

Strasbourg, 29 Haziran 2001
CDPC (2001) 17
Ek I

AVRUPA KONSEYİ
SİBER SUÇLAR SÖZLEŞMESİ TASLAĞI

Hazırlayan
Siber Suç Uzmanları Komitesi
(PC-CY)

Onaylayan
Avrupa Suç Sorunları Komitesi'nin (CDPC)
50. Genel Kurulu
(18 - 22 Haziran 2001)

ANKARA BAROSU
BİLGİ ve BELGE MERKEZİ

II

Ankara Barosu Bilgi İşlem Merkezi Yayınları

I. Basım

1000 adet basılmıştır.

Ankara, 2006

ISBN 975-6037-58-X

Bu çeviri metni Avrupa Birliği resmi çevirisi olmayıp İnternet ve Hukuk Platformu tarafından gönüllü olarak Türkçeye çevrilmiştir.

İlgilenen herkesin ücretsiz olarak faydalanması amacıyla bu kitabın kâğıt ve baskı giderleri Ankara Barosu tarafından karşılanmıştır.

Ankara Barosu Bilgi ve Belge Merkezi tarafından kataloglanmıştır.
(bilgibelgemerkezi@ankarabarusu.org.tr)

343.099 9

Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu/Haz.:Siber Suç
Uzmanları Komitesi, Çev.: İnternet ve Hukuk Platformu.____
Ankara:Ankara Barosu,2006
XX,313 s. :19 cm. (Ankara Barosu Bilgi İşlem Merkezi Yayınları)
ISBN 975-6037-58-X

I. Siber Suçlar 2. İnternet ve Hukuk I. Ankara Barosu II. Siber Suç
Uzmanları Komitesi
III. İnternet ve Hukuk Platformu

İletişim Adresi:

Ankara Barosu Başkanlığı

Ankara Adalet Sarayı Kat: 5

(06100) Sıhhiye / Ankara

Tel : + 90 (312) 310 55 26

Faks : + 90 (312) 309 22 37

E-Posta: ankarabarusu@ankarabarusu.org.tr

Web : www.ankarabarusu.org.tr

Baskı: Ustaoğlu Basım Yayın Ltd. Şti.

Tel : + 90 (312) 229 64 81

UB0704/41/0000
KİTAP KİTAP

Bu çeviri metni Avrupa Birliđi resmi çevirisi olmayıp İvHP (İnternet ve Hukuk Platformu) tarafından gönüllü olarak Türkçeye çevrilmiştir.

İlgilenen herkesin ücretsiz olarak faydalanması amacıyla bu kitabın kağıt ve baskı giderleri Ankara Barosu tarafından karşılanmıştır.

1. The first part of the paper discusses the importance of the study of the history of the United States. It is argued that a knowledge of the past is essential for a full understanding of the present and for the development of a sound policy for the future.

2. The second part of the paper discusses the importance of the study of the history of the United States. It is argued that a knowledge of the past is essential for a full understanding of the present and for the development of a sound policy for the future.

Avrupa Konseyi Siber Suç Sözleşmesi Hakkında...

Hazırlanması 4 yıl kadar süren Avrupa Konseyi Siber Suç Sözleşmesi, 23 Kasım 2001'de, Konsey üyesi olmayan ülkeler de dahil olmak üzere Budapeşte'de imzaya açıldı. O zaman, 26'sı üye ve 4'ü üye olmayan (ABD, Japonya, Kanada ve Güney Afrika) 30 ülke Sözleşme'yi imzalamış, Sözleşme'nin imzacı ülkelerin kendi iç hukuklarına uyarlamaları için yapılacak çalışmaların da 30 Haziran 2003 tarihine dek tamamlanması öngörülmüştü. Konsey, 23 Ocak 2003 tarihinde bilgisayar sistemleri aracılığıyla yapılan ırkçılık ve yabancı düşmanlığı eylemlerini de kapsama alan bir Ek Protokol yayınladı. Mart 2006 itibariyle, 12 ülkenin herhangi bir çekince koymadan imzaladığı bu Sözleşme, 30 ülke tarafından çeşitli çekinceler konarak imzalanmıştır.

Türkiye ise henüz Sözleşmeyi imzalamamıştır. "İfade özgürlüğünü kısıtlaması", "insancıl ceza normlarına aykırı" olması, adı "siber suç" olmakla birlikte özellikle "usule dair hükümlerinin amacını aşan biçimde düzenlenmesi" ve ayrıca "diğer tüm suçları da kapsayacak olması" gibi niteliklerinden dolayı bu Sözleşme bir çok sivil toplum kuruluşu tarafından ciddi eleştiriler almıştır.

İnternet ve hukuk konusundaki küresel gelişmeleri, bilgi ve iletişim teknolojileri politikalarını izlemek ve

VI

Türkiye'nin çağdaş yaklaşımlara geçişini hızlandırmak amacıyla 2001 yılında kurulan "İnternet ve Hukuk Platformu" (İv H P), kendisinin de eleştirdiği bu niteliklerine karşın, tartışılan Sözleşmeyi herkesin bilgisine sunmak amacıyla 2002 yılında Türkçe'ye çevirerek, www.ivhp.org.tr adresindeki web sitesine yüklemiş, bu konuda Bilgi Üniversitesi ve İstanbul Barosu ile birlikte bir de panel düzenlemişti. Şimdi de Ankara Barosu işbirliği ile kitapçık haline gelen bu metnin iç hukukumuza uyarlanması konusunda "çok dikkatli okunması ve değerlendirilmesi" gerektiği açık...

