluğuna da gidilemeyeceği anlaşıldığından, davacının manevi tazminat talebinin reddi gerektiği sonuç ve kanaatine varılmıştır.”

Başka bir ifadeyle, kararların hepsi şablon ve “kes-kopyala-yapıştır” şeklinde verilmiştir. Üç ayrı Ankara idare mahkemesinin üç farklı davayı noktası ve virgülüne kadar aynı gerekçeyle reddetmesi, bu davalarla ilgili idare mahkemelerinin tavrını göstermesi adına önemlidir ve bu mahkemelere açılacak tazminat davalarının etkili bir yol olmadığına göstergesidir.

57 Ankara 3. İdare Mahkemesinin 27/11/2019 T., 2019/365 E., 2019/2456 K. sayılı kararı.

58 Ankara 23. İdare Mahkemesinin 24/12/2020 T., .2020/1651 E., 2020/2229 K. sayılı kararı.

59 Ankara 23. İdare Mahkemesinin 3/10/2019 T., .2018/740 E., 2019/353 K. sayılı kararı.

Bu üç davadan Ankara 3. İdare Mahkemesi tarafından verilen kararın istinaf incelemesini yapan Ankara Bölge İdare Mahkemesi 10. İdari Dava Dairesi, istinaf başvurusuna konu idare mahkemesi kararının usul ve hukuka uygun olduğunu ve kaldırılmasını gerektiren bir neden bulunmadığını belirterek **kesin olarak** onamıştır.⁶⁰ Kararın kesinleşmesinden sonra başvuru AYM'ye bireysel başvuruda bulunmuş, özel yaşam ve adil yargılanma haklarının ihlali edildiğini iddia etmiştir. AYM ise özel yaşam hakkına ilişkin şikayeti, Anayasa'da öngörülen temel hak ve özgürlüklere yönelik bir müdahalenin bulunmaması nedeniyle açıkça dayanaktan yoksun, adil yargılanma hakkına ilişkin şikayeti de konu bakımından yetkisizlik nedeniyle kabul edilemez bulmuştur.⁶¹ Bunun üzerine başvuru AİHM'e başvurmuştur ve dosya AİHM önünde derdesttir.

Bu davalardan Ankara 23. İdare Mahkemesi tarafından verilen kararın istinaf incelemesini yapan Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesi, istinaf başvurusuna konu idare mahkemesi kararının usul ve hukuka uygun olduğunu ve kaldırılmasını gerektiren bir neden bulunmadığına karar vermiştir.⁶²

Konuyla ilgili açılan bir başka davada davacı; BTK'nın 26/12/2017 tarihli raporunda 11.480 kişinin irade dışı Bylock Uygulamasının hizmet verdiği sunucu IP'lerine yönlendirildiğine ilişkin idari inceleme sonucu bir değerlendirme yapıldığı ve söz konusu raporda 0532..... numaralı gsm hattının irade dışı Bylock sunucusuna yönlendirilenlere ilişkin sınıflandırma dışında tutulmuş olduğunu, bu hatalı idari işlem nedeniyle kişisel haklarının ihlal edildiğini ve bunun neticesinde mağdur olduğu iddialarıyla söz konusu raporun iptali istemiyle dava açmıştır. Davaya bakan mahkeme, BTK'nın dava konusu raporunun hukuki sonuç doğurmasının ancak bu rapor üzerine tesis edilecek işlemlerle mümkün olduğunu, anılan raporun bu aşamada tek başına davacının hak ve hukukuna etki edici mahiyette bulunmadığından, **kesin ve yürütülebilir nitelikte olmadığını ve bu itibarla görülmekte olan davanın esasının incelenme olanağının bulunmadığını** belirterek davanın incelenmeksizin reddine karar vermiştir.⁶³ Görüldüğü üzere, Hükümetin BTK'nın

60 Ankara Bölge İdare Mahkemesi 10. İdari Dava Dairesinin 25/6/2020 T., 2020/1272 E., 2020/1004 K. sayılı kararı.

61 Anayasa Mahkemesinin 2020/29100 B. Numaralı ve 22/12/2020 tarihli kararı.

62 Ankara Bölge İdare Mahkemesi 7. İdari Dava Dairesinin 16/01/2020 T., 2020/19 E., 2020/32 K. sayılı kararı.

63 Ankara 16. İdare Mahkemesinin 22/5/2018 T., 2018/1032 E., 2018/1153 K. sayılı kararı.

gerçekleştirdiği her türlü işlemin idari işlem olması nedeniyle bu idari işlemten zarar gören kişilerin, idare mahkemeleri önünde tam yargı davası açarak zararın giderilmesini isteyebileceğine ilişkin Çamurşen başvurusunda AİHM'e sunduğu savunmanın (§ 111 ve 112), İdare mahkemesi tarafından benimsenmediği ve *“HTS kayıtlarının idari davaya konu olabilecek bir işlem niteliğinde olmadığı”* gerekçesiyle tazminat davalarının esasının dahi incelenmeksizin reddine karar verildiği anlaşılmaktadır.

Konuyla ilgili tespit edebildiğimiz son karara konu olayda davacı; sanık olarak yargılandığı ceza dosyasında mahkemece BTK'dan istenilen kayıtların 2 yıllık bulundurma süresi dolmasına rağmen BTK tarafından mahkemeye gönderilmesi nedeniyle bu kurum aleyhine maddi ve manevi tazminat davası açmıştır.⁶⁴ Ancak mahkeme, Uyap üzerinden yaptığı inceleme sonucu, davacının İstanbul Anadolu 7. Asliye Hukuk Mahkemesinin 2017/454 esas sayılı dosyasında Turkcel İletişim Hizmetleri A.Ş aleyhine de dava açmış olduğunu tespit ederek her iki davanın birleştirilmesine ve yargılamanın Anadolu 7. Asliye Hukuk Mahkemesinde görülen dava üzerinden devamına karar vermiştir. Anadolu 7. Asliye Hukuk Mahkemesi de yaptığı yargılama sonucu; *“somut olayda davalının hukuka aykırı ve kusurlu bir eylemi bulunmadığı, buna göre sorumlu tutulmasının söz konusu olmadığı, sadece Ağır Ceza Mahkemesi tarafından istenen bilgileri gizli olarak mahkemeye gönderdiği anlaşıldığından davanın reddine dair aşağıdaki şekilde hüküm kurulması netice ve kanaatine varılmıştır”* diyerek davayı reddetmiştir.⁶⁵

AİHM'in Çamurşen başvurusunu reddederken; bu neticenin, ilgili yolların etkililiği ve bilhassa ulusal mahkemelerin kişisel verilerin saklanmasına ilişkin olarak yeknesak ve Sözleşme'yle uyumlu bir yaklaşım geliştirme yeteneği meselesinin daha sonradan incelenmesine hiçbir şekilde halel getirmeyeceğini belirtmiş ve bu yolların etkililiği meselesini tamamen kapatmayıp bu meseleyi tekrar inceleyebileceğine işaret etmiştir. AİHM'den beklenen, AYM'nin örnek gösterdiği, ancak tazminata hükmedilmeyen dört karardan hareketle etkili gördüğü tazminat yoluna ilişkin görüşünden vaz geçmesidir.

e) AYM'nin Çelişkisi; Tazminat Yolu Tüketilmesi Gereken Bir Yol mudur?

