AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİNDE CEZA MUHAKEMESİNE İLİŞKİN HÜKÜMLERİN DEĞERLENDİRİLMESİ

Yard. Doç. Dr. Serap Keskin*

I-Genel Bilgiler

Elektronikteki hızlı değişim ile gelişim ve elektronik süreçteki hız, elektronik ortamda işlenen suçlara ceza hukukunun ve bu suçların kendilerine uygun biçimde elektronik ortamda soruşturulması ve failin belirlenebilmesi yönünde, Ceza Muhakemesi Hukukunun uyum göstermesi zorunluluğunu doğurmuştur. Özellikle, yalnızca elektronik ortamda bulunan delillerin, elektronik süreçteki saniyelerle söylenen olağanüstü hız nedeniyle karartılabilmesindeki kolaylık, söz konusu delillerin karartılabilmesi olasılığını en aza indirgeyecek Ceza Muhakemesi Hukuku koruma önlemlerini oluşturmayı gerekli kılmaktadır. Aksi takdirde elektronik ortam kullanılmak suretiyle işlenen ve ülke sınırı da tanımayabilen ve bu özellikleri nedeniyle kendisine siber suç denilen suçların faillerinin ve bu suçların ispatı için aranan delillerin saptanamaması, ele geçirilememesi ve özgün olarak korunamaması tehlikesi bir gerçek olarak karşımızda duracaktır. Sözleşme, gerekçesinde ceza muhakemesi hukuku alanındaki bu zorunluluğu, "çok sayıda iletişim biçimi ve hizmetin, ortak iletim ortamları ve taşıyıcılarıyla birbirleriyle bağlantılı ve ilişki içinde olduğu elektronik otobanı da içine alan teknolojik devrim Ceza Hukuku ve Ceza Muhakemesi Hukukunu da değiştirdi"[1] söylemiyle açıklamaktadır.

---

* İstanbul Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı Öğretim Üyesi.

1 Bkz. Convention on Cybercrime, Explanatory Report, no.132 (http://conventions.coe.int/Treaty/EN/projets/FinalCyberRa-

Bu nedenle Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesi Hukukuna ilişkin hükümlerin, ceza muhakemesi sürecinde, bir yönüyle ceza muhakemesinin yürüyüşüne, bu bağlamda da delillerin elde edilmesi ve korunmasına hizmet eden koruma önlemleriyle ilgili olduğu görülmektedir. Bu hükümler Sözleşmenin 14-21. maddeleri arasında düzenlenmişlerdir. Sözleşmenin 22.maddesinde de yargı yetkisi üzerine özel bir hükme yer verilmiştir.

Sözleşmede öngörülen koruma önlemleri, siber suçu ve bu suçun fail/faillerini ortaya çıkarabilmek için delil elde edebilmek amacıyla, Ceza Muhakemesi Hukukunda klasik koruma önlemlerinden olan arama ve elkoyma önlemlerinin elektronik ortamdaki özel birer çeşididir. Sözleşmenin gerekçesinden elektronik ortamda arama terimi yerine bu ortama uygun bir terim olan erişim ve elkoyma terimi yerine de kopyalama teriminin üzerinde düşünülmüş olduğu anlaşılmaktadır. Bu noktada karma bir terimlemenin de düşünüldüğü ve arama yerine "arama ya da benzeri erişim" ve elkoyma yerine "elkoyma ya da benzer biçimde güven altına alma" söylemlerinin de öngörüldüğü görülmektedir.[2] Sözleşme söz konusu terim konusunu ülkelere bırakmıştır. Bundan başka Sözleşme, Ceza Muhakemesi Hukukundaki arama koruma önleminde elektronik ortamdaki olağanüstü hız nedeniyle delile özgün niteliğiyle ulaşabilmek bakımından geç kalınması tehlikesi var olduğundan, elektronik dünyadaki verileri arama işlemi öncesinde aramayı olanaklı kılacak, verileri ön koruyucu nitelikteki önlemlere de yer vermiştir.

Bu bağlamda Sözleşmede öngörülen ve bizim bilişim koruma önlemleri olarak adlandırmayı uygun gördüğümüz koruma önlemleri şunlardır:

a) 16.maddede düzenlenen "depolanmış bilgisayar verilerinin hızlı bir biçimde korunması(expedited preservation of stored computer data)",

---

pex.htm) ve Türkçe çevirisi için: İnternet ve Hukuk Platformu www.ivhp.net, Açıklayıcı Rapor, no.82

2 Bkz. adı geçen İngilizce özgün gerekçe, no.137 ve a.g.Türkçe çevirisi, no.87

b) 17.maddedeki "trafik verilerinin hızlı bir biçimde korunması ve kısmen açıklanması (expedited preservation and partial disclosure of traffic data)",

c) 18.maddedeki "üretim emri (production order)",

d) 19.maddedeki "depolanmış bilgisayar verilerinin aranması ve bunlara elkoyma (search and seizure of stored computer data)",

e) 20.maddedeki "trafik verilerinin anında/gerçek zamanlı toplanması (real-time collection of traffic data)",

f) 21.maddedeki "içerik verilerinin yolunun kesilip ele geçirilmesi (interception of content data)".

Sözleşmenin öngördüğü bu koruma önlemlerine genel olarak başvurulamayacak, somut bir ceza soruşturmasıyla ilgili olarak başvurulabilecektir. Burada bilişim alanındaki verilere ve iletişime müdahale söz konusu olduğundan bu önlemlere genel olarak başvurma emri/kararı, hem özel yaşamın dokunulmazlığı hakkını hem de iletişim özgürlüğünü ortadan kaldıracaktır. Nasıl ki genel olarak telefon dinleme emri ya da kararı verilemeyip, ancak somut bir ceza soruşturması nedeniyle bu soruşturmaya konu olan suç/suçlar ve bu suçlardan şüpheli/sanık durumunda bulunan kişilerle sınırlı olarak söz konusu koruma önlemine başvurulabilirse, burada da bilişim dünyasını ilgilendiren Sözleşmedeki koruma önlemlerine de -Ceza Muhakemesi Hukukundaki tüm koruma önlemlerinde olduğu gibi- yalnız somut suç/suçlar ve fail/faillerle sınırlı olarak başvurulabilecektir.

II- Bilişim Koruma Önlemlerinin Kapsamı

Sözleşmede öngörülen bilişim koruma önlemleri, elektronik ortamda, depolanmış ya da halen iletişim sürecinde bulunmak gibi iki biçimde görünebilen, trafik verileri, içerik verileri ve abone verilerini de içeren her tür bilgisayar verisiyle ilgilidir. Öngörülen her bir bilişim koruma önleminin hangi veriye uygulanabileceği tek tek ilgili maddelerde belirtilmiştir.

Sözleşme, düzenlediği koruma önlemlerinin kapsamını yalnızca Sözleşmede öngördüğü suç tipleri ile sınırlı tutmamıştır. Sözleşmenin 14.maddesine göre, 20. ve 21.maddelerde öngörülen trafik verilerinin anında/gerçek zamanlı toplanması ile içerik verilerinin yolunun kesilip ele geçirilmesi koruma önlemleri dışındaki diğer önlemlerden, Sözleşmede öngörülen tüm suçların soruşturmasından başka, bir bilgisayar sistemi aracılığıyla işlenen bütün diğer suçların soruşturmasında da yararlanılabileceği gibi, herhangi bir suçun elektronik ortamdaki delilinin toplanması amacıyla da yararlanılabilecektir.

Sözleşmenin 14.maddesinde bilişim koruma önlemlerinin kapsadığı, bir başka deyişle uygulanabildiği tüm suçlar bakımından, 20. ve 21.maddelerde öngörülen trafik verilerinin anında/gerçek zamanlı toplanması ile içerik verilerinin yolunun kesilip ele geçirilmesi koruma önlemleri, gerek özel yaşamın dokunulmazlığı hakkına, gerekse iletişim özgürlüğüne ağır müdahale edici niteliği göz önüne alınarak ayrık tutulmuştur.