İvHP Yürütme Kurulu

www.ivhp.org.tr

Mart 2006

Sevgili Meslektaşlarım,

'Tuhaf Hava/Sınırlar Çağında Kültür-Bilim ve Teknoloji' adlı özgün eserinde *Andrew Ross*'un ifade ettiği üzere, teknolojiye teslim olan sanayi sonrası kapitalist kültür ciddi bir bunalım içinde. Bu bunalımın nedenini, teknoloji ile kültürün birbirinden kopmasına ve kültürsüz kalan teknolojinin yarattığı, kime ve neye hizmet ettiği belli olmayan kaosa bağlayan *Ross*'a göre, sınır tanımazlığın etkili bir aracı haline gelen teknoloji, insanlığın geleceğini ciddi biçimde tehdit ediyor.

İçinde yaşadığımız geç modern çağda teknoloji; yaşamın ve insanın kendini geliştirmesinden ibaret bulunan, sanat gibi, etik gibi, din gibi değerleri kucaklayan, hem etkileyen hem de etkilenen, kendi içinde büyüyen bir şey olan *kültürü* hemen her yerde dışladı. Teknoloji sadece kültürü dışlamakla kalmadı; kendini hissetme, anlama, algılama, başkalarına karşı duygulu, duyarlı ve saygılı olma hali olan yaşamı esir aldığı gibi, özünde duyumlardan, duygulardan, coşkulardan oluşan dünyamızı, en önde gelen insani özelliklerimiz, olan duygularımızı, duyarlılıklarımızı kirletti, yaratıcılığımızı köreltti, naifliğimizi yok etti.

İşte! Avrupa Birliği Siber Suç Uzmanları Komitesi tarafından hazırlanan ve yine Avrupa Birliği Avrupa Suç Sorunları Komitesinin 50. Genel Kurulunda onaylanan *'Siber Suçlar Konvansiyon Taslağı ve Açıklayıcı Memorandumu'* isimli bu kitabın konusunu

VIII

oluşturan '*siber suç*'; bilgisayar ağlarının, bilgisayar veri ve sistemlerinin, elektronik bilgilerin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetler ile bu sistemlerin, ağların, bilgilerin ve verilerin kötü amaçlı kullanılması ile oluşan, kısaca bilgisayar üç kağıtçılığından, siberpunk gibi anti-kültürel pratiklerden ibaret bulunan ve giderek artış gösteren bir yeni suç tipi olup, kültürden kopan teknolojinin doğurduğu çağımızın en önemli, en tehlikeli suçlarından birisidir.

Siber sözcüğünün kökünü oluşturan ve Yunanca '*yönetmek*' anlamına gelen '*kybernan*' sözcüğünden türetilen '*sibernetik*' kavramı, '*bir insanın veya otomatik bir makinenin, modern tekniğin olanakları çerçevesinde herhangi bir işi yönetmesini veya belli bir amaca ulaşmasını sağlayan*' bilim dalına verilen isim.

Plato'nun diyaloglarının bir çoğunda da rastladığımız '*sibernetik*' kavramını bilimsel olarak inceleyen ilk kişi Amerikalı *Norbert Wiener*. 1947 yılında otomatik kumandalı sistemlerin tekniği üzerine yayınladığı '*Cybernetics*' isimli kitabında *Wiener*, sibernetiği bir kavşak bilim olarak tanımlar ve yönetim işlevini yerine getirebilecek mekanizmalarla ilgili genel kavramlara yer verir. *Wiener*'in bu çalışması kendisinden sonra gelen süreçte, üstün yapılı canlıların yaşamsal işlevleri ile bu işlevlerin yapay olarak yaratılmasına olanak veren süreçleri mantıksal bir analize vurmak suretiyle,

gerçek bir akıl devrimi sayılabilecek önemli bir akımın başlangıç noktası oldu.

Hayal gücü oldukça yüksek kimi fanatik siberetikçilerin, toplumsal olayların bilgi alışverişinden doğduğunu ve dolayısıyla bu olayların siberetik yöntemleriyle incelenmesinin olanaklı bulunduğunu ileri sürdükleri dikkate alındığında, geleceğin toplumlarının düşünme ve yönetme makineleriyle yönetilebileceğini düşünmek, acaba olmazı düşünmek midir? Bunu bu aşamada daha henüz bilmiyoruz. Ama teknolojinin yarattığı yeni iletişim sistemleri ve bilgi teknolojilerine dayanan bilgi tabanlı gelişme ile birlikte, üretim ve tüketim süreçlerinin belli bir yere bağlı olmaktan çıktığı, şirketlerin bilgi ağlarının, dünya kapitalist sisteminin genişlemesinin ve bütünleşmesinin tabanını oluşturduğu, bilgisayarın, internetin, elektronik postanın, yani makinenin, bizi mi yönettiğinin, yoksa bizim onları mı yönettiğimizin birbirine karıştığı günümüzde, hiçbir şey için *'bu kadarı da olmaz'* dememek gerekir.