64 İstanbul Anadolu 16. Asliye Hukuk Mahkemesinin 29/5/2018 T., 2017/558 E., 2018/209 K. sayılı kararı.

65 İstanbul Anadolu 7. Asliye Hukuk Mahkemesinin 15/10/2020 T., 2017/454 E., 2020/212 K. sayılı kararı.

Çamurşen dışındaki altı dosyada cezai yola başvurulmasını iç hukuk yolunun tüketilmesi için yeterli gören ve bu başvuruları “*esastan*” reddeden AYM, daha sonra sadece cezai başvuru yolunun tüketildiği Ertan Erçıktı (3) başvurusunda, **idari veya adli yargıda tazminat yoluna başvurulmadığını ve dolayısıyla iç hukuk yollarının tüketilmediğini belirterek başvuruyu reddetmiştir.** AYM’nin ve AİHM’in etkin gördüğü hukuk yolları; Borçlar Kanunu’nun 58 ve 72. maddeleri gereğince internet trafik bilgilerinin yasal süreden daha fazla süre saklandığının öğrenilmesinden itibaren 2 yıl ve her halükârda 10 yıl içinde açılacak manevi tazminat veya İYUK’un 12. maddesi kapsamında açılacak tam yargı davasıdır.

Ancak, yukarıda yer verildiği üzere, tazminat yolunun etkin olduğunu ve bu davaların lehe sonuçlandığını gösteren bu zamana kadar verilmiş tek bir karar yoktur. Ayrıca, başvuru sahiplerinin bu başvurulardaki amacı tazminat almak değil, internet trafik verileri ve HTS kayıtlarının saklanması gereken süreden daha uzun saklanması nedeniyle hukuka aykırı delil haline geldiklerinin ve yargılamada kullanılamayacaklarının tespitini sağlamaktır. Aynı şekilde, tazminat hükmedilmesi durumunda da özel yaşam hakkına yapılan müdahale sona ermeyecektir. Zira bu durumda ilgili kişi hükmedilen tazminatı alsa bile imha süresinden daha fazla tutulan internet trafik verilerinin silinmesini bu kararla birlikte kimden isteyecektir?

BTK’dan mı? Önceki bölümde yer verildiği üzere, BTK’nın kendiliğinden verileri isteme ve de gelen verileri tutma yetkisi yoktur. Mevzuat gereğince bu verilerin zaten BTK’da olmaması gerekmektedir. Çünkü BTK “*icracı*” değil, “*aracı*” bir kurumdur ve istenilen bilgileri internet servis sağlayıcılardan alarak adli mercilere iletmekle görevlidir. Yani, BTK’nın bu verileri imha ve ihlali sonlandırma yetki ve görevi yoktur. BTK’ya verilen yetki, internet trafik verileri ve HTS kayıtlarının süresinden daha fazla saklanmalarına engel olmak amacıyla verilmiştir. Ancak, BTK bu yetkiyi veri ve kayıtların imhasını sağlamak için değil, hiçbir yasal dayanağı olmamasına rağmen kendisine gönderilmesi için kullanmaktadır. Başka bir ifadeyle, BTK kendisine verilen yetkiyi açıkça kötüye kullanmaktadır ve ortaya çıkan sorunun nedeni, BTK’nın yetkisi olmamasına rağmen verileri ve kayıtları şirketlerden alıp saklamasıdır.

İnternet servis sağlayıcılardan mı isteyecektir? Hiçbir internet ya da erişim sağlayıcısı verileri saklaması gerekenden daha fazla sakladığını kabul etmeyecek, bu verileri ve kayıtları

BTK'ya gönderdiğini söyleyecektir. Zira verilerin ön gör lenden fazla saklanması TCK'nın 138. maddesinde açıkça suç olarak d zenlendiđi gibi ilgili řirketlerin 5809 sayılı Kanun geređince idari para cezasıyla cezalandırılması g ndeme gelecektir. Dolayısıyla tazminata h kmedilmesi durumunda ihlalin, yani internet trafik verileri ya da HTS'lerin kim tarafından imha edileceđi gibi sorun ortaya  ıkacaktır.       normalde bu verilerin, zaten  nceden imha edilmesi ve hi bir řekilde kullanılmaması gerekirdi. Tam da bu nokta sorunun kaynađı ve on binlerce kiřinin  zel yařam hakkına yapılan m dahalenin sebebi, yetkisi olmamasına rađmen BTK'nın t m veri ve kayıtları d zenli olarak internet servis sađlayıcılar ve iřletmelerden istemesi ve bu řirketlerin de mevzuata aykırı olmasına rađmen, BTK'nin kullandığı kamu g c nden  ekinmeleri nedeniyle bu talebi kabul etmek zorunda kalmalarıdır.

Hukuk yolunun etkinliđiyle ilgili diđer bir sorun, AYM gibi A HM'in de cezai bařvuru yolunu etksiz g rmesidir. Oysa ki TCK'nın 138. maddesinde *“Verileri yok etmeme”* açıkça suç olarak d zenlenmiř ve kanunların belirlediđi s relerin ge miř olmasına karřın verileri sistem i inde yok etmekle y k ml  olanlara, g revlerini yerine getirmemeleri halinde bir yıldan iki yıla kadar hapis cezasıyla cezalandırılacakları  n g r lm řt r. Ayrıca, TCK'nın 139. maddesi geređince bu suç řikayete tabi deđildir. Aynı řekilde, TCK'nın 134. maddesinde *“ zel hayatın gizliliđini ihlal”*, 136. maddesinde de *“Verileri hukuka aykırı olarak verme veya ele ge irme”* suç olarak d zenlenmiř ve bu su ların kamu g revlisi tarafından ve g revinin verdiđi yetki k t ye kullanılmak suretiyle iřlenmesi ađırlatıcı sebeptir.