21.maddede düzenlenen içerik verilerinin yolunun kesilip ele geçirilmesi koruma önlemi, telefon görüşmesinin anında dinlenmesi koruma önleminin bilişim dünyasındaki biçimidir. Bu özelliğiyle de telefon dinleme koruma önleminde olduğu gibi hem özel yaşamın gizliliğine hem de iletişim özgürlüğüne müdahaledir. Bu nedenle Sözleşme, içerik verilerinin yolunun kesilip ele geçirilmesi bilişim koruma önleminin ancak ağır suçlarda uygulanabileceğini kayıt altına almıştır. Sözleşme, ağır suçları kendisi göstermemiş, bu hususu ulusal hukuklara bırakmıştır. Ancak devletler, söz konusu bu bilişim koruma önlemini tüm suçlar bakımından uygulayamayacaklar, mutlaka ağır suçlar sınıflaması yaparak bir sınırlama getireceklerdir.

Sözleşme 20.maddedeki trafik verilerinin anında/gerçek zamanlı toplanması bilişim koruma önlemi bakımından ise, devletlere, söz konusu koruma önleminin kapsamını belirli suç kategorileri ile sınırlamayı saklı tutabilme hakkını vermektedir. Trafik verilerinde elektronik veri ya da iletinin içeriğine ulaşılmamakta, yalnızca bu veri ya da iletinin kaynağına, vardığı noktaya, izlediği elektronik yola, saatine, tarihine, boyutlarına

ve süresine ve ne olduğu (örneğin elektronik dosya, elektronik posta ya da mesaj gibi) bilgisine ulaşılmaktadır. Ancak devletler, bu sınırlamayı yapma hakkını saklı tutarlarsa, belirledikleri suç kategorisi, içerik verilerinin yolunun kesilip ele geçirilmesi koruma önlemi bakımından belirledikleri suç kategorisinden daha sınırlı olamayacaktır. Ayrıca, trafik verilerinin anında/gerçek zamanlı toplanması koruma önlemi, elektronik iletinin izlediği yol ile çıktığı ve vardığı yeri saptayabilmek, dolayısıyla da failleri belirleyebilmek bakımından önemli olduğundan, Sözleşme, saklı tutma hakkını kullanan devletlerin, söz konusu bilişim koruma önleminin en geniş biçimde uygulanabilmesini sağlamaları yönünde devletleri yönlendirmektedir.

Bundan başka Sözleşme, ulusal hukuklarda var olabilen sınırlamalar yüzünden, kapalı kullanıcı grubunun yararına işletilen, kamuya açık iletişim ağlarını kullanmayan ve diğer bilgisayar sistemleriyle bağlantılı olmayan bilgisayar sistemlerindeki iletişime müdahale edemeyen devletlerin, söz konusu her iki bilişim koruma önlemini uygulamama hakkını saklı tutabileceklerini de hüküm altına almıştır. Kapalı kullanıcı grubundan, örneğin şirketleri tarafından bir bilgisayar ağı aracılığıyla kendi aralarında iletişim kurabilen çalışanlar gibi, hizmet sağlayıcı ile bağlantıları açısından sınırlı bir grup kastedilmektedir. Diğer bilgisayar sistemleriyle bağlantılı olmamak, Sözleşmenin 20. ve 21.maddelerindeki trafik verilerinin anında/gerçek zamanlı toplanması ile içerik verilerinin yolunun kesilip ele geçirilmesi koruma önlemlerine emredildiği tarihte, kendisine ileti gönderilen bir sistemin başka bir bilgisayar ağıyla fiziksel ya da mantıksal bir bağlantısının olmamasıdır. Kamuya açık iletişim ağlarını kullanmamak ise, kullanıcı bilsin ya da bilmesin, kamuya açık bilgisayar ağlarını(internet dahil), kamuya açık telefon ağlarını ve diğer kamuya açık telekomünikasyon olanaklarını kullanan sistemleri kullanmamaktır.[3]

---

3 Bkz. a.g. İngilizce özgün gerekçe, no.144 ve a.g.Türkçe çevirisi, no.144

III- Bilişim Koruma Önlemlerinde İnsan Hak ve Özgürlüklerine Saygı ve Orantılılık İlkesi

Sözleşmenin 15.maddesine göre, Sözleşmeyi imzalayıp, onaylayan devletler, Sözleşme hükümleri doğrultusunda, öngörülen bilişim koruma önlemlerine ilişkin iç hukuklarında düzenleme yaparlarken, insan hak ve özgürlükleri ile koruma önlemleri arasında denge kuran, hak ve özgürlüklere yeterli koruma getiren düzenlemeler yapmak zorundadırlar. Söz konusu dengeyi sağlayıcı unsurları Sözleşme göstermemekte, bu unsurları belirleme işini devletlere bırakmaktadır. Ancak devletler için ortak standartların da bulunduğunu, devletlerin söz konusu düzenlemeleri yaparken bu ortak standartları temel almak zorunda olduğunu da açıklamaktadır. İlgili ortak standartlar, insan hak ve özgürlükleri hakkındaki uluslararası belgelerde belirli olan standartladır. Bu uluslararası belgeler arasında, taraf olan Avrupa devletleri için 1950 tarihli Avrupa İnsan Hakları Sözleşmesi ve ek protokolleri, Birleşmiş Milletler çerçevesinde 1966 tarihli Medeni ve Siyasal Haklar Sözleşmesi ve diğer bölgesel düzeydeki insan hakları sözleşmeleri gelmektedir(Örneğin, 1969 Amerika İnsan Hakları Sözleşmesi, 1981 Afrika İnsan Hakları ve Ulusların Hakları Sözleşmesi).[4]

Ceza Muhakemesi Hukukunda her koruma önleminde olduğu gibi, başvurulabilecek bilişim koruma önlemi ile işlendiğinden şüphe edilen suç arasında bir dengenin olması ve hafif bir koruma önlemi ile delile ulaşmak ceza muhakemesi amacına ulaşabilmek olanaklı iken ağır veya daha ağır bir bilişim koruma önlemine de başvurulamaması gerekmektedir. Bu özellik Ceza Muhakemesi Hukukunda koruma önlemlerinin ortak özelliklerinden biridir ve bu husus koruma önlemlerindeki „orantılılık ilkesi"dir. Sözleşme, yukarıda da açıklandığı üzere, bilişim koruma önleminin hak ve özgürlüklere müdahale edici özelliğindeki ağırlık ile suçun ağırlığı arasındaki dengeyi, içerik verilerinin yolunun kesilip ele geçirilmesi bilişim koruma önlemi bakımından bizzat öngörmüştür. Bunun dışında devletler, Sözleşmede öngörülen koruma önlemlerini iç hukuklarında

---

4 Bkz. a.g. İngilizce özgün gerekçe, no.145 ve a.g.Türkçe çevirisi, no.145

düzenlerlerken, her bir koruma önlemi için başvurma koşullarını ve usulünü orantılılık ilkesini gözönünde tutarak belirlemek zorundadırlar. Bu çerçevede soruşturma organlarının ilgili bilişim koruma önlemine başvuru koşulu, yetkisi ve süresi bakımından adli ya da başka bir bağımsız denetim mekanizmasının oluşturulması zorunluluğu getirilmektedir.

Bilişim koruma önlemlerine başvuruda, Ceza Muhakemesi Hukukunun temel ilkelerinden biri olan ve Anayasa'mızın da 38/5.maddesinde „hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda bir delil göstermeye zorlanamaz" biçiminde dile getirilen, kişinin kendisine veya yakınlarına karşı yüklenen bir suçun ispatı eylemine katılmama, hatta buna karşı gelebilme hakkına da saygı duyulacaktır. Yine bunun dışında kalan tanıklıktan çekinme hakkı sahiplerine tanınmış olan çekinme hakkı hukuksal ayrıcalığının da gözönünde bulundurulması zorunluluğu vardır.

Sözleşmenin 15.maddesinin son fıkrasına göre devletler, kamu yararını ve adaletin sağlıklı şekilde yürütülmesini de dikkate alacaklardır. Bu bağlamda kamu yararıyla tutarlı olduğu ölçüde, öngörülen bilişim koruma önlemlerinin uygulanmaları sonucunda, hizmet sağlayıcılar da dahil üçüncü kişilerin hak, sorumluluk ve haklı yararları üzerindeki etki ve bu etkiyi hafifletmenin yolları da değerlendirilmek durumundadır.