Televizyon bağımlılığı ve bağımlıları ile dalgasını geçerken: *'Ne sağcıyım, ne solcu / Sadece evdeyim bu gece / O umutsuz küçük ekranda kaybolmak üzere'* diyor *Leonard Cohen*. Ben de, devede küre gibi kendilerini sakladıklarını sanan siber suç ve suçlular ile dalga geçmek için *Cohen*'den ödünç alarak: *'Ne sağcıyım, ne solcuyum / Sahte bey değil, en esaslı bey*

benim / Bilgisayarımın yanında, internetin başındayım / Siber suça bayılıyorum / Kaydı olan her elektronik posta adresine erişiyorum / Sistemlere, verilere müdahale ediyorum / Cesaretim yok, açıktan söyleyemiyorum / Elektronik posta ile ona buna çamur atıyorum / Ben bu işi çok seviyorum / Adımı saklıyorum / Çünkü adımlarım kaçmaya ayarlı / Onun için nickname kullanıyorum / Kuyruğunu saklayamayan tilki gibi miyim? / Kümeste yiyemediği tavukları bile boğan sansar gibi miyim? / Bilmiyorum! / Ama ben bu işi çok seviyorum / Ben bu işi hep yapıyorum' diyor ve başta, Baromuz Bilişim Kurulu Başkanı değerli meslektaşımız Özgür Eralp ile yardımcısı sevgili Çağatay Cengiz olmak üzere, bu kitabın yayınlanmasında emeği geçen herkese teşekkür ediyor, bize yabancı yeni bir kavramı ve konuyu içeren bu kitabın hepimize yeni ufuklar açmasını ve yararlı olmasını diliyorum.

Saygılarımla.

Av.V.Ahsen Coşar
Ankara Barosu Başkanı

İÇİNDEKİLER

SİBER SUÇLAR KONVANSİYON TASLAĞI VE AÇIKLAYICI MEMORANDUMU

Sayfa No :

Avrupa Konseyi Siber Suç Sözleşmesi Hakkında...	V
ÖNSÖZ	VII
GİRİŞ	I
KISIM – I	
Terimler	7
Madde 1 - Tanımlar	7
BÖLÜM – II	
Ulusal Düzeyde Alınacak Önlemler	9
KISIM – I	
Maddî Ceza Hukuku	9
BAŞLIK – I	
Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar	9
Madde 2 - Yasadışı Erişim	9
Madde 3 - Yasadışı Müdahale	9
Madde 4 - Verilere Müdahale	10
Madde 5 - Sistemlere Müdahale	10
Madde 6 - Cihazların Kötüye Kullanımı	11
BAŞLIK 2	
Bilgisayarlarla İlişkili Suçlar	13
Madde 7 - Bilgisayarlarla İlişkili Sahtecilik Fiilleri	13
Madde 8 - Bilgisayarlarla İlişkili Sahtekârlık Fiilleri	13