řikayete konu olayla ilgili, dođrudan TCK'da bir d zenleme varken ve internet trafik verileri ya da HTS kayıtlarının mevzuatta  ng r len s rede imha edilememesi suç olarak d zenlenmiřken, bu yolun etkin kabul edilmeyip, etkili olduđuna ve netice alındığına iliřkin bir  rneđin bulunmadığı tazminat yolunun t ketilmesinin istenmesindeki ısrar nedendir? Kaldı ki, tazminat yolunda ihlalin ortadan kalkması m mk n kabul ediliyorsa, aynı durum cezai bařvuru yolu i in de ge erlidir. Zira bir ceza mahkemesi  ncelikle verilerin  ng r lenden daha fazla saklanıp saklanmadığını tespit edecek ve bu tespitten sonra da verileri silmeyen kiři/ler cezalandırılacaktır. Verilen kararla birlikte trafik verileri ve kayıtların hukuka aykırı řekilde tutulduđu ortaya  ıkacađından, bu verilerin ceza yargılamasında delil olarak kullanılabilmesi de m mk n olmayacaktır. Bu yol sayesinde, hem bařvurucuların  zel

yaşamlarına yönelik ihlal, hem de bu kişiler için daha önemli olan ve cezalandırılmalarına gerekçe yapılan veri ve kayıtların delil kabul edilme durumu ortadan kalmış olacaktır.

Somut gerçeklik bu olmasına rağmen, AİHM sanki AYM kararında örnek gösterilen mahkeme kararlarında davacılar lehine verilmiş bir tazminat varmış gibi hukuk ve idare mahkemeleri nezdinde etkin şekilde işleyen bir hukuki yolun olduğunu söylemiştir. Örnek gösterilen kararlara bakıldığında ya esas dahi incelenmeksizin (idari yargının konusu olmadığı gerekçesiyle) reddine karar verildiği ya da Türk hukukunda trafik bilgisinin en fazla bir yıl süre ile saklanabileceğine ilişkin emredici düzenlemeler içeren 5651 ve 5809 sayılı Kanunlar ile bu yasaların uygulanmasına ilişkin Yönetmelik hükümleri dikkate alınmadan soyut gerekçelerle idarenin ve erişim sağlayıcılarının kusurunun bulunmadığı belirtilerek tazminat taleplerinin reddine karar verildiği anlaşılmaktadır. Görüldüğü üzere, Hükümetin idari yargı ve hukuk mahkemelerindeki tazminat yollarının etkin bir iç hukuk yolu olduğunu gösterme adına Mahkeme'ye sunduğu kararlar dahi, bu yolun pratikte başarı şansı sunan etkin bir iç hukuk yolu olmadığını göstermektedir. Diğer bir ifade ile Hükümet, sunmuş olduğu mahkeme kararları ile Hukuk ve İdare Mahkemesi'ne başvurulmasının, etkin bir iç hukuk yolu olduğunu ispatlayamamış, aksine bu yasa yollarına başvurmanın etkili olmadığını ortaya koymuştur.

Somut olayda kişisel verilerin korunmasını isteme hakkının ihlalinin tespiti ile hukuka aykırı elde edilen bu verilerin ceza yargılamasında delil olarak kullanılmasının engellenmesi bağlamında, tazminat davalarının ceza soruşturmasına göre başvurucunun amacına daha uygun ve makul bir başarı kapasitesi sunmadığı anlaşılmaktadır. Diğer bir ifade ile başvurucunun ihlal iddiaları dikkate alındığında, Hukuk ve İdare Mahkemesi'ndeki tazminat yolunun, ilk bakışta ulaşılabilir ve ihlal iddialarıyla ilgili başarı şansı sunma ve yeterli giderim sağlama kapasitesi bulunmamaktadır.

Aslında aynı durum cezai başvuru yolu için de geçerlidir. Zira 5809 ve 5651 sayılı yasalardaki internet trafik verilerinin silinmesinin zorunluluğu ve TCK'da bunların silinmemesinin suç olarak düzenlenmesine rağmen Çamurşen başvurusuyla birleştirilen altı dosyanın tamamı *"işleme koymama"* kararı ile sonuçlanmıştır. Yani, şikayetler hiç soruşturulmamıştır. Örneğin, 2014-2016 yılları arasındaki internet trafik verilerinin silinmesi gereken süreden sonra mahkemeye gönderildiği için suç duyurusunda bulunulan bir dosyada

Ankara C. Başsavcılığı; şikayetçinin iddiasının yargılandığı davada savunma niteliğinde olduğunu, bu talebin yargılandığı mahkemece değerlendirilmesi gerektiğini ve ortada suçla konu bir eylemin bulunmadığını belirterek dilekçenin işleme konulamamasına karar vermiştir.⁶⁶

Aynı nitelikteki başka bir şikayette verilen işleme koymama kararının gerekçesi daha ilginçtir. Zira Ankara C. Başsavcılığı kararında; 5651 sayılı Yasanın 6. maddesinde internet trafik bilgilerinin iki yıla kadar saklanabileceğinin belirtildiğini, Yönetmelikte bir yıl olarak belirlenmesinin eylemi suç haline getirmeyeceğini, normlar hiyerarşisinde, öncelikle kanunun hükmünün geçerli olduğunu, kaldı ki trafik bilgilerinin belli bir süre saklanmasıdaki amacın bu işlemin erişim sağlayıcı ve yer sağlayıcılarına yüklü miktarda külfet getirmesinden kaynaklı olduğunu, Kanun Koyucunun suç teşkil eden eylemleri ortaya çıkarmaya yönelik olarak iki yıla kadar bu verilerin saklanması zorunlu kıldığını, ayrıca kişisel verileri hukuka aykırı olarak ele geçirmek ve yaymak, hukuka aykırı olarak kişisel verileri kaydetmek suçların kasten işlenmesi gerektiğini, mahkeme talebine cevap mahiyetinde bilgilerin gönderilmesinin kişisel verilerin başkasına verilmesi ve yayma olarak değerlendirilemeyeceğini ve suç teşkil etmeyeceğinin anlaşıldığını belirterek şikayeti işleme dahi koymamıştır.⁶⁷

Oysa ki, TCK'nın 138. maddesinde yapılan düzenleme tam da şikayetlere konu eylemlerin cezalandırılması amacıyla getirilmiştir. Kişisel veri niteliğindeki internet trafik verilerinin silinmesindeki amacın şirketlere daha fazla külfet getirilmemesi olduğunu sanan, şikayete konu olayların özel yaşam hakkının ihlaliyle doğrudan ilgili olduğundan habersiz ve mevzuattaki düzenlemeler yerine şahsi görüşlerine istinaden başvuruları işleme koymayan bir yargı pratiğinde konuyla ilgili etkili bir hukuki yolun varlığından söz edilemez. Tam da bu nedenle, ne mahkemeler ne de savcılıklardan etkili olduğu söylenen tazminat yolu da dahil lehe hiçbir karar çıkmamaktadır.

AIHM'de bilmektedir ki, başta Bylock yargılamaları olmak üzere, on binlerce kişi saklanma süresi geçtiği halde imha edilmeyen internet trafik verileri ve HTS kayıtlarına

66 Ankara Cumhuriyet Başsavcılığının 30/10/2018 T., 2018/19086 soruşturma ve 2018/115623 karar numaralı işleme koymama kararı.