IV- Sözleşmede Öngörülen Bilişim Koruma Önlemleri

1- Depolanmış Bilgisayar Verilerinin Hızlı Biçimde Korunması (Expedited Preservation of Stored Computer Data)

Sözleşmenin 16.maddesinde yer alan depolanmış bilgisayar verilerinin hızlı bir biçimde korunması önlemi, bilgisayar verileri üzerinde gelecekte arama/erişim ve elkoyma/kopyalama önlemlerini gerçekleştirebilmeyi olanaklı kılmak için öngörülmüş bir koruma önlemidir. Bununla, bilgisayar verilerinin silinmeden, değiştirilmeden, bozulmadan, özgün niteliğiyle korunabilmesi amaçlanmaktadır. Koruma, zorunlu olarak, koru-

ma altına alınan verilerin ya da kopyalarının haklı kullanıcılar tarafından kullanılamaması, bir başka deyişle erişilememesi anlamına da gelmemektedir. Buna verilerin „dondurulması" denmektedir. Ancak Sözleşme, verilerin dondurulup, dondurulmama, yani erişilmez kılma hususunun belirlenmesini devletlere bırakmıştır.[5]

Bu bilişim koruma önleminin konusu, hizmet sağlayıcılar ve veri depolayıcılar tarafından toplanmış ve depolanmış durumda bulunan elektronik verilerdir. Şimdiki zamanda bulunan bir iletişim sürecinde akış durumundaki elektronik veriler bu koruma önleminin konusunu oluşturamazlar.

Sözleşmenin gerekçesine göre bilgisayar dilinde „verileri korumak" ile „verileri tutmak" eylemlerinde farklılık vardır: Verileri korumaktan anlaşılan, depolanmış durumda bulunan verilerin, depoda tutulmaya devam edilmesi, böylece var olan özgün nitelik veya durumunun değişmesine ya da bozulmasına neden olabilecek etkenlerden korunmasıdır. Verileri tutmaktan anlaşılan ise, şimdiki zamanda üretilmekte olan verilerin, belli birinin mülkiyetinde gelecek için yine şimdiki zamanda depolanması eylemidir. Bir başka deyişle veriler şimdi biriktirilmekte ve bunlar gelecek için tutulmaktadır. Kısaca, verileri tutmak, verileri depolama sürecidir. Verileri korumak ise tutulmuş verilerin, depoda sağlam ve güvenlik içinde bulundurulmasına devam etmektir.[6] İncelediğimiz koruma önleminde söz konusu olan verilerin korunmasıdır.

Sözleşme bu düzenlemesiyle, hizmet sağlayıcılarına ya da başka kişi veya kurumlara, faaliyetleri sırasında topladığı verileri kısmen veya tamamen depolama yükümlülüğünü getirmemektedir. Söz konusu koruma önlemi, bir bilgisayar sistemi aracılığıyla depolanmış durumdaki veriler için geçerlidir. Sözleşmenin gerekçesinden, Sözleşmeyi kaleme alanlarca, Sözleşmenin, hizmet sağlayıcılarına belli bir zaman aralığı için rutin olarak trafik verilerini toplama ve depolama zorunluluğu getir-

---

5 Bkz. a.g. İngilizce özgün gerekçe, no.159 ve a.g.Türkçe çevirisi, no.159

6 Bkz. a.g. İngilizce özgün gerekçe, no.151 ve a.g.Türkçe çevirisi, no.151

mesinin gerekip gerekmediğinin düşünüldüğü, ancak uzlaşmaya varılamadığı için böyle bir zorunluluğun Sözleşmeye alınmadığı anlaşılmaktadır.[7]

Bu koruma önlemi ile bazı devletlerin veri koruma yasalarında ve Avrupa Birliğinin yönergelerinde getirilen, kişisel verilerin, tutulmaları için ticari neden yoksa tutulmamaları ve derhal silinmeleri ile depolanmaları gerekli olmaktan çıkar çıkmaz verilerin silinmesi zorunluluğuna, suçların önlenmesi ve soruşturulması amacıyla istisna getirebilme yolu açılmaktadır.

Her koruma önleminde olduğu gibi, depolanmış bilgisayar verilerinin hızlı bir biçimde korunması önlemi de yalnızca somut bir ceza muhakemesi faaliyeti için geçerli olabilir. Bu bağlamda kısaca verilerin hızlı korunması da diyebileceğimiz bu önlem, hakkında bu koruma önlemine başvurma kararının verildiği somut bir ceza soruşturmasında, bu soruşturmaya konu olan belli eylem ve belli failler hakkında uygulanabilir. Ayrıca verilerin hızlı biçimde korunması emri/kararında korunması istenen verinin ne olduğunun da belirtilmesi gerekmektedir. Fakat Sözleşme, her tür depolanmış verinin bu koruma emrinin konusunu oluşturabileceğini de belirtmektedir. Söz konusu önleme, bilgisayar verilerinin kaybedilmesinin ya da değiştirilmesinin söz konusu olabileceğine dair şüphe nedenleri bulunduğu takdirde başvurulabilecektir.[8] Verilerin hızlı biçimde korunması emri/kararının yönelik olduğu kişi, söz konusu depolanmış verileri mülkiyetinde ya da kontrolünde bulunduran kişidir.

Bilgisayarla bağlantılı suçların büyük ölçüde, örneğin, çocuk pornografisi, bilgisayar virüsü ya da bilgisayar sisteminin gerektiği gibi işlemesine engel olabilecek diğer iletiler gibi yasa dışı içeriğe sahip olan ya da uyuşturucu kaçakçılığı veya sahtekarlık, dolandırıcılık gibi suçlarla ilgili deliller içerebilen elektronik iletilerin, bilgisayar sistemi aracılığıyla iletilmesi sonucunda işlendiği gözönünde tutulacak olduğunda, verilerin hız-

---

7 Bkz. a.g. İngilizce özgün gerekçe, no.135 ve a.g.Türkçe çevirisi, no.85

8 Bkz. a.g. İngilizce özgün gerekçe, no.161 ve a.g.Türkçe çevirisi, no.161

lı bir biçimde korunması emri/kararının, geçmiş zamanda kalan bu iletilerin, iletişim sürecini saptayabilmek ve dolayısıyla kaynak ve varış noktası bilgisine ulaşabilmek olanaklı olabilecektir. Böylelikle gerçek suçlu/suçluların kim oldukları belirlenebilecektir. Aynı şekilde bu verilere özgün nitelikleriyle elkoyma/kopyalama da, delillerin karartılamaması bakımından yararlı olacaktır.

Verileri hızlı biçimde koruma kararı üzerine, koruma yükümlülüğü altına giren kişinin bu yükümlülüğünü ulusal yasalar en fazla 90 günlük süre ile sınırlı tutmak zorundadırlar. Koruma yükümlülüğü, verilerin, soruşturma organlarına açıklanması yükümlülüğünü içermemektedir. Bunun için ayrıca açıklama ya da arama/erişim emri/kararının verilmesi gerekmektedir. Bundan dolayı koruma emrini/kararını alan kişi, ilgili bilgisayar verilerinin doğruluğu için, 90 günü aşmayan yasal süre içinde olmak kaydıyla, somut ceza soruşturmasında koruma emrinde belirli kesin süre boyunca, yetkili mercilerin bu bilgilerin açıklanmasını ya da aranması/erişilmesini isteyebilmelerini sağlamak üzere onları korumak zorundadır. Süre, arama/erişim, elkoyma/kopyalama ya da üretim emri gibi diğer bilişim koruma önlemlerini almaya yetecek kadar uzun olmalıdır.[9]

Sözleşmenin 16.maddesi bu koruma önlemi ile ilgili olarak, koruma emri/kararı gereği verileri korumakla yükümlü kılınan kişiye, koruma usulü ile ilgili sır saklama yükümlülüğü de getirmektedir. Bir başka deyişle verilerin hızlı korunması önlemi gizli uygulanan bir önlemdir. Ancak bu gizlilik de bir süreyle sınırlı tutulmak zorundadır. Sözleşme, sürenin belirlenmesi hususunu ulusal hukuklara bırakmıştır. Sözleşmenin gerekçesine göre söz konusu koruma önlemi, ceza muhakemesinde hazırlık soruşturmasında başlangıç soruşturmasının bir parçasıdır ve bu nedenle gizlilik, ceza soruşturma organlarının, şüphelinin soruşturmadan haberdar olmaması gereksinimini ve bireylerin gizlilik gereksinimini karşılamaktadır. Gerekçeye göre, başka kişilerin verileri bozmaya veya silmeye kalkışma-

---

9 Bkz. a.g. İngilizce özgün gerekçe, no.162 ve a.g.Türkçe çevirisi, no.162

ması için gizlilik gereklidir. Ayrıca gizlilik, verilerin konusunun ya da verilerde adı geçen veya kimliği belirtilen başka kişilerin de gizliliğini korumaya yardımcı olur.[10]

2- Trafik Verilerinin Hızlı Biçimde Korunması ve Kısmen Açıklanması (Expedited Preservation and Partial Disclosure of Traffic Data)

Sözleşmenin 17.maddesinde öngörülen bu bilişim koruma önlemi ile, 16.maddede düzenlenmiş verilerin hızlı biçimde korunması önlemi çerçevesinde, trafik verilerinin hızlı biçimde korunması ile ilgili somut zorunluluklar getirilmekte ve iletişim sürecinde birden fazla hizmet sağlayıcının da bulunabileceği gözönünde tutularak, bunları ve iletinin izlediği elektronik yolu belirleyebilmek amacıyla bazı trafik verilerinin açığa vurulması sağlanmaktadır.