XII

BAŞLIK - 3

İçerikle İlişkili Suçlar

15

Madde 9 - Çocuk Pornografisiyle İlişkili Suçlar

15

BAŞLIK - 4

Telif Haklarının ve Benzer Hakların

İhlaline İlişkin Suçlar

17

Madde 10 - Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar

17

BAŞLIK - 5

İlave Yükümlülük ve Yaptırımlar

19

Madde 11 - Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek

19

Madde 12 - Kurumsal Yükümlülük

20

Madde 13 - Yaptırımlar ve Önlemler

21

KISIM - 2

Usul Hukuku

22

BAŞLIK - 1

Genel Hükümler

22

Madde 14 - Usul Hükümlerinin Kapsamı

22

Madde 15 - Şartlar ve Önlemler

24

BAŞLIK - 2

Saklanan Bilgisayar Verilerinin Korunmasının

Kolaylaştırılması

26

Madde 16 - Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması

26

Madde 17 - Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması

27

BAŞLIK - 3

Üretim Talimatı

29

Madde 18 - Üretim Talimatı

29

BAŞLIK - 4

Saklanan Bilgisayar Verilerinin Aranması ve
Bunlara El Koyulması

31

Madde 19 - Saklanan Bilgisayar Verilerinin Aranması ve
Bunlara El Konulması

31

BAŞLIK - 5

Bilgisayar Verilerini Gerçek Zamanlı
Olarak Toplanması

34

Madde 20 - Trafik Bilgilerinin Gerçek
Zamanlı Olarak Toplanması

34

Madde 21 - İçerikle İlgili Bilgilere Müdahale Edilmesi

36

KISIM - 3

Yargı Yetkisi

38

Madde 22 - Yargı Yetkisi

38

BÖLÜM - III

Uluslararası İşbirliği

40

KISIM - I

Genel İlkeler

40

BAŞLIK - I

Uluslararası İşbirliğine İlişkin Genel İlkeler

40

Madde 23 - Uluslararası İşbirliğine İlişkin Genel İlkeler

40

BAŞLIK - 2

İadeye İlişkin İlkeler

41

Madde 24 - İade

41

BAŞLIK - 3

Yardımlaşmaya İlişkin Genel İlkeler

45

Madde 25 - Yardımlaşmaya İlişkin Genel İlkeler

45

Madde 26 - Anında İletilen Bilgiler

47

XIV

BAŞLIK - 4

**Uluslararası anlaşmaların Yürürlükte Bulunmadığı
Durumlarda Gelen Yardım Taleplerine İlişkin Usuller 48**

**Madde 27 - Uluslararası anlaşmaların Yürürlükte
Bulunmadığı Durumlarda Gelen Yardım
Taleplerine İlişkin Usuller 48**

Madde 28 - Kullanımda Gizlilik ve Sınırlama 53

KISIM – 2

Özel Hükümler 55

BAŞLIK – 1

**Geçici Önlemlerin Alınması Konusunda
Yardımlaşma 55**

**Madde 29 - Saklanan Bilgisayar Verilerinin
Korunmasının Kolaylaştırılması 55**

**Madde 30 - Korunan Trafik Verilerinin Açıklanması
İşleminin Kolaylaştırılması 58**

BAŞLIK – 2

Soruşturma Yetkileri Konusunda Yardımlaşma 60

**Madde 31 - Saklanan Bilgisayar Verilerine Erişilmesine
İlişkin Yardımlaşma 60**

**Madde 32 - Saklanan Bilgisayar Verilerine İzinli Şekilde
ya da Bu Verilerin Halka Açık Olduğu
Durumlarda Sınır Ötesinden
Erişim Sağlamak 61**

**Madde 33 - Trafik Verilerinin Verçek Zamanlı Olarak
Toplanması Konusunda Yardımlaşma 62**

**Madde 34 - İçerikle İlgili Verilere Müdahale Edilmesi
Konusunda Yardımlaşma 62**

BAŞLIK - 3

24 Saat 7 Gün Boyunca Elverişli Ağ 63

Madde 35 - 24/7 Ağı 63

BÖLÜM - IV**Diğer Hükümler 65****Madde 36 - İmza ve Yürürlük 65****Madde 37 - Konvansiyona Katılım 66****Madde 38 - Belirli Bölgelerde Yürürlük 67****Madde 39 - Konvansiyonun Sonuçları 68****Madde 40 - Yazılı Beyanlar 69****Madde 41 - Federal Ükelere İlişkin Hüküm 69****Madde 42 - Hakların Saklı Tutulması 70****Madde 43 - Saklı Tutulan Hakların Durumu ve
Hakların Saklı Tutulması İşleminde
Vazgeçilmesi 71****Madde 44 - Değişiklikler 72****Madde 45 - Anlaşmazlıkların Çözümü 73****Madde 46 - Tarafların Görüş Alışverişinde Bulunmaları 74****Madde 47 - Konvansiyondan Ayrılma 76****Madde 48 - Bildirimler 76****AÇIKLAYICI RAPOR TASLAĞI 79****I. GİRİŞ 79****II. HAZIRLIK ÇALIŞMALARI 82****III. KONVANSİYON 90****KONVANSİYONUN MADDELERİYLE İLGİLİ
DEĞERLENDİRMELER 93****BÖLÜM - I****Terimler 93****Madde I Tanımlara Giriş 93****Madde I/a Bilgisayar Sistemi 93**

XVI

Madde 1/b	Bilgisayar Verileri	95
Madde 1/c	Hizmet Sağlayıcı	95
Madde 1/d	Trafik Verileri	97
BÖLÜM - II		
Ulusal Düzeyde Alınacak Önlemler		99
KISIM - I		
Maddi Ceza Hukuku		100
BAŞLIK - I		
Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açıklığına Yönelik Suçlar		107
Madde 2 -	Yasadışı Erişim	107
Madde 3 -	Yasadışı Müdahale	111
Madde 4 -	Verilere Müdahale	116
Madde 5 -	Sistemlere Müdahale	118
Madde 6 -	Cihazların Kötüye Kullanımı	121
BAŞLIK 2		
Bilgisayarlarla İlişkili Suçlar		127
Madde 7 -	Bilgisayarlarla İlişkili Sahtecilik Fiilleri	128
Madde 8 -	Bilgisayarlarla İlişkili Sahtekarlık Fiilleri	130
BAŞLIK - 3		
İçerikle İlişkili Suçlar		133
Madde 9 -	Çocuk Pornografisiyle İlişkili Suçlar	133
BAŞLIK - 4		
Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar		141
Madde 10 -	Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar	141

BAŞLIK - 5	
İlave Yükümlülük ve Yaptırımlar	147
Madde 11 - Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek	147
Madde 12 - Kurumsal Yükümlülük	149
Madde 13 - Yaptırımlar ve Önlemler	152
KISIM - 2	
Usul Hukuku	154
BAŞLIK - 1	
Genel Hükümler	159
Madde 14 - Usul Hükümlerinin Kapsamı	159
Madde 15 - Şartlar ve Önlemler	163
BAŞLIK - 2	
Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması	168
Madde 16 - Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması	175
Madde 17 - Trafik Verilerinin Hızlı Bir Biçimde Korunması ve Kısmen İfşası	180
BAŞLIK - 3	
Üretim Talimatı	185
Madde 18 - Üretim Talimatı	185
BAŞLIK - 4	
Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konması	195
Madde 19 - Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konması	195