67 Ankara Cumhuriyet Başsavcılığının 28/5/2018 T., 2018/102318 soruşturma ve 2018/63023 karar numaralı işleme koymama kararı.

dayanılarak cezalandırılmıştır ve cezalandırılmaktadır. Başvurucular bu hususu yargılamanın her aşamasında ileri sürmelerine rağmen, talepleri hiçbir şekilde kabul görmemekte ve hatta mevzuatta açıkça düzenlenen bu husus mahkemeler tarafından dikkate alınmamaktadır. Çamurşen başvurusu örneğinde olduğu gibi başvurucuların son çare olarak müracaat ettiği AİHM, yukarıda yer verildiği üzere, yapılan başvuruyu reddedebilmek için iptal ettiği kanun maddesini bile “*ilgili hukuk*” adı altında kararına yazan AYM’nin gerekçelerine atıfla yapılan başvuruyu reddetmiştir.

Kısaca, AİHM’in tüketilmesini istediği tazminat yolu kesinlikle etkin değildir ve yukarıda yer verilen kararlardan da anlaşılacağı üzere, mahkemeler bu konuda tazminata hükmetmemek için ellerinden geleni yapmaktadır. Tüm bunlara rağmen AİHM, Çamurşen kararında işlemeyen tazminat yolunun tüketilmesini istemiştir. Burada akla, AİHM’in Çamurşen grubundaki altı dosyayı da bu karara atıfla reddetmek için mi ayırdığı sorusu gelmektedir.

f) Çamurşen Başvurusundan Ayrılan Dosyayla İlgili AİHM’in Tavrı Ne Olacaktır?

Çamurşen kararıyla ilgili ortaya ilginç ve eleştiriye hak eden bir durum ortaya çıkmıştır. Zira, Çamurşen başvurusunun iç hukuk yollarının tüketilmemesi nedeniyle reddedilmesine ve diğer altı dosyanın başvurucularının da sadece cezai başvuru yolunu tüketmelerine rağmen AİHM’in, AYM’nin bu başvuruları aynı sebeple değil de hak ihlali olmadığı gerekçesiyle reddettiğini görmezden gelmesidir. Eğer, yalnızca cezai yolun tüketilmesi etkin değilse, AYM niçin Çamurşen dışındaki altı başvuruyu bu neden yerine “*esastan*” reddetmiştir? AİHM, cezai yolun tüketilmesinin AYM tarafından yeterli görüldüğünü bilmesine rağmen, bu dosyayı ayırma gereği duyarak karar vermeyi ve diğer dosyaları bekletmeyi uygun görmüştür.

AİHM’in bu konuyla ilgili eleştiriye açık ilk kararı şüphesiz Yüksel Yalçınkaya/Türkiye başvurusuna ilişkindir. Zira aynı hususların dile getirildiği bu başvuruda Hükümete iç hukuk yollarının tüketilip tüketilmemesiyle ilgili soru dahi yöneltmeyen AİHM, adil yargılanma hakkı kapsamında verdiği ihlali gerekçe göstererek, 8. madde kapsamında yapılan başvuruyu inceleme gereği dahi duymamıştır. Eğer Yalçınkaya başvurusunda bu konu incelse açıkça hukuka aykırı olan bu hususla ilgili ihlal verilecek ve on binlerce kişiyi doğrudan ilgilendiren bu yargı pratiğinin hukuksuzluğu hüküm altına alınacaktı. Ancak, AİHM kolay yolu seçmiş ve sanki adil yargılama kapsamında yaptığı incelemede internet trafik verilerinin elde edilmiş

yönteminin hukuka aykırı olduğunu söylemiş gibi bu verilerin hukuka aykırılığının en önemli göstergesini, yani 8. madde kapsamında ileri sürülen hususları görmezden gelmiştir.

AİHM, adil yargılanma hakkı kapsamında yaptığı değerlendirmede bu tespiti yapmış olsaydı 8. maddeye ilişkin ihlal iddialarını incelememesi belki kabul edilebilirdi. Fakat AİHM, hem adil yargılanma hakkı kapsamında yaptığı incelemede somut ve net bir şey söylemeyip internet trafik verilerinin savcılığa tesliminden önceki dönemde veri bütünlüklerinin korunmasıyla ilgili şüphe sebeplerinin bulunduğunu belirtmekle yetinmiş; hem de bu şüphe sebepleri kadar önemli olan verilerin daha fazla saklanmaları nedeniyle hukuka aykırı hale geldiklerinin tespiti anlamına gelecek incelemeden kaçınmıştır.

Çamurşen kararından sonra merak edilen husus, AYM'nin iç hukuk yollarının tüketilmemesi yerine esastan, yani ihlal edilmiş bir hak olmadığı gerekçesiyle kabul edemez bulduğu altı dosyada AİHM'in tavrının ne olacağı ve nasıl bir karar vereceğidir. Bu dosyalarda AİHM'in, AYM gibi esastan bir inceleme yaparak özel yaşama saygı hakkının ihlaline karar vermesi beklenmektedir. Aşağıda, AİHM'in bu hak kapsamında ihlal vermesinin en önemli gerekçesi olması beklenen kanunilik unsuruna ilişkin açıklamalara ve iç hukuktaki mevzuat ve uygulamanın neden bu unsuru karşılamadığına yer verilmiştir

Özel yaşama saygı hakkının unsurlarından biri olan haberleşme hürriyeti Anayasa'nın 22. ve AİHS'in 8. maddesinde düzenlenmiş olup, bu hakla ilgili olarak Anayasa'da; *"herkes haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır"*, AİHS'te de; *"herkes haberleşmesine saygı gösterilmesi hakkına sahiptir"* ifadelerine yer verilmiştir.

Bu hak, kişilerin engellenmeksizin ve sansüre uğramaksızın diğer kişilerle iletişim kurma hakkını güvence altına alır ve bu güvenceye haberleşmenin gizliliği de dâhildir. AİHM, hakkın kapsamını belli iletişim araçlarıyla sınırlamamış, telefon, mektup, faks ve internet vasıtasıyla gerçekleştirilen her türlü haberleşmeyi içine alacak şekilde geniş yorumlamıştır. Mahkeme, aranan telefon numaralarını, telefonla, e-postayla ve internet kullanımıyla ilgili kişisel bilgileri, başvurusunun iş ilişkilerine ait soruşturma mercileri tarafından bir kartta saklanan bilgileri, kamuya açık uzak geçmişiyile ilgili yetkililer tarafından saklanan bilgileri ve başvurusunun kendi çevrim içi etkinliğiyle ilgili kimliğini koruması konusundaki menfaatlerini *"özel yaşam"* kavramı içinde ve dolayısıyla 8. madde kapsamında görmektedir. Ayrıca mahkeme, belli bir zaman için tahsis edilmiş dinamik IP adresiyle ilişkili abone bilgilerinin kamuya açık olmadığını

ve bu nedenle geleneksel telefon rehberinde veya hükümet tarafından tescil edilen araç plakaları gibi kamuya açık veri tabanında bulunan bilgilerle mukayese edilemeyeceğini ve bu gibi depolanmış verilerin kullanımının başlı başına özel yaşama müdahale oluşturabileceğini belirtmiştir.⁶⁸

Bu hak mutlak haklardan, yani AİHS'in 15. maddesinde kullanımı durdurulamayacak haklardan olmayıp, şartların varlığı halinde hakka müdahale edilebilir. AİHS'in 8/2. maddesinde hakka yapılacak müdahaleyle ilgili olarak; *"Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzeninin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir"* ifadesine yer verilmiş, Anayasa'nın 22/2. maddesinde de; milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden bir veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı bulunması halinde haberleşmenin engellenebileceği ve gizliliğine dokunulabileceği belirtilmiştir.