Sözleşmenin 1/d. maddesine göre trafik verisi, somut bir hukuksal rejime tabi olan bir bilgisayar verisi kategorisidir. Bu veriler, bir iletiyi başlangıç noktasından varış noktasına göndermek için iletişim zincirindeki bilgisayarlar tarafından üretilir. Trafik verilerinin kategorileri ise Sözleşmede ayrıntılı olarak sayılmıştır. Bunlar, iletişimin başlangıç noktası, varış noktası, izlediği yol, saat, tarih, boyutlar, süre ve bu iletişimde kullanılan hizmet tipidir. Başlangıç noktası, bir hizmet sağlayıcının hizmet verdiği iletişim aracını tanımlayacak bir telefon numarası, internet protokol adresi (IP numarası), ya da benzer bir bilgi olabilir. Varış noktası, iletinin aktarıldığı iletişim aracına ait benzer bilgilerdir. İletişimde kullanılan hizmet tipi terimi, ağ içerisinde kullanılan hizmetin tipi, örneğin dosya transferi, elektronik posta ya da anında mesaj anlamına gelmektedir.[11]

Gerekçeye göre genellikle bir iletinin iletilmesine, birden fazla hizmet sağlayıcı katıldığından, her bir hizmet sağlayıcı, iletişimin kendi sisteminden geçişi üzerine trafik verilerini üretmekte ve tutmaktadır. Bazen de trafik verilerinin hizmet

---

10 Bkz. a.g. İngilizce özgün gerekçe, no.163 ve a.g.Türkçe çevirisi no.163

11 Bkz. a.g. İngilizce özgün gerekçe, no.30 ve a.g.Türkçe çevirisi no.30

sağlayıcılar arasında paylaşıldığı görülmektedir. Böyle bir durumda ceza soruşturması için önem taşıyan veriler, hizmet sağlayıcılardan herhangi birinin elinde bulunabilir. Bu nedenle, her bir hizmet sağlayıcı, bütünün bir parçasına sahiptir ve kaynak ve varış noktasını belirlemek için bu parçaların hepsinin incelenmesi gerekmektedir. Bu nedenle, 17. madde, bütün hizmet sağlayıcılar arasında trafik verilerinin hızlı biçimde korunmasını sağlama amacı gütmektedir. Bunun yollarını belirlemek ise ulusal hukuklara bırakılmıştır. Sözleşmenin gerekçesine göre, seçenek olarak önerilen yöntem, somut iletinin iletişimine katıldıkları saptanan bütün hizmet sağlayıcılar için geçerli olacak tek koruma emri/kararının verilmesi ve bunun her bir hizmet sağlayıcıya ayrı ayrı tebliğ edilmesidir. Diğer bir yöntem seçeneği olarak da kendisine koruma kararı tebliğ edilen hizmet sağlayıcının, zincirde kendisinden sonra gelen hizmet sağlayıcıya koruma kararını ve hükümlerini bildirmesi koşulunun getirilmesi ve bu hususun zincirde böyle devam etmesinin sağlanmasıdır.[12]

Trafik verilerinin hızlı biçimde korumaya alınması kararı, bu verileri aramayı/erişimi ve elkoymayı/kopyalamayı içermediğinden, soruşturma organları hizmet sağlayıcının önemli bütün verilere sahip olup olmadığını ve iletişim sürecinde başka hizmet sağlayıcıların da bulunup bulunmadığını bilemeyeceklerdir. Bu nedenle 17. maddede ayrıca, koruma kararının bildirildiği hizmet sağlayıcının, yetkili makamlara, iletişim zincirinde bulunan diğer hizmet sağlayıcıları ve iletişim yolunu belirleyebilmesine yetecek kadar trafik verisini hızlı biçimde açığa vurması yolu da getirilmiştir. Ancak yetkili makamlar, açığa vurulması gereken trafik verisinin türünü açıkça belirtmek zorundadırlar. Böylece yetkili makamların, başka hizmet sağlayıcılar için de koruma önlemi alıp almama konusunda karar verebilmeleri sağlanmış olmaktadır.[13]

---

12 Bkz. a.g. İngilizce özgün gerekçe, no.167,168 ve a.g.Türkçe çevirisi no.167,168

13 Bkz. a.g. İngilizce özgün gerekçe, no.169 ve a.g.Türkçe çevirisi no.169

3- Üretim Emri (Production Order)

Sözleşmenin 18. maddesinde düzenlenen üretim emri ile ceza soruşturma makamlarının ulusal sınırlar içinde bulunan bir kişiyi, kendi mülkiyetinde ya da kontrolünde bulunan ve depolanmış durumdaki bilgisayar verilerini açıklamaya ve yine ulusal sınırlar içindeki bir hizmet sağlayıcının, mülkiyetinde ya da kontrolünde bulunan hizmete ilişkin abone bilgilerini teslim etmeye zorlamaları olanağı getirilmektedir. Böylelikle söz konusu kişi veya hizmet sağlayıcının da sözleşmeden veya başka bir nedenden kaynaklanan hukuksal yükümlülüklerini de hukuka aykırı olarak çiğnememiş olmaları sağlanmaktadır. Üretim emrinin konusunu oluşturan veriler de depolanmış konumda olan verilerdir. Yoksa şimdiki zamanda iletişim sürecinde akış durumunda olan bilgisayar verileri üzerinde üretim emrinin verilebilmesi olanaklı değildir. Bu koruma önlemi ancak, kişi ya da hizmet sağlayıcının söz konusu verileri depoladığı durumda anlam taşıyacaktır. Ancak Sözleşme, kişi ya da kurumlara veri depolama yükümlülüğü veya depoladıkları takdirde de verilerin doğruluğunu güvenceye bağlama yükümlülüğü getirmemektedir. Eğer hizmet sağlayıcı, hizmetlerinin aboneleriyle ilgili kayıt tutmuyorsa bu bilişim koruma önlemi uygulanamayacaktır.

„Mülkiyetinde ya da kontrolünde" söylemi ile anlatılmak istenen, verilerin, üretim emrini veren ülkenin sınırları içinde fiziksel mülkiyet dahilinde bulunması, ya da fiziksel mülkiyetin dışında ise, kişinin ya da hizmet sağlayıcının üretim emrini veren ülkenin sınırları içinden verilerin üretimini serbestçe kontrol edebilme olanağıdır. Örneğin, uzaktaki bir online depolama hizmeti yoluyla hesabında depoladığı bilgiler için kendisine üretim emri verilen kişi ile başka bir şirketin sağladığı veri depolama olanağından yararlanıp, abone bilgilerini uzakta depolayan hizmet sağlayıcı söz konusu abone bilgilerini üretmek zorunda kalacaktır. „Hizmete ilişkin„ söylemiyle anlatılmak istenen ise, üretim emrini veren ülkenin sınırları içinde sunulan hizmetlerle ilgili abonelik bilgileridir.[14]

---

14 a.g. İngilizce özgün gerekçe, no.173 ve a.g.Türkçe çevirisi no.173

Sözleşme, devletlere, kişi ya da hizmet sağlayıcılara üretim emri çıkartılabilmesinde, ulaşmak istedikleri veriler bakımından farklı koşullar, farklı merciler ve farklı usuller öngörebilme olanağını açık bırakmaktadır. Örneğin kamuya açık abonelik bilgileri için bir yargılama makamının kararı aranmayabilecekken, kamuya açık olmayan abonelik bilgileri için mutlaka bir yargılama makamının, yani ceza muhakemesindeki aşamaya göre bir yargıç ya da mahkeme kararı aranabilecektir. Sonuç olarak devletler, bu bilişim koruma önlemini düzenlerlerken, koruma önlemlerinde aranan orantılılık ilkesini gözönünde tutmak zorundadırlar. Söz konusu koruma önleminde gizliliğe ilişkin olarak Sözleşme, bu konuda elektronik olmayan dünyayla paralelliği sağlamak için özel bir düzenleme yapmamıştır.[15] Önlemin gizliliği hususu ulusal hukukların seçimine bırakılmıştır.