XVIII

BAŞLIK - 5

Bilgisayar Verilerinin

Gerçek Zamanlı Olarak Toplanması

209

Madde 20 - Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması

217

Madde 21 - İçerikle İlgili Bilgilere Müdahale Edilmesi

226

KISIM - 3

Yargı Yetkisi

229

Madde 22 - Yargı Yetkisi

229

KISIM - 1

Genel İlkeler

234

BAŞLIK - 1

Uluslararası İşbirliğine İlişkin Genel İlkeler

235

Madde 23 - Uluslararası İşbirliğine İlişkin Genel İlkeler

235

BAŞLIK - 2

İadeye İlişkin İlkeler

238

Madde 24 - İade

238

BAŞLIK - 3

Yardımlaşmaya İlişkin Genel İlkeler

245

Madde 25 - Yardımlaşmaya İlişkin Genel İlkeler

245

Madde 26 - Anında İletilen Bilgiler

251

BAŞLIK - 4

Uluslararası Anlaşmaların Yürürlükte Bulunmadığı

Durumlarda Gelen Yardım Taleplerine

İlişkin Usuller

254

Madde 27 - Uluslararası Anlaşmaların Yürürlükte Bulunmadığı Durumlarda Gelen Yardım Taleplerine İlişkin Usuller

254

Madde 28 - Kullanımda Gizlilik ve Sınırlama

266

KISIM - 2	
Özel Hükümler	270
BAŞLIK - 1	
Geçici Önlemlerin Alınması Konusunda Yardımlaşma	271
Madde 29 - Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması	271
Madde 30 - Korunan Trafik Verilerinin Hızlı Bir Biçimde İfşası	277
BAŞLIK - 2	
Soruşturma Yetkileri Konusunda Yardımlaşma	280
Madde 31 - Saklanan Bilgisayar Verilerine Erişilmesine İlişkin Yardımlaşma	280
Madde 32- Saklanan Bilgisayar Verilerine İzinli Şekilde ya da Bu Verilerin Halka Açık Olduğu Durumlarda Sınır Ötesinden Erişim Sağlamak	281
Madde 33 - Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması Konusunda Yardımlaşma	283
Madde 34 - İçerikle İlgili Verilere Müdahale Edilmesi Konusunda Yardımlaşma	285
BAŞLIK - 3	
24/7 Ağı	287
Madde 35 - 24/7 Ağı	287
BÖLÜM - IV	
Diğer Hükümler	291
Madde 36 - İmza ve Yürürlük	292
Madde 37 - Konvansiyona Katılım	293
Madde 39 - Konvansiyonun Sonuçları	295
Madde 40 - Yazılı Beyanlar	301

XX

Madde 41 -	[Federal Ülkelere İlişkin Hüküm (11)]	302
Madde 42 -	Hakların Saklı Tutulması	305
Madde 44 -	Değişiklikler	307
Madde 45 -	Anlaşmazlıkların Çözümü	308
Madde 46 -	Tarafların İstişarede Bulunmaları	308
NOTLAR		311

SİBER SUÇLAR KONVANSİYON TASLAĞI

Giriş

Avrupa Konseyine üye Ülkeler ve bu belgeyi imza eden diğer Ülkeler;

Avrupa Konseyinin amacının üyeler arasında daha geniş bir birlik sağlamak olduğu düşüncesinden hareketle;

Bu Konvansiyona taraf olan diğer Ülkelerle işbirliğinin geliştirilmesi amacıyla;

Toplumun siber suçlara karşı korunması için atılacak diğer adımlarla birlikte gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yollarıyla ortak bir cezaî politikanın öncelikli olarak kabul edilmesi gereğiyle;

Bilgisayar ağlarının sayısal hale gelmesinin, tek bir noktaya yönelmesinin ve sürekli küreselleşmesinin beraberinde getirdiği önemli değişikliklerin bilincinde olarak;

Bilgisayar ağlarının ve elektronik bilgilerin cezaî suçların işlenmesi amacıyla kullanılabileceği ve bu tür

2 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

suçlara ilişkin delillerin bu ağlarda saklanabileceği ve bu ağlar aracılığıyla aktarılabilmesi riskini göz önünde bulundurarak;

Siber suçlara karşı mücadelede Ülkelerle özel sektör arasında işbirliğinin gerekliliği ve bilgi teknolojilerinin kullanımı ve geliştirilmesine ilişkin meşru hakların korunması ihtiyacının bilincinde olarak;

Siber suçlara karşı etkili mücadelenin cezaî hususlar konusunda artan, hızlı ve verimli bir uluslararası işbirliğiyle gerçekleşeceğine inanarak;

Bu Konvansiyonun, bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetlerin, ayrıca bu sistemlerin, ağların ve verilerin kötü amaçlı kullanımının engellenmesi, ayrıca bu tür faaliyetlerin cezaî niteliklerini belirlemek ve söz konusu cezaî suçlarla etkili biçimde mücadele edilmesi için gerekli yetkilerin temin edilmesini sağlamak, ayrıca, bu tür cezaî suçların hem ulusal hem de uluslararası düzeyde belirlenmesi, soruşturulması ve yargıya götürülmesini kolaylaştırmak ve hızlı ve güvenilir bir uluslararası işbirliğinin sağlanması için gerekli düzenlemelerin yapılmasını temin etmek için gerekli olduğu inancıyla;