Madde metinlerinden anlaşılacağı üzere, hakka yapılacak müdahaleyi haklı kılacak hususlar; müdahalenin hukuken öngörülmüş olması (hukukilik), meşru bir amacının bulunması ve demokratik toplumda gerekli olmasıdır. AİHM, başvurularda bu şartların varlığını sırayla incelemekte ve hukukilik şartı gerçekleşmemişse diğer şartların varlığını araştırmamaktadır.

Hukukilik şartı Sözleşme'nin 8., 9., 10. ve 11. maddelerinin ortak ögesi olup, hakkın kullanılmasına ilişkin müdahalenin iç hukukta bir dayanağının bulunmasını gerektirir. Davalı ülke, hakka yaptığı müdahale için kendisine yetki veren bir hukuk kuralının varlığını göstermelidir.⁶⁹ Bu kuralın kaynağı yazılı hukuk, yani Anayasa, yasa, KHK, tüzük ve yönetmelik olabileceği gibi, içtihat hukuku da olabilir. Başka bir ifadeyle, AİHM hukuk kavramını biçimsel değil, maddi anlamıyla yorumlamaktır.⁷⁰

68 AİHM'in Benedik/Slovenya Kararı § § 104-108.

69 AİHM'in Silver ve Diğerleri/Birleşik Krallık Kararı, B.No:5947/72, 25/3/1983, § 86.

70 AİHM'in Malone/Birleşik Krallık Kararı, B.No:8691/79, 02/8/1984, AİHM'in Sunday Times/İngiltere Kararı, B.No:6538/74, 26/4/1979, § 47.

Hukukilik denetimi; müdahalenin dayanağı olan düzenlemenin erişilebilir, doğuracağı sonuçların öngörülebilir şekilde açık olmasını ve kötüye kullanmaya karşı da teminatlar içermesini gerektirir.⁷¹

Erişilebilirlik kriteri gereğince, müdahalenin dayanağını oluşturan hukuki düzenleme yayımlanarak ulaşılabilir hale getirilmeli ve ilgililer belli bir olaya uygulanacak hukuk kuralı hakkında gerekli ve yeterli bilgiye sahip olmalıdır.⁷² Öngörülebilirlik kriteri gereğince de, iç hukuk müdahaleye esas teşkil eden tedbire hangi durumlarda ve hangi nedenlerle başvurulabileceğine ilişkin yeterli açıklıkta olmalıdır. Bu açıklık, müdahale edilen hakkın ve uygulanan tedbirin niteliğine, hukuki düzenlemenin içeriğine, düzenlediği alana, ilgilendirdiği kişilerin statüsü ve sayısına göre değişiklik gösterebilir.⁷³

Hukuki bir dayanağının bulunması, erişilebilir ve öngörülebilir olması yapılan müdahalenin hukuki olarak kabulü için yeterli değildir ve mevcut hukukun aynı zamanda keyfi müdahalelere karşı teminatlar da sunması gerekir.

Kanuniliğin unsurlarından olan, mevcut hukukun aynı zamanda keyfi müdahalelere karşı teminatlarda sunması gerekir şartı, mevcut ve benzer dosyalarda hiçbir şekilde karşılanmamaktadır. Zira bu amaçla getirilen verilerin saklanma sürelerine BTK kendisi riayet etmemektedir. Konuyla ilgili AİHM'n yakın zamanda verdiği **Skoberne/Slovenya** kararında koyduğu ilkeler Çamurşen başvurusundan ayrılan dosyaları da yakından ilgilinedirmektedir. Bahse konu kararda ihlal tespit eden AİHM, ilgili hizmet sağlayıcının internet trafik verilerini Kanunda öngörülen on dört aylık yasal süre boyunca sakladığını ve yetkililere yalnızca bu süre zarfındaki verileri teslim ettiğini belirterek, söz konusu müdahalenin yürürlükteki yerel hukuka uygun olduğunu belirterek kanunilik açısından yapılan müdahalede bir sorun görmemiştir (§ 130).

AİHM'e göre Slovenya Yasası, bu konuda herhangi bir kararı Devletin veya Devlet dışı kuruluşun takdirine bırakmamıştır ve uygulaması konusunda belirsiz değildir. Slovenya'daki telekomünikasyon sağlayıcılarının hizmetlerini kullanan her birey veya kuruluş, telekomünikasyon verilerinin kapsamlı veri toplamının bir parçası olarak saklandığını tahmin

71 AİHM'in PG ve JH/Birleşik Krallık Kararı, B.No: 44787/98, 25/9/2001.

72 AİHM'in Silver ve Diğerleri/Birleşik Krallık Kararı, § § 87-88.

73 AİHM'in Sunday Times/İngiltere Kararı, § 49.

edebilir. Ancak, telekomünikasyon verilerinin **genel ve ayırım gözetmeksizin saklanması belirleyen yasanın belirsizliği, hukukun üstünlüğü ve orantılılık ilkelerine uygunluğunun yeterli bir garantisini oluşturduğu şeklinde yorumlanamaz** (§ 138).

Mahkeme, Slovenya'da değiştirilen 2004 Yasası'nın telekomünikasyon verilerinin saklanması gereken bir dizi amacı belirlediğini, ancak bu amaçlara ulaşmak için gerekli olanla ilgili olarak önlemin kapsamını ve uygulamasını sınırlayan hiçbir hüküm içermediğini belirtmektedir. Mahkemenin içtihatları uyarınca, asgari gereklilerin bir parçası olarak ulusal mevzuatın, ilgili inceleme şekline uygun bir tarzda bahse konu tedbirin uygulanmasının kapsamını tanımlaması ve böyle bir tedbire hükmedilmesi ve/veya gerekli olanın sınırlarında tutma amacıyla bunun gözden geçirilmesi için uygun usuller getirmesi gerekmektedir. Somut olaydaki müdahalenin niteliği dikkate alındığında; bu asgari gerekliliklerin, iletişim verilerinin tutulmasını gerektiren bir tedbir halinde de karşılanması gerekmektedir. Tedbirin, 2004 sayılı Yasa'da sayılan belirli amaçlar açısından *“demokratik bir toplumda gerekli”* olanla gerçekten sınırlı kalmasını amaçlayan hükümlerin veya mekanizmaların yokluğu, böyle bir rejimi devletin 8. madde altındaki yükümlülükleriyle bağdaşmaz hale getirmektedir. Verilerin tutulmasının kayda değer bir süre olan yalnızca 14 ayla sınırlandırılması bu sonucu değiştirmemektedir (§ 139).