Üretimin nasıl yapılacağı hususunda devletler, belli bilgisayar verilerinin ya da abonelik bilgilerinin, örneğin açıklamanın yapılmak zorunda olduğu zaman dilimi veya veri ya da bilgilerin salt metin, online, kağıt çıktı ya da diskette sunulması gerektiği gibi, üretim emrinde belirtilen biçimde üretilmesi için zorunluluklar koyabileceklerdir.[16]

18. maddede abonelik bilgilerinin neler olduğu açıklanmıştır. Bunlar, hizmet sağlayıcının hizmetlerinin aboneleriyle ilgili tuttuğu her tür bilgidir. Madde hükmüne göre bunlar, abonenin kimliği, posta ya da bulunduğu yerin adresi, telefon numarası ve aboneye ulaşılabilecek diğer numaralar, hizmet sözleşmesi veya düzenlemesi esas alınarak verilen fatura ve ödeme bilgileri, kullanılan iletişim hizmetinin türü, teknik olanaklar ve hizmet süresi bilgileri ile hizmet sözleşmesi veya düzenlemesi esas alınarak verilen ve iletişim ekipmanının kurulduğu bölgeye ilişkin olan diğer bilgilerdir. Abone bilgileri kavramı içinde trafik verileri ve içerik verileri bulunmamaktadır.

Gerekçeye göre ceza soruşturmasında abonelik bilgilerine

---

15 a.g. İngilizce özgün gerekçe, no.175 ve a.g.Türkçe çevirisi no.175

16 a.g. İngilizce özgün gerekçe, no.176 ve a.g.Türkçe çevirisi no.176

başlıca iki durumda gereksinim duyulabilir. Birincisi, (örneğin cep telefonu gibi yararlanılan telefon hizmetinin türü, çağrı iletme, sesli mesaj gibi yararlanılan diğer bağlantılı hizmetlerin türü, telefon numarası ya da elektronik posta adresi gibi) abonenin hangi hizmetleri ve bu hizmetten yararlanabilmesi için hangi teknik olanakları kullandığı ve kullanmakta olduğunun saptanmasında abonelik bilgilerine gereksinim duyulur. İkincisi, teknik bir adres bilindiğinde, ilgili kişinin kimliğini saptamakta abonelik bilgilerinden yararlanılır. Abonenin fatura bilgileri ve ödeme kayıtlarıyla ilgili ticari bilgiler gibi abonelik bilgileri de ekonomik bir suçun soruşturmasını ilgilendirebilir.[17]

Üretim emri bilişim koruma önlemi de somut bir ceza soruşturması dolayısıyla verilebilir. Bu yolla, üretim emrinde geçen belli bir isim esas alınarak bağlantılı bir telefon numarası veya elektronik posta adresi istenebileceği gibi, belli bir telefon numarası ya da e-posta adresi esas alınarak ilgili abonenin isim ve adresi istenebilir. Ancak, genel olarak veri madenciliği amacıyla hiç kimseye üretim emri verilemez.[18]

4- Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara Elkoyma (Search and Seizure of Stored Computer Data)

Sözleşmenin 19. maddesinde yer alan bu bilişim koruma önlemi ile, somut bir ceza soruşturmasında, delil elde edebilmek amacıyla depolanmış durumda bulunan bilgisayar verilerinin aranması/erişimi ve bu verilere elkoyma/kopyalama işlemleri öngörülmektedir. Bu önlem, elektronik olmayan ortamdaki arama ve elkoyma koruma önlemlerinin elektronik ortama uyumlu duruma getirilmiş bir görünümüdür. Bu önlemde bilgisayar verilerinin maddi bir veri taşıyıcısının aranması ve bu taşıyıcıya el konması söz konusu olabilmektedir. Bu bağlamda maddi olmayan bilgisayar verilerinin üzerinde saklandığı bilgisayar sabit diski ya da disket gibi fiziksel ortama el konulması

---

17 a.g. İngilizce özgün gerekçe, no.178 ve a.g.Türkçe çevirisi no.178

18 a.g. İngilizce özgün gerekçe, no.182 ve a.g.Türkçe çevirisi no.182

ve bu ortamın götürülmesi için verilerin örneğin yazıcı çıktısı gibi maddi ya da disket gibi fiziksel bir ortam üzerine maddi olmayan bir kopyasının üretilmesi söz konusu olmaktadır. Bu son durumda verilerin bir kopyası da doğal olarak bilgisayar sisteminde ya da depolama cihazında kalmaktadır. Bundan başka bilgisayar sistemlerinin birbirlerine bağlanabilme özelliklerinden dolayı veriler doğrudan aramanın yapıldığı bilgisayarda değil de o sistemden kolayca erişilebilecek başka bir sistemde bulunabilir. Bu durum, aramayı verilerin gerçekte bulunduğu yeri içine alacak biçimde genişletmeyi ya da verileri bulundukları yerden aramanın yapılmakta olduğu bilgisayara getirmeyi gerekli kılabilir.[19] Ancak Sözleşmenin 19/2. maddesine göre bu genişletme için de verinin başka bir sistemde olduğuna dair yeterli şüphe nedenlerinin bulunması gerekmektedir. Koruma önleminin genişletilmesi durumunda, aranacak verilerin ilk bilgisayar sisteminden yasal olarak erişilebilir durumda olması gerekmektedir.

Sözleşmenin 19/1. maddesine göre bir bilgisayar sistemi ya da bu sistemin bağlantılı ya da bağlantısız veri depolama(CD-Rom ya da disket gibi) parçaları ve bunlarda depolanmış bilgisayar verileri aranabilecek veya bilgisayar diliyle bu bilgilere erişilebilecektir.

İncelediğimiz koruma önlemi de depolanmış durumda bulunan veriler için geçerli olan bir önlemdir. Bu bağlamda, alıcının kendi bilgisayar sistemine indirilinceye kadar, internet hizmeti sağlayıcının posta kutusunda bekleyen elektronik postaların depolanmış bilgisayar verisi mi, yoksa şimdiki zamanda akış durumunda olan bir veri olarak mı değerlendirilmesi hususunda seçimi Sözleşme ulusal hukuklara bırakmaktadır.[20]

Sözleşmenin 19. maddesi aranmış/erişilmiş bilgisayar verilerine elkoymayı/kopyalamayı da düzenlemektedir. Eğer bilgisayar verisinin kopyalanması olanaksız ise, veri taşıyıcısına elkoymak gerekmektedir. Bu çerçevede elkoymak koruma ön-

---

19 a.g. İngilizce özgün gerekçe, no.187 ve a.g.Türkçe çevirisi no.187

20 a.g. İngilizce özgün gerekçe, no.190 ve a.g.Türkçe çevirisi no.190

lemi, hem bilgisayar verilerinin kayıtlı olduğu fiziksel ortamı alıp götürmek, hem de bu verilerin ya da bilgilerin kopyasını üretmek ve tutmak anlamına gelmektedir. El koymak, el konan verilere erişmek için gereken programların kullanılmasını ve bu programlara da el konmasını da içermektedir. Ceza muhakemesinde önemli olan delilin gerçeği yansıtan niteliğidir. Bu nedenle elkoyma, elkonan verilerin doğruluğunun da korunması sonucunu doğurmaktadır. Bundan dolayı elkoyma terimi kısaca, verilerin kontrolünü ele geçirmeyi ya da verileri alıp götürmeyi ifade etmektedir.[21]

Elektronik ortamdaki delilin gerçeği yansıtan niteliğini koruyabilmek için elkonan bu delilin erişilemez kılınması, taşınması ya da silinmesi de 19. maddede öngörülmektedir. Verilerin erişilmez kılınmasının yasadışı içerik taşıyan verilerin var olduğu durumlarda uygulanmasının yararlı olabileceği belirtilmektedir. Veriler taşınmakla veya erişilmez kılınmakla yok edilmemekte, varlıklarını sürdürmektedirler. Ancak şüpheli, geçici olarak verilerden yoksun bırakılmaktadır; ceza soruşturmasının sonucuna göre bu verilerin kendisine verilmesi yolu açıktır.[22]

19. maddenin son fıkrasında, elektronik ortamda delil aramak ve elkoymak konusunda teknik bilgiye sahip olan kişilere, soruşturma organlarının işini kolaylaştırmak için yardım etme zorunluluğunun getirilebilmesini düzenlemektedir. Bu çerçevede Sözleşme, bilgisayar sisteminin işleyişi ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında bilgi sahibi olan herhangi bir kişinin arama ve elkoyma konusunda yardımcı olmaya zorlanmasına izin vermektedir.