Ankara Barosu
Bilgi İşlem Merkezi Yayınları

17000 H 2000
1-3000 1-2000 1-2000

Her bir bireyin herhangi bir müdahale olmaksızın düşünme, düşündüklerini ifade etme, her türlü bilgiyi ve düşünceyi sınırsız şekilde aramak, almak ve iletme hakkını ve özel hayata saygıya ilişkin hakları teyit eden 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Konvansiyonu, 1966 Birleşmiş Milletler Uluslararası Sivil ve Siyasi Haklar Sözleşmesi ve diğer insan hakları anlaşmalarının gereken şekilde belirttiği üzere, yasaların yürürlüğe sokulması hususu ile temel insan haklarına saygı konusunda sağlıklı bir denge belirlenmesine ihtiyaç duyulduğunu bilerek;

1981 Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Konusunda Avrupa Konvansiyonu tarafından da belirtilen kişisel bilgilerin korunmasına hususuna da gerekli önemi vererek;

1989 Birleşmiş Milletler Çocuk Hakları Konvansiyonu ve 1999 Uluslararası Çalışma Örgütü Çocuk İşçilerin Kötü Durumları Konvansiyonunu göz önünde bulundurarak;

Cezaî hususlarda işbirliğine ilişkin mevcut Avrupa Konseyi konvansiyonlarını ve Avrupa Konseyine

üye Ülkeler ve diğer Ülkeler arasındaki benzer nitelikli anlaşmaları dikkate almak, ayrıca, işbu

4 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

Konvansiyonun bilgisayar sistemlerine ve verileriyle ilgili cezaî suçlara ilişkin soruşturmaları ve yasal işlemleri daha etkin kılmak amacıyla başka konvansiyonları desteklemek ve cezaî suçlara ilişkin olarak elektronik ortamda delil toplanabilmesini sağlamak amacına yönelik olduğu hususunun üzerinde durmak suretiyle;

Siber suçlara karşı mücadelede uluslararası anlayış ve işbirliğini geliştirici nitelikteki gelişmelere ve Birleşmiş Milletlerin, OECD'nin, Avrupa Birliğinin ve G8 ülkelerinin bu çerçevedeki çalışmalarına gereken önemi vererek;

İletişime müdahale edilmesi konulu istinabe müzekkerelerine ilişkin olarak, Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonunun uygulanması hakkındaki R (85) sayılı Tavsiye Kararını, telif ve benzeri haklar alanında korsanlık hakkındaki R (88) 2 sayılı Tavsiye Kararını, emniyet birimlerinin kişisel bilgileri kullanımını düzenleyen R (87) 15 sayılı Tavsiye Kararını, telekomünikasyon hizmetleri ve bu çerçevede özellikle telefon hizmetleri alanında kişisel verilerin korunması hakkındaki R (95) sayılı Tavsiye Kararını, bilgisayar suçlarının tanımlanmasına ilişkin olarak ulusal yasama mercilerine kılavuzluk eden ve bilgisayarla ilgili suçlar hakkındaki R (89) 9 sayılı

Tavsiye Kararını, ayrıca, Bilgi Teknolojisi konusundaki cezaî usuller hukukunun sorunları hakkındaki R (95) 13 sayılı Tavsiye Kararını dikkate alarak;

Ulusal ceza hukuku hükümlerini birbirine benzer kılmak ve siber suçlara ilişkin olarak daha etkin sorgulama yapılmasını sağlamak amacına yönelik olan ve Bakanlar Komisyonunun, Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu tarafından siber suçlara yönelik olarak yaptığı çalışmaları desteklemesini tavsiye edici nitelikteki 21. Avrupa Adalet Bakanları Toplantısı (Haziran 1997, Prag) 1 sayılı Kararını, ayrıca, 23. Avrupa Adalet Bakanları Toplantısında (Haziran 2000, Prag) alınan ve toplantıya katılan tarafları, uygun çözümler bulmak suretiyle mümkün olan en fazla sayıda Ülkenin işbu Konvansiyona taraf olmasını temin etmek üzere çalışmalarına devam etmek yönünde teşvik edici nitelikte olan ve, hızlı ve verimli işleyen uluslararası ölçekte ve siber suçlara karşı mücadelenin özel şartlarını göz önünde bulunduracak bir işbirliğine olan ihtiyacı belirten 3 sayılı Kararı dikkate almak suretiyle;

Avrupa Konseyi Devlet ve Hükümet Başkanları tarafından 10-11 Ekim 1997 tarihinde Strazburg'da yapılan İkinci Zirve'de kabul edilen ve yeni bilgi teknolojilerinin gelişimi konusunda Avrupa Konseyinin

6 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

standartları ve değerlerine dayanan ortak tepkiler verme amacına yönelik dayalı Eylem Planını göz önünde bulundurarak;

Aşağıda belirtilen hususlarda mutabık kalmışlardır:

KISIM - I

Terimler

Madde I - Tanımlar

İşbu Konvansiyonda kullanılan aşağıdaki terimler aşağıdaki anlamları ifade edecektir:

- a. “bilgisayar sistemi” terimi, bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı ifade edecektir;
- b. “bilgisayar verisi” terimi, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti ifade edecektir;
- c. “hizmet sağlayıcı” terimi aşağıdaki anlamları ifade edecektir:
 - i. hizmetlerinden faydalanan kullanıcılara bir bilgisayar aracılığıyla iletişim kurma imkânı sağlayan her türlü kamu ve özel sektör tüzel kişisi, ve

8 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

- ii. söz konusu iletişim hizmeti veya bu hizmetin kullanıcıları adına bilgisayar verilerini işleyen veya saklayan diğer her türlü kişi ve kuruluş.
- d. “trafik bilgileri” terimi, bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini veya bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisini ifade edecektir.