Bu dosyada başvuru, verilerinin haksız yere saklanması nedeniyle, bunların yerel yargılamalarda elde edilmesinin ve kullanılmasının 8. maddeyi ihlal ettiğini ileri sürmüştür. AIHM'e göre, telekomünikasyon verilerinin saklanmasının *“hukuk niteliği”* gerekliliğine ve/veya orantılılık ilkesine uymadığı için 8. maddeyi ihlal ettiği tespit edildiğinde, bu verilere erişimin -ve daha sonra yetkililer tarafından işlenmesinin ve depolanmasının- aynı nedenle 8. maddeye aykırı olacaktır. Bu bağlamda ABAD'ın görüşüne atıfta bulunan AIHM, iletişim verilerinin ciddi suçlarla mücadele amacıyla genel ve ayırım gözetmeksizin alıkonulamayacağına ve dolayısıyla bu tür verilere erişimin aynı amaçla haklı gösterilemeyeceğini belirtmiştir (§ 144).

Başvurucunun şikayeti, kolluk kuvvetleri tarafından elde edilen ve daha sonra söz konusu ceza davasının amaçları doğrultusunda işlenen, saklanan ve incelenen on dört aylık bir döneme ilişkin verilerinin tamamıyla ilgilidir. Bu kadar çok verinin sözleşmeye dayalı amaçlarla tutulamayacağı ve tutulmadığı, bunun yerine Mahkeme'nin yukarıda Sözleşme'nin

8. maddesini ihlal ettiğini tespit ettiği genel ve geliş güzel bir saklama rejiminin bir parçası olarak tutulduğu tartışmasıdır. (145)

Sonuç olarak AİHM, başvuranın telekomünikasyon verilerinin alıkonulmasına dayanak teşkil eden Kanunu'nun itiraz edilen hükümlerinin “*kanun niteliği*” gerekliliğini karşılamadığını ve başvuranın 8. madde kapsamındaki haklarına yapılan “*müdahale*” “*demokratik bir toplumda gerekli*” olanla sınırlayamadığını tespit etmiş ve telekomünikasyon verilerinin saklanması, erişimi ve işlenmesinin Sözleşme'nin 8. maddesini ihlaline neden olduğunu belirtmiştir. 14 aylık saklama süresinden daha fazla ve keyfi şekilde verilerin sınırsız şekilde saklandığı bir uygulamanın kanun niteliğinde olmadığı ve ilgililerin özel yaşam haklarını ihlal ettiği izahtan varestedir. Şöyle ki;

AYM kararına konu Ertan Erçıktı (3) başvurusunda, başvurucunun özel yaşama saygı hakkına yapılan müdahalenin kanuni dayanağı olsa da, AİHM'in Skoberne/Slovenya kararından sonra hakka yönelik önleyici bir mekanizma olarak görmeyeceği düşünülen, verilerin imhası için öngörülen 2 yıllık süreyi bizzat BTK işlemez hale getirmiş ve hak ihlaline kendisi neden olmuştur. Zira önceki bölümlerde yer verildiği üzere, özel yaşam hakkına açıkça müdahale teşkil eden ve BTK'ya kişisel verileri hakim kararı olmadan isteyip, saklayabilme ve işleyebilme yetkisi veren 5651 sayılı Kanun'un 3. maddesinin 4. fıkrası, 5. maddesinin 5. fıkrası ve 6. maddenin 1. fıkrasının (d) bendi AYM tarafından iptal edilmiştir. Mevzuattaki düzenlemeler gereğince, BTK'nın servis sağlayıcılardan internet trafik bilgilerini bir mahkeme kararı olmadan alabilmesi ve tutabilmesi mümkün değildir. Ancak, BTK mahkeme kararı olmadan saatlik olarak bu verileri almakta, servis sağlayıcılar tarafından 06/11/2016 öncesinde 1, sonrasında da 2 yıl sonra imha edilmesi gereken veriler imha edilemeyip bizzat BTK tarafından saklanmakta ve daha sonra talep üzerine mahkemelere gönderilen bu verilerle kişiler cezalandırılmaktadır. Bu yönüyle, mevzuatta öngörülen prosedür, tıpkı Slovenya'daki gibi geliş güzel bir saklama rejiminin parçasıdır ve bu düzenlemenin kanunilik şartını karşıladığını söylemek mümkün değildir.

Bu durumda farkında olan ve kanunda öngörülen sürelerden daha fazla internet trafik verilerinin saklandığını, hatta hiç imha edilmediğini bilen AYM, Ertan Erçıktı (3) kararının “*ilgili mevzuat*” başlığı altında yer verdiği 5809 sayılı ve 5651 sayılı Kanunlarla ilgili düzenlemelerle; BTK'ya geniş yetkiler verildiğini, BTK'nın veri saklama yetkisinin yasal

dayanağı bulunduğunu ve trafik verilerini saklama süresinin internet erişim sağlayıcılar için geçerli olup BTK için süre sınırlaması olmadığını ispata çalışmıştır.

Bunu doğrulayan ilk husus, 5809 sayılı Kanun'un 6/1-ı maddesindeki *"elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak"* şeklindeki düzenlemeye kararda yer vermesi olmuştur. Daha önce de değinildiği üzere, bu madde lafzından ilk başta BTK'nın görevi kapsamında her türlü bilgi, belge ve veri alabileceği anlaşıyor olsa da Kanun BTK'ya bu yetkiyi vermemektedir.