Ancak bu yardım yükümlülüğü „makullük" ölçütü ile sınırlandırılmıştır. Gerekçeye göre bazı durumlarda bilgi sağlama, bir şifrenin ya da başka bir güvenlik önleminin açığa vurulmasının diğer kullanıcıların gizliliğini ya da aranması için

---

21 a.g. İngilizce özgün gerekçe, no.197 ve a.g.Türkçe çevirisi no.197

22 a.g. İngilizce özgün gerekçe, no.197 ve a.g.Türkçe çevirisi no.197

yetki verilmeyen verileri tehdit ediyorsa makul olmayabilir. Bu durumda arama ve elkoymanın teknik olarak en iyi şekilde nasıl yürütüleceğine ilişkin teknik bilgi sağlama, yetkili mercilerce aranmakta olan asıl verilerin anlaşılabilir ve okunabilir bir biçimde açığa vurulması olabilecektir.[23]

Arama/erişim ve elkoyma/kopyalama önlemlerinin gizli tutulup tutulmaması veya ilgilisine bu durumun bildirilip bildirilmemesi hususu ulusal hukuklara bırakılmıştır. Ancak Gerekçe, hukuk düzenlerinde bildirim yapma zorunluluğunu getirmeyi düşünen devletlere, böyle bir bildirimin soruşturmaya zarar verebileceği riskini de hesaba katmalarını ve bu durumda bildirimin ertelenmesi seçeneğini de önermektedir.[24]

5- Trafik Verilerinin Anında/Gerçek Zamanlı Toplanması (Real-Time Collection of Traffic Data)

Sözleşmenin 20.maddesi trafik verilerinin anında, bir başka deyişle gerçek zamanlı toplanmasını bir bilişim koruma önlemi olarak öngörmektedir. Söz konusu trafik bilgileri, bir bilgisayar sistemi üzerinden aktarılan ve ilgili devletin ulusal sınırları içinde bulunan özel iletişim sayılan bilgilerdir. Bu nedenle trafik bilgilerinin anında toplanması, iletişim özgürlüğüne müdahaledir. Bir başka açıdan bu koruma önleminin konusu, bir bilgisayar sistemi aracılığıyla iletilen, başka bir bilgisayar sistemine ulaşmadan önce telekomünikasyon ağları aracılığıyla da iletilebilen belirli iletilerdir.[25]

Trafik verileri daha önce de açıklandığı üzere Sözleşmenin 1/d. maddesinde tanımlanmıştır. Tekrar edecek olursak trafik verisi, bir iletiyi başlangıç noktasından varış noktasına göndermek için iletişim zincirindeki bilgisayar sistemleri tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini ve bu iletişim-

---

23 a.g. İngilizce özgün gerekçe, no.202 ve a.g.Türkçe çevirisi no.202
24 a.g. İngilizce özgün gerekçe, no.204 ve a.g.Türkçe çevirisi no.204
25 a.g. İngilizce özgün gerekçe, no.206 ve a.g.Türkçe çevirisi no.206

de kullanılan hizmet tipini gösteren herhangi bir bilgisayar verisidir. Başlangıç noktası, bir hizmet sağlayıcının hizmet verdiği iletişim aracını tanımlayacak bir telefon numarası, internet protokol adresi (IP numarası), ya da benzer bir bilgi olabilir. Varış noktası, iletinin aktarıldığı iletişim aracına ait benzer bilgilerdir. İletişimde kullanılan hizmet tipi terimi, ağ içerisinde kullanılan hizmetin tipi, örneğin dosya transferi, elektronik posta ya da anında mesaj anlamına gelmektedir.[26]

Trafik verilerinin gerçek zamanlı toplanmasında, iletişimi şimdiki zamanda gerçekleştirilen iletiye ait trafik verilerinin de aynı zamanda bir başka deyişle anında toplanması söz konusudur. Veriler, ses ya da elektronik sinyallerin iletilmesi biçiminde maddi olmayan verilerdir. Verilerin toplanması işlemi verilerin bir kopyasının üretilmesi biçiminde gerçekleştirilir. Trafik verileri anında toplanırken, verinin iletişim sürecindeki akışına engel olunmaz ve veri iletişim sürecinde ulaşması istenen yere ulaşır. Bu noktada, iletişim hizmetlerinin kamusal ya da özel kuruluşlarca sağlanması veya kamuya açık ya da kapalı bir kullanıcı grubuna veya özel kişilere sunulmuş olması arasında bir fark yapılmamaktadır. Kısaca her türlü iletişime ait trafik verilerinin anında toplanması kararı verilebilecektir.

Sözleşmeye göre trafik verilerinin anında/gerçek zamanlı toplanması bilişim koruma önlemi her suç bakımından uygulanabilecek bir önlemdir. Ancak yukarıda, „Bilişim Koruma Önlemlerinin Kapsamı" başlığı altında da açıklandığı üzere, Sözleşme, 14. maddesinde devletlere bu önlemi belirli suçlarla sınırlayabilmeyi saklı tutabilme hakkını vermiştir. Ancak bu hakkın sınırı da belirlenen suçların aşağıda da inceleneceği gibi içerik verilerinin yolunun kesilip ele geçirilmesi bilişim koruma önleminin uygulanabileceği suçlardan daha kısıtlı olmamasıdır.

Sözleşmenin gerekçesine göre trafik verilerinin anında toplanması, özellikle Sözleşmede tanımlanmış olan bilgisayar sistemlerine yasadışı erişimle ilgili olan ve virüslerin ve çocuk por-

---

26 a.g. İngilizce özgün gerekçe, no.30,209 ve a.g.Türkçe çevirisi no.30,209

nografisinin dağıtımı gibi suçların soruşturmasında büyük önem taşıyabilecektir. Örneğin bazı durumlarda trafik verileri anında toplanmadan tecavüzün ya da dağıtımın kaynağı belirlenemeyebilecektir.[27] Genellikle bilgisayar sistemine izinsiz giren kişi iletişimin izlediği yolu değiştirdiği için trafik verilerinin anında tutulması bu kişiye ulaşabilmek bakımından da önemli bir önlemdir.