BÖLÜM - II
Ulusal Düzeyde Alinacak Önlemler

KISIM - I
Maddî Ceza Hukuku

BAŞLIK - I
***Bilgisayar Veri ve Sistemlerinin Gizliliğine,
Bütünlüğüne ve Kullanıma Açık
Bulunmasına Yönelik Suçlar***

Madde 2 - Yasadışı Erişim

Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, bilgisayar verilerinin elde edilmesi amacıyla veya sahtekârlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesi şeklinde, veya, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler.

Madde 3 - Yasadışı Müdahale

Taraflardan her biri, aşağıda sözü edilen bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar

verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimine haksız surette dahil olma fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemleri ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, sahtekârlık amacını güden bir fiil şeklinde, veya, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler.

Madde 4 - Verilere Müdahale

1. Taraflardan her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin, kasıtlı olarak yapıldıklarında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemleri ve diğer işlemleri yapacaktır.
2. Taraflar, yukarıda Paragraf 1'de tanımlanan fiili, söz konusu fiilin ciddi zararlar sonuçlanması şartına bağlama haklarını saklı tutabilirler.

Madde 5 - Sistemlere Müdahale

Taraflardan her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek

veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

Madde 6 - Cihazların Kötüye Kullanımı

- I. Taraflardan her biri, aşağıdaki fiillerin, kasıtlı ve haksız olarak yapıldıklarında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. Aşağıda sıralanan unsurların, Madde 2 ile 5'te tanımlanan fiillere yönelik olarak kullanılmak amacıyla üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilmesi:
 1. Bilgisayar yazılımları da dahil olmak üzere, esas itibarıyla Madde 2 ile 5'te tanımlanan fiillerden herhangi birinin yapılması amacıyla tasarlanmış veya bu amaca uygun hale getirilmiş cihazlar;
 2. bir bilgisayar sisteminin tamamına veya bir kısmına erişim sağlayan bilgisayar şifreleri, erişim kodları veya benzeri veriler;

12 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

- b. yukarıda (a)(1) ve (2) numaralı paragraflarda sözü edilen unsurların, Madde 2 ile 5'te tanımlanan fiillere yönelik olarak kullanılmak amacıyla elde bulundurulması. Taraflar, alacakları önlemlerde, cezaî sorumluluk doğması için söz konusu unsurlardan belli bir sayıda elde bulundurulması şartı getirebilirler.
2. Yukarıda Paragraf 1'de tanımlanan üretim, satış, kullanım amacıyla tedarik, ithal, dağıtım, başka surette elde etme veya elde bulundurma fiillerinin, işbu Konvansiyonun 2 ile 5 numaralı maddelerinde tanımlanan fiillere yönelik olarak kullanılmak amacıyla değil de, örneğin, bir bilgisayar sisteminin yetkili kişilerce test edilmesi veya korunması amacıyla yapıldığı durumlarda, işbu madde hükümleri cezaî yükümlülük doğurur şekilde yorumlanmayacaktır.
3. Taraflardan her biri, söz konusu hakkın 1(a) ve 2 numaralı paragraflarda belirtilen unsurların satışına, dağıtımına ve başka suretle kullanıma sunulmasına ilişkin durumlarda kullanılmaması şartıyla, işbu maddenin 1 numaralı paragrafını uygulamama haklarını saklı tutmaktadır.

BAŞLIK 2 *Bilgisayarlarla İlişkili Suçlar*

Madde 7 - Bilgisayarlarla İlişkili Sahtecilik Fiilleri

Taraflardan her biri, söz konusu verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiilinin, söz konusu farklı verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapıldığında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar, bu gibi durumlarda cezaî sorumluluğun ortaya çıkmasını, hile veya benzeri bir sahtekârlık niyetinin mevcut olması şartına bağlayabilirler.

Madde 8 - Bilgisayarlarla İlişkili Sahtekârlık Fiilleri

Taraflardan her biri, aşağıdaki faaliyetlerde bulunmak suretiyle bir başkasının mülkiyetinin ziyanına sebep olma fiilinin, kasıtlı ve haksız olarak yapıldığında, kendi ulusal mevzuatı kapsamında cezaî

14 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:

- a. Sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma;
- b. Sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme.