Nitekim, söz konusu düzenlemeyi inceleyen Anayasa Mahkemesi;⁷⁴ kuralların anlam ve kapsamının belirlenmesinde yukarıda belirtilen kuralların bir bütün olarak göz önünde bulundurulması gerektiğini, anılan maddede Kuruma siber güvenliği sağlama görevi verildikten sonra, söz konusu hükmü izleyen fıkrada BTK'nın *"...görevi kapsamında..."* ilgili yerlerden bilgi, belge, veri ve kayıtları alabilmesinin, değerlendirmesini yapabilmesinin, arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilmesinin, bunlarla irtibat kurabilmesinin ve bu kapsamda diğer gerekli önlemleri alabilmesinin veya aldırabilmesinin öngörüldüğünü; BTK'ya tanınan bu yetki ve imkânların, BTK'nın **siber güvenliğin sağlanması göreviyle sınırlı olduğunu**, öte yandan aynı maddenin devamında BTK'nın maddedeki görevleriyle ilgili taleplerinin yerine getirilmesinin zorunlu olduğu belirtilirken *"...bu maddedeki görevleri ile ilgili..."* ibaresine yer verilmesi ve siber güvenliğin sağlanması görevinin verildiği hükme atıfta bulunulması dava konusu kuralların yukarıda belirtilen anlam ve kapsamını teyit ettiğini söylemiştir.⁷⁵

Kısaca, **BTK'nın söz konusu yetki ve görevi, siber güvenliğin sağlanması göreviyle sınırlıdır.** BTK, bu madde kapsamında da kişisel veri niteliğinde olan trafik bilgilerini kaydetme, ilgili kurum veya kuruluşlardan isteme, saklama ve arşivleme görev ve yetkisi yoktur. Somut gerçeklik bu olsa da AYM bu konuda daha önce bir değerlendirmede bulunmamış gibi bu düzenlemeyle BTK'ya her türlü bilgi ve belgeyi isteyebilme yetkisi verildiği izlenimi doğurmuştur.

74 Anayasa Mahkemesinin 24/7/2019 T., 2017/16 E., 2019/64 K. sayılı kararı; <https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2019/64?EsasNo=2017%2F16>

75 AYM, E.2017/16, K.2019/64, 24/07/2019, § 38-39

Kararla ilgili daha ilginç ve sıkıntılı durum ise 5651 sayılı Kanunun erişim sağlayıcıların; *“Kurumun talep ettiği bilgileri talep edilen şekilde Kuruma teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla”* yükümlü olduklarını belirten 6/1-d maddesine AYM’nin kararda yer vermiş olmasıdır. Oysa ki AYM, bu maddeyi 08/12/2015 tarihinde şu gerekçeyle iptal etmiş ve madde 28/01/2017 tarihinde yürürlükten kalmıştır; *“...bu çerçevede iptali istenilen kurallarda, TİB’in (BTK) hangi koşullarda ve hangi gerekçelerle istediği bilgilerin içerik, yer ve erişim sağlayıcılar tarafından Başkanlığa teslim edileceğine ya da verilen bilgilerin ne kadar süre ile TİB’de saklanacağına, talep edilen bilgilerin mahiyetine, içerik, yer ve erişim sağlayıcılara bildirilecek tedbirlere ilişkin herhangi bir belirlilik bulunmamaktadır. Kurallar bu yönleriyle belirli ve öngörülebilir değildir. Anayasa’da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin konu, amaç ve kapsam bakımından yeterli sınırlamaya tabi kılınmaksızın koşulsuz olarak TİB’e verilmesine imkân tanımakta, böylece kişiler idareye karşı korumasız hale getirilmektedirler. Dolayısıyla iptali istenilen kurallar, belirli ve öngörülebilir olmadığından kişilerin kişisel verilerin korunması hakkını ölçsüzce sınırlandırmakta ve Anayasa’nın 20. maddesine aykırılık teşkil etmektedir. Açıklanan nedenlerle kurallar, Anayasa’nın 2., 13. ve 20. maddelerine aykırıdır.”*⁷⁶ AYM’nin kendi iptal ettiği maddeye hala yürürlükteymiş ve bu maddeye dayanarak BTK’nın talep ettiği belge ve bilgiler ilgili kuruluşlarca gönderilmeliymiş gibi kararda yer verilmesinin hukuken bir izahı yoktur.

Hükümet de BTK’nın CGNAT verilerini kanunda öngörülenden daha uzun süre sakladığı iddiasına ilişkin olarak AİHM’e sunduğu savunmada (Hükümet savunması § 71), 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun’un ve bu kanunun uygulanmasını gösterir İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik’in hükümlerinin özel hukuk hükümlerine göre kurulmuş ve faaliyet gösteren yer sağlayıcıları, erişim sağlayıcıları ve içerik sağlayıcılara ilişkin olduğunu, erişim sağlayıcıların internet trafik bilgilerini sadece bir yıl tutmakla yükümlü olduğunu, 5651 sayılı Yasa ile Yönetmeliğin bir kamu kurumu olan BTK’ya herhangi bir yükümlülük yüklenmediğini iddia etmiştir.

76 Anayasa Mahkemesinin 08/12/2015 T., 2014/87 E., 2015/112 K. sayılı kararı.

Hükümetin görüşünde de yazıldığı üzere, (uygulamada) ceza yargılaması sırasında mahkemeler CGNAT kayıtlarını (trafik bilgilerini) BTK'dan istenmekte, BTK da mahkeme kararını erişim sağlayıcılara göndererek bu verilerin kendisine gönderilmesini istemektedir. BTK, CGNAT kayıtları (trafik bilgileri) erişim sağlayıcılardan geldiğinde, Bylock örneğinde olduğu gibi kişilerin Bylock sunucusuna bağlantı yapıp yapmadıklarına ilişkin sorgulama yapmakta ve sorgu sonucunu tabloya dönüştürüp ilgili mahkemeye göndermektedir. (BTK verileri aynen göndermiyor, kişilerin bylock serverinin İp adreslerine bağlı olup olmadığına dair sorgulama yapıp sorgu sonucunu tabloya donusturup verileri bu şekilde işleyerek gönderiyor) Hal böyle iken, Hükümetin bir taraftan CGNAT kayıtlarını (trafik bilgilerini) mahkemelerin CMK'nın 135. maddesi kapsamında erişim sağlayıcılardan değil BTK'dan istediklerini, bu nedenle erişim sağlayıcıların belirtilen sürelerden daha uzun süre bu bilgileri saklayıp saklamadıklarını incelemenin bir anlamının olmadığını iddia ederken, diğer taraftan internet trafik bilgilerinin sadece bir yıl tutulmasına ilişkin yasal düzenlemelerin özel hukuk hükümlerine göre kurulmuş ve faaliyet gösteren yer sağlayıcılar, erişim sağlayıcılar ve içerik sağlayıcılara ilişkin olduğunu, 5651 sayılı Yasa ile Yönetmeliğin bir kamu kurumu olan BTK'ya herhangi bir yükümlülük yüklenmediğinin iddia edilmesi çelişki oluşturmaktadır. Ayrıca Hükümet bu görüşü ile erişim sağlayıcıların internet trafik bilgilerinin sadece bir yıl tutulmasına ilişkin yasal düzenlemelere de uymadığını kabul etmiştir.