Telefon konuşmaları gibi telekomünikasyon araçlarıyla yapılan iletişimde, bu araçlar kullanılarak işlenen tehdit, taciz gibi suçlarda faile veya uyuşturucu kaçakçılığı gibi suçlarda faillere ve delile ulaşabilmek bakımından iletişimin kaynağını belirlemekte, trafik verilerinin iletişim yapıldığı anda toplanması soruşturma organlarını iletişimin kaynağına ve varış noktasına ulaştırdığı gibi, bilgisayar sistemi kullanılarak yapılan iletişimde de aynı şey geçerlidir. Bu koruma önleminde yapılan da budur. Çocuk pornografisinin yasadışı dağıtımı, bilgisayar sistemine yasadışı erişim veya bilgisayar sisteminin işleyişine müdahale bilişim suçu işlendiği zaman, suç uzaktan, örneğin internet aracılığıyla işlenmişse, iletişimin izlediği yolu geriye izlemek önemlidir. Bu koruma önlemi ile, şüphelinin iletişimlerinin saat, tarih, kaynak ve varış noktasıyla, mağdurların sistemlerine izinsiz girildiği tarih arasında bağlantı kurulabilir, diğer mağdurlara ulaşılabilir ya da suç ortakları arasındaki bağlantılar ortaya çıkarılabilir.[28]

Söz konusu koruma önlemi de her önlemde olduğu gibi ulusal sınırlar içindeki belirli iletişimlerle ve somut bir ceza soruşturmasıyla ilgilidir. İletişimde bulunan taraflardan(insan) ya da iletişimde kullanılan cihazlardan biri (bilgisayar gibi) ulusal sınırlar içindeyse ulusallık gerçekleşmiş sayılır. Bu nedenle trafik verilerinin anında toplanması emri/kararının hangi iletişimler hakkında olduğu söz konusu emir/kararda açıklanmalıdır. Bunun dışında henüz öğrenilmemiş suçların keşfedilebileceği umuduyla „denize olta atmak" benzeri girişimlere yetki verilmemektedir.[29]

---

27 a.g. İngilizce özgün gerekçe, no.214 ve a.g.Türkçe çevirisi no.214

28 a.g. İngilizce özgün gerekçe, no.218 ve a.g.Türkçe çevirisi no.218

29 a.g. İngilizce özgün gerekçe, no.219 ve a.g.Türkçe çevirisi no.219

Sözleşme 20. maddesiyle devletlere, hazır teknik olanakları elverdiği ölçüde hizmet sağlayıcıların, trafik verilerinin anında toplanması işleminde soruşturma organlarıyla işbirliği yapma ve onlara yardımcı olma yükümlülüğü yanında, verilen karar uyarınca bu toplama işlemini bizzat yapma yükümlülüğünü getirmelerini de öngörmektedir. Ancak devletlerin söz konusu işlemi gerçekleştirebilecek ya da yardım isteyebilecek teknik olanaklara ve bilgiye sahip olmaları da gerekmektedir.

Trafik bilgilerinin anında toplanması koruma önlemi de gizli olduğu takdirde ceza soruşturmasında etkin olur. Bu nedenle trafik verilerinin anında toplanması işleminin gizli yapılması öngörülmektedir. Bu çerçevede, müdahale, iletişimin taraflarının algılayamayacakları bir şekilde yürütülmelidir. Ayrıca işbirliği yapan ya da yardım eden hizmet sağlayıcılarının ve bilgisi bulunan çalışanlarının ulusal hukuklarca belirlenecek bir süre boyunca sır saklama yükümlülüğü getirilmektedir.

6- İçerik Verilerinin Yolunun Kesilip Ele Geçirilmesi (Interception of Content Data)

İçerik verilerinin yolunun kesilip ele geçirilmesi bilişim koruma önlemi, Sözleşmenin 21.maddesinde düzenlenmiştir. İçerik verilerine ilişkin bir tanım Sözleşmede yoktur. Ancak içerik verileri kavramı ile anlatılmak istenen, trafik bilgileri dışında kalan, iletişimin içeriği, yani, iletişimin anlamı ve niyeti ya da iletişimle taşınan mesaj veya bilgidir.[30] İçerik verilerine müdahalede de iletişim sürecinde bulunan iletişim ya da iletişimlerin içeriklerine anında ulaşılmaktadır. Bu özelliğiyle iletişim özgürlüğüne ve özel yaşamın dokunulmazlığı hakkına en ağır biçimde müdahale edici nitelikte bir bilişim koruma önlemidir. Ancak bazı durumlarda içerik verilerine anında erişmeden iletişimin niteliği keşfedilememektedir. Trafik verilerinin anında toplanması koruma önleminde olduğu gibi, bu önlemde de iletişimin varış noktasına ulaşması engellenmez; bilgilerin bir

---

30 a.g. İngilizce özgün gerekçe, no.209,229 ve a.g.Türkçe çevirisi no.209,229

kopyası üretilir. Burada da yine kamusal ya da özel hizmet sağlayıcı veya kamuya açık ya da kapalı iletişim ayırımı yapılmaz.

İçerik verilerinin yolunun kesilip bu verileri ele geçirmenin, özel yaşamın dokunulmazlığı hakkı ile iletişim özgürlüğüne ağır derecede müdahale edici özelliğinden dolayı Sözleşme, 21. maddesinde bu önlemin ulusal hukuklarca belirlenecek ağır suçların soruşturmasında uygulanabileceği hükmünü getirmiştir. Bunun dışında hak ve özgürlüğe müdahale açısından alınması gerekebilecek diğer önlem ve koşulları Sözleşme, Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi kararları doğrultusunda yine ulusal hukuklara bırakmaktadır. Bu hususun trafik verilerinin anında toplanması bilişim koruma önlemi bakımından da geçerli olduğu belirtilmelidir. Ancak içerik verilerinin yolunun kesilip ele geçirilmesi önlemi için ulusal hukuklarca getirilecek koşullar, trafik verilerinin anında toplanması önlemine göre daha sıkı olabilecektir.

Trafik verilerinde olduğu gibi, içerik verilerinin anında ele geçirilmesi de, tıpkı bir telefon görüşmesinin anında dinlenmesinde olduğu gibi, iletişimin yasadışı bir içeriğe (örneğin tehdit, hakaret ya da pornografi gibi) sahip, dolayısıyla bir suç niteliğinde olduğunu belirlemek ya da uyuşturucu kaçakçılığı veya ekonomik suçlar gibi suçların delillerine ulaşabilmek bakımından önemli bir soruşturma aracı olabilir. Ayrıca, örneğin bir bilgisayar sistemine yasadışı erişim gerçekleştirmek için veya bilgisayar virüslerini dağıtmak için gönderilen iletilerin içeriğine anında erişmeden bu iletilerin yasadışı veya zararlı olduğunu belirlemek olanaksızdır.

İçerik verilerinin yolunu kesip bunlara anında erişebilmek için devletler, trafik verilerinde olduğu gibi teknik yapıyı oluşturmalıdırlar. Hizmet sağlayıcıların işbirliği ve yardım yükümlülüğü ile gizlilik kuralı burada da trafik verilerinde olduğu gibidir.

V- Yargılama Yetkisi

Sözleşmede Ceza Muhakemesi Hukuku ile ilgili son hüküm 22.maddede yer alan yargılama yetkisine ilişkin hükümdür. Bu hüküm ile, Sözleşmeyi onaylayan devletlere, Sözleşmede Ceza Hukukuna ilişkin hükümlerde 2-11. madddelerde sıralanmış suçlar hakkında yargılama yetkisini düzenlerlerken uymaları gereken ölçütler sunulmaktadır. Öncelikle ülkesellik ilkesine yer verilmektedir. Bu bağlamda ulusal devlet, gerçek ülkesi ile varsayılan ülkesi (bayrağını taşıyan gemi ve uçak gibi) sınırları içinde işlenmiş suçları yargılama yetkisini oluşturmak durumundadır. Türk hukuku açısından durum tüm suçlar bakımından zaten böyledir. Sözleşmede öngörülen suçlar bakımından örneğin, bilgisayar sistemine saldıran kişi ile saldırının mağduru olan sistem ya da saldırgan olmasa bile saldırıya uğrayan sistem belli bir ülke sınırları içinde ise suç, o ülkede işlenmiş kabul edilecektir.[31]

Bundan başka Sözleşmenin 22. maddesinde faile göre kişisellik ilkesine yer verilmiştir. Buna göre, bir devletin yurttaşı, ülke sınırları dışında, başka bir ülkenin sınırları içinde suç işlediğinde, eylem, suçun işlendiği yerde de suç sayılmak kaydıyla devlet kendi yurttaşını yargılama yetkisine sahip olacaktır. Ya da ülke dışında suç işleyen yurttaş, herhangi bir devletin yargılama yetkisi dışında kalıyorsa, yine faile göre kişisellik ilkesi devreye girecektir.

Sözleşme 22.maddesinde devletlere, öngörülen yargılama yetkisini belirli durum ve koşullarda uygulama ya da uygulamama haklarını saklı tutabileceklerini de belirtmektedir. Ancak, bir devletin, kendi ülke sınırları içinde bulunan bir kişi hakkındaki Sözleşme hükümleri çerçevesinde (Sözl.24.md) yapılan bir geri verme istemini, yurttaşı olduğu gerekçesiyle reddettiği bir durumda, yargılamama yetkisine ilişkin hak saklı tutma hakkı yoktur. Devletler, Sözleşmede öngörülen bu ölçütler dışında kalan ölçütlere dayanarak da yargılama yetkisi oluşturabileceklerdir.

---

31 a.g. İngilizce özgün gerekçe, no.234 ve a.g.Türkçe çevirisi no.234

Suç ortaklığında, şeriklerin başka başka ülkelerde bulunması olasılığında, birden fazla devlette aynı ceza soruşturmasının yapılmasının önüne geçmek için 22.maddede, devletlerin soruşturma ve yargılama için en uygun yeri seçmeleri bakımından görüş alışverişinde bulunmaları önerilmektedir.

VI- Ortak Avrupa Ceza ve Ceza Muhakemesi Hukuku Yolundaki Çalışmalar

Bu çalışmada Siber Suç Sözleşmesi yanında, Ceza ve Ceza Muhakemesi Hukuku açısından çok önemli bir gelişme olan ortak bir Avrupa Ceza ve Ceza Muhakemesi Hukuku oluşturabilme yolundaki çalışmalara da kısaca değinilmesinin gerekli olduğunu düşünmekteyiz. Bu konudaki ilk çalışmalar, Avrupa Komisyonu'nun girişimi ve desteği ile 1995 yılında Avrupa ceza hukukçularından oluşturulan bir grup tarafından başlatılmıştır. Bu ilk adımdaki amaç, öncelikle Avrupa Birliği'nin mali çıkarlarının ceza hukukunca korunması yönündeki belli ortak ilkeleri saptamaktı. Bu çalışma „Avrupa Birliğinin Mali Çıkarlarının Korunmasına İlişkin Ceza Hukuku Kuralları, Corpus Juris"[32] başlığını taşıyan ilk ürününü 1997 yılında vermiş ve ortaya Avrupa Birliğine üye ülkelerin tartışma ve değerlendirmelerine sunulan, kısaca „Corpus Juris 1997"[33] denilen bir metin çıkmıştır. Söz konusu uzman grubu çalışmalarına devam etmiş ve „Corpus Juris 1997" üzerindeki tartışma ve değerlendirmeler gözönüne alınarak 2000 yılında, „Corpus Juris 2000"[34] metni ortaya çıkarılmıştır. Corpus Juris üzerindeki çalışmalar halen devam etmektedir. Corpus Juris'in, Ceza Huku-

---

32 Bu konudaki gelişimi ortaya koyan ortak bir çeviri çalışmasını iki meslektaşımla birlikte yapmış bulunuyoruz. Bunun için Bkz. **KESKİN**, Serap/**ZAFER**, Hamide/**KOCASAKAL**, Ümit, „Avrupa Birliğinin Mali Çıkarlarının Korunmasına İlişkin Ceza Hukuku Kuralları (Corpus Juris)" Seçkin Yayınevi, Ankara, Kasım 2001

33 Corpus Juris 1997 metninin tam çevirisi Serap Keskin ve Hamide Zafer tarafından yapılmıştır: Bkz. **KESKİN/ZAFER/KOCASAKAL**, age. sh.19 vd.

34 Corpus Juris 2000 metninin tam çevirisi Ümit Kocasakal tarafından yapılmıştır: Bkz. **KESKİN/ZAFER/KOCASAKAL**, age. sh.89 vd.

ku ve Ceza Muhakemesi Hukukunun Avrupa bütünleşmesindeki rolü üzerinde toplumsal tartışma yaratarak bir işlev gördüğü düşünülmektedir: Bu tartışmanın konusu da cezai korumayı gerektiren Avrupa düzeyindeki çıkarların neler olduğu ve Avrupa sathında cezai koruma ve etkinliğin sağlanabilmesi için ne gibi düzenlemelerin yapılacağıdır.[35]

Corpus Juris, Avrupa Birliğinin mali çıkarlarını zedelediği düşünülen suç tiplerini yarattıktan başka ortak bir Avrupa Ceza Muhakemesi Hukuku yolunda da hükümler içermektedir. Bu bağlamda en önemli değişim ve gelişim ceza muhakemesinde hazırlık soruşturmasıyla ilgilidir. Corpus Juris, ülke sınırı tanımayan suçlulukla mücadelede soruşturma araçlarının da ülke sınırı tanımadan kullanılabilmesini amaçlamaktadır. Bu amaç doğrultusunda gelecekte, devletlerin anayasa, ceza ve ceza muhakemesi yasalarında ve özellikle adli teşkilatlarında önemli değişiklikler yapmaları gündeme gelebilecektir. Corpus Juris'in Ceza Muhakemesi Hukuku açısından önerdiği en önemli değişim Avrupa Ceza Hukukunca suç kabul edilen eylemlerin soruşturulmasında, dava edilmesinde ve infazında yetkili Avrupa Savcılığı kurumunu oluşturmasıdır. Avrupa Birliğine üye, örneğin İngiltere gibi ülkelerde, savcılık kurumunun işini başka makamlar da yapabildiğinden Corpus Juris buna Avrupa Ceza Soruşturma ve Kovuşturma Makamı demektedir. Türk Hukuku açısından uygun kavram „Avrupa Savcılığı"dır.

Corpus Juris'e göre Avrupa Savcılığının soruşturma alanı tüm Avrupa ülkesidir; yani Avrupa Birliğine üye ülkelerin, ülkeleri arasındaki sınırlar kalkmaktadır. Avrupa Savcılığı, merkezi Brüksel olan bir Avrupa Başsavcısı ile her bir üye ülkenin kendi ulusal hukuklarına göre belirleyip yetkilendirecekleri, her üye ülkede bulunacak Avrupa Savcılarından oluşacaktır. Her bir üye ülkede bulunan Avrupa Savcıları aynı yetkilere sahip olacaktır. Ulusal ceza soruşturma makam ve memurlarının da Avrupa Savcılarına destek olma yükümlülüğü öngörülmektedir. Herhangi bir üye ülkedeki Avrupa Savcısının verdiği ör-

---

35 Bkz. **VERVAELE** J., Corpus Juris 2000 metnindeki önsöz (Çeviren Ümit Kocasakal: **KESKİN/ZAFER/KOCASAKAL**, age.sh.13)

neğin bir Avrupa arama emri, tüm Avrupa ülkesinde geçerli ve uygulanmak zorunda olan bir emir olacaktır. Buna Avrupa Savcılarının verdiği kararların „dolaşım ehliyeti" denmektedir.[36] Aynı ehliyet, ulusal mahkemelerin benzer nitelikli kararları için de kabul edilmektedir. Kararlara dolaşım ehliyetinin getirilmesinin en önemli gerekçesi, faillerin bilgisayar ağı üzerinden diğer devletlerde ispata yarayacak bilgileri saniyede değiştirebildikleri bir ortamda, varolan resmi-adli yardımlaşma sürecinin artık yetersiz kalmasıdır.[37]

Hazırlık Soruşturmasındaki yargıçsal denetim yetkisini ulusal hukuklar kendileri oluşturacaklardır. Bu bağlamda örneğin Türk Hukuku açısından hazırlık soruşturmasında yetkili yargılama makamı olan Sulh Ceza Yargıçlığı, Avrupa Savcısının, Avrupa yakalama kararı, Avrupa arama kararı gibi işlemlerde denetim mercii, Avrupa tutuklama kararı gibi işlemlerde de yetkili makam olabilecektir. Ancak devletler, bugün de olduğu gibi, böyle bir yargıçsal denetim mekanizmasını oluşturmak zorundadırlar. Son olarak diğer bir önemli husus da, bir üye ülkede, ulusal hukuka göre hukuka uygun biçimde elde edilmiş bir delilin, diğer üye ülkelerde de, bu ülkelerin hukukuna bakılmaksızın hukuka uygun kabul edilmesi önerisidir.[38]

---

36 **SIEBER**, Ulrich: „Avrupa Ceza Hukuku Yolunda", Corpus Juris 1997'nin Almanca çevirisinin başındaki makale (Çevirenler: Serap Keskin ve Hamide Zafer: Keskin/Zafer/Kocasakal, age. sh.22)

37 **SIEBER** U., (Çeviri metni) age. sh.27

38 **SIEBER** U., (Çeviri metni) age. sh.31 ve Corpus Juris 1997 md.33 ve Corpus Juris 2000 md.33