Hükümet, 5651 sayılı Yasa'nın 1. maddesindeki tanımdan hareketle 5651 Sayılı Yasa'nın 6/1.b maddesi ve bu yasaya dayanılarak çıkartılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in erişim sağlayıcıların yükümlülüklerini düzenleyen 8/1.b maddesindeki; *"...sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla,* cümlesindeki 1 yıllık sürenin erişim sağlayıcıları bağladığını, diğer bir ifadeyle bu sürelerin BTK'yı bağlamadığını iddia etmişti. Ancak, bu Yönetmelik hükmü Danıştay Onüçüncü Dairesi tarafından iptal edilmiş⁷⁷ ve iptal kararı Danıştay İdari Dava Daireleri Kurulu'nun onamasıyla kesinleşmiştir.⁷⁸ Dolayısıyla,

77 Danıştay 13. Dairesinin 12/12/2019 T., 2013/239 E., 2019/4266 K. sayılı kararı.

78 Danıştay İDDK'nın 24/2/2022 T., 2020/1851 E., 2022/649 K. sayılı kararı.

Hükümetin iddialarının hukuki bir temeli ve karşılığı yoktur. BTK'ya internet trafik verilerini, alma, saklama ve imha yetkisi veren hiçbir yasal düzenleme bulunmamaktadır. Özel yaşam hakkına yapılacak müdahaleleri engellemek amacıyla kurulan BTK, kendisine verilmiş bir yetki olmamasına rağmen, kişisel verileri işletmelerden almakta, yıllarca tutmakta ve mahkeme göndermek suretiyle ilgililerin özel yaşam haklarını açıkça ihlal etmektedir. Mevcut durum itibarıyla, konuyla ilgili düzenlemeler kişisel verileri korumaya yönelik bir teminat içermemekte ve hiçbir şekilde kanunilik unsurunu karşılamamaktadırlar.

6. AİHM Hangi Madde(ler) Kapsamında İnceleme Yapacak ve Karar Verecektir?

Konuyla ilgili merak edilen bir diğer husus, AİHM'in Çamurşen dosyasından ayırdığı altı dosyada incelemeyi hangi hak/lar kapsamında yapıp karar vereceğidir. Zira başvuruçular ağırlıklı ve öncelikli olarak özel yaşam haklarının ihlalini iddia etseler de; gerekçeli karar hakkının, yani adil yargılanma haklarının ihlali iddiasında da bulunmuşlardır. Bu konuda da AİHM'in **Skoberne/Slovenya** kararında ortaya konulan ilkeler bu sorunun cevabı olacak niteliktedir.

Bu karara konu olayda başvuruçular, verilerinin haksız yere tutulması nedeniyle, bu verilerin elde edilmesinin ve iç hukuk yargılamalarında kullanılmasının 8. maddeyi ihlal ettiğini ileri sürmüştür. AİHM, iletişim verilerinin tutulmasının "*yasa niteliği taşıma*" ve/veya orantılılık şartına aykırılık nedeniyle Sözleşme'nin 8. maddesini ihlal ettiği tespit edildiğinde; bu verilere erişim ve yetkililerin sonrasında bunları işlemekten geçirmesi ve saklaması da aynı gerekçeyle 8. maddeye aykırı olacağını belirtmiştir (§ 144).

AİHM'e göre mevcut başvurudaki ihlalin, başvuruçular mahkum edilirken ulusal mahkemelerce 8. maddeye aykırı bir şekilde tutulan verilere değinilip değinilmemesinden bağımsız olarak meydana geldiğini kaydetmektedir. 8. madde açısından, bu başvuruda başvuruçuların mahkum edilirken ulusal mahkemelerin söz konusu iletişim verilerinin sınırlı bir kısmından (bir aylık bir dönemi ilgilendiren ve sözleşmeyle alakalı nedenlerle tutulabilecek olan) bahsetmesinin bir önemi yoktur. Çünkü başvuruçuların şikayeti, kolluk makamları tarafından elde edilen ve sonrasında işlenen, saklanan ve ilgili ceza kovuşturması açısından incelenen on dört aylık bir döneme ilişkin veri setinin tamamını ilgilendirmektedir. Böyle bir miktardaki verinin sözleşmeyle alakalı gerekçelerle tutulamayacağı ve tutulmadığı;

daha ziyade Mahkemenin 8. maddeye aykırı gördüğü genel ve ayırım yapmayan bir saklama rejiminin bir parçası olduğu tartışmasızdır (§ 145).

Son olarak Mahkeme, başvurucunun 8. madde kapsamındaki şikayetine ilişkin bulguların, başvuru aleyhine elde edilen delillerin kabul edilebilirliğini ilgilendirmediğini, bunun yürürlükteki ulusal hukuk doğrultusunda ulusal mahkemeler tarafından değerlendirilmesi gereken bir konu olduğunu ve 8. maddeyi ihlal ederek elde edilen delillerin yargı süreçlerinde kabul edilmesi ve kullanılmasının zorunlu olarak 6. maddenin ihlali sonucuna yol açmadığını belirterek 8. maddenin ihlaline karar vermiştir (§ 146).

Çamurşen başvurusundan ayrılan ve AİHM'in esastan incelemesi beklenen altı dosyada da durum tam olarak budur ve hatta bu dosyalarda ihlalin boyutu çok daha fazladır. Zira yukarıda ayrıntılı olarak anlatıldığı üzere, Türkiye'de internet trafik verileri ve kayıtlarının tutulmasının "*yasa niteliği taşımadığı*"nda, orantılılık şartına aykırı olduğunda ve Sözleşme'nin 8. maddesinin ihlal edildiğinde şüphe yoktur. Dolayısıyla, BTK'nın bu verilere erişimi, işleminden geçirmesi ve saklaması da aynı gerekçeyle 8. maddeye aykırılık teşkil etmektedir.

Aynı şekilde, altı dosyanın başvuru sahiplerinin şikayeti; mahkemeler tarafından elde edilen ve sonrasında işlenen, saklanan ve ilgili ceza kovuşturması açısından incelenen 1 yıllık bir döneme ilişkin verilerden öte bu süreden daha fazla tutulan, dolayısıyla imhası, yani olmaması gereken verilere ilişkindir. Slovenya Yasasında ön görülen 14 aylık bir döneme ilişkin verilerin tamamının dahi sözleşmeyle ilgili gerekçelerle tutulmadığını ve bunun daha çok 8. maddeye aykırı olup genel ve ayırım yapmayan bir saklama rejiminin parçası olduğunu belirten AİHM'in, Türkiye'de hakim kararı olmadan, sınırsız süreyle ve hiçbir denetime tabi olmadan saklanan verilerle ilgili daha güçlü bir ihlal kararı vermesi şaşırtıcı olmayacaktır.

Son olarak, AİHM'e göre 8. maddeyi ihlal ederek elde edilen delillerin yargı süreçlerinde kabul edilmesi ve kullanılmasının zorunlu olarak 6. maddenin ihlali sonucunu doğurmaz. Bu başvurulardaki temel ihlal iddiası da özel yaşam hakkı ihlal edilerek elde edilen internet trafik verilerinin delil olarak kullanılması ve Sözleşme'nin 8. maddesinin ihlali iddiasıdır ve aynı gerekçeyle AİHM altı dosyada ihlal vermesi beklenmektedir.