BAŞLIK - 3
İçerikle İlişkili Suçlar

Madde 9 - Çocuk Pornografisiyle İlişkili Suçlar

- I. Taraflardan her biri, aşağıdaki fiillerin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek;
 - b. bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak ya da çocuk pornografisine erişim sağlamak;
 - c. bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ya da yaymak;
 - d. kişinin, bir bilgisayar sistemi üzerinden kendisi ya da başkası için çocuk pornografisi temin etmesi;
 - e. bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak

16 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

2. Yukarıdaki paragraf 1'de geçen "çocuk pornografisi" terimi aşağıdakileri görsel anlamda teşhir eden pornografik malzemeler anlamına gelmektedir:
 - a. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı;
 - b. Cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı;
 - c. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren görüntüler;
3. Yukarıdaki paragraf 1'de geçen "reşit olmayan kişi" terimi, 18 yaşından küçük kişiler anlamına gelmektedir. Ancak, Taraflardan herhangi biri, daha düşük bir yaş sınırı belirleyebilir. Söz konusu yaş sınırı 16'dan az olmayacaktır.
4. Taraflardan her biri, paragraf 1(d) ve 1(e), ayrıca 2(b) ve 2(c)'yi kısmen uygulama ya da hiç uygulamama haklarını saklı tutar.

BAŞLIK - 4
Telif Haklarının ve Benzer Hakların
İhlaline İlişkin Suçlar

Madde 10 - Telif Haklarının ve Benzer Hakların
İhlaline İlişkin Suçlar

1. Taraflardan her biri, kendi yasalarında tanımlandığı şekliyle telif haklarının ihlali fiilinin, Edebi ve Sanatsal Eserlerin Korunmasına Yönelik Bern Konvansiyonu çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Telif Hakları Anlaşması uyarınca, kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlakî haklar bu hükme tabi değildir.
2. Taraflardan her biri, kendi yasalarında tanımlandığı şekliyle telif haklarına benzer hakların ihlali fiilinin, Roma'da imza edilen Oyuncuların, Fonogram Yapımcılarının ve Yayım Kuruluşlarının Korunması Hakkında Konvansiyon

18 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

(Roma Konvansiyonu), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Oyunculuk ve Fonogramlar Anlaşması uyarınca, kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlakî haklar bu hükme tabi değildir.

3. Taraflardan herhangi biri, belirli durumlarda işbu maddedeki paragraf 1 ve 2 çerçevesinde cezaî yükümlülük ihdas etmeme hakkını, bu konuda başka yasal yolların bulunması ve bu hakkın saklı tutulmasının söz konusu Tarafın işbu maddedeki paragraf 1 ve 2'de belirtilen uluslararası belgelerdeki uluslararası yükümlülüklerin dışına çıkmasına sebep olmaması şartıyla, saklı tutar.

BAŞLIK - 5

İlave Yükümlülük ve Yaptırımlar

Madde 11 - Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek

1. Taraflardan her biri, işbu Konvansiyonun 2 ila 10. Maddelerinde tanımlanan suçların işlenmesine, söz konusu suçların işlenmesi maksadıyla yardım veya yataklık edilmesi fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
2. Taraflardan her biri, işbu Konvansiyonun 3 ila 5, 7, 8, 9 (1) a ve 9 (1) c Maddelerinde tanımlanan suçları işlemeye teşebbüs edilmesi fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
3. Her bir Ülke, işbu Maddedeki paragraf 2'yi kısmen uygulama ya da hiç uygulamama hakkını saklı tutar.

Madde 12 - Kurumsal Yükümlülük

1. Taraflardan her biri, müstakilen ya da bir tüzel kişilik birimi adına hareket eden ve tüzel kişilik nezdinde aşağıda belirtilen bakımlardan önde gelen bir konumu haiz olan herhangi bir kişi tarafından tüzel kişilik menfaatine işlenen ve işbu Konvansiyonda tanımlanan bir cezaî suça ilişkin olarak tüzel kişiliklerin yükümlü tutulabilmesini temin etmek için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. tüzel kişiliği temsil etme yetkisi bakımından;
 - b. tüzel kişilik adına karar alma yetkisi bakımından;
 - c. tüzel kişilik dahilinde kontrolde elinde tutma bakımından.
2. Paragraf 1'de belirtilenlere ek olarak, paragraf 1'de belirtilen bir kişi tarafından gözetim ya da denetim yapılmamasının işbu Sözleşmede tanımlanan bir cezaî suçun tüzel kişilik yetkilerine tabi herhangi bir kişi tarafından tüzel kişilik menfaatine işlenmesine sebep olması halinde tüzel kişiliğin yükümlü tutulabilmesini temin etmek üzere gerekli işlemleri yapacaktır.

3. İlgili Tarafın yasal düzenlemelerine tabi olmak kaydıyla, bir tüzel kişiliğin yükümlülüğü cezaî, adlî ya da idarî nitelikli olabilir.
4. Söz konusu yükümlülük, ilgili suçu işleyen kişinin cezaî yükümlülüğünün hilafına olmayacaktır.

Madde 13 - Yaptırımlar ve Önlemler

1. Taraflardan her biri, Madde 2 ile 11'de tanımlanan cezaî suçların, özgürlüklerin kısıtlanmasını da içeren etkin, adil ve caydırıcı yaptırımlarla cezalandırılabilmesini temin etmek amacıyla gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
2. Taraflardan her biri, Madde 12 uyarınca yükümlü tutulan tüzel kişiliklerin, parasal cezalarını da içeren cezaî nitelikli olan ya da olmayan etkin, adil ve caydırıcı yaptırımlara tabi olmalarını temin edeceklerdir.

KISIM - 2
Usul Hukuku

BAŞLIK - 1
Genel Hükümler

Madde 14 - Usul Hükümlerinin Kapsamı

1. Taraflardan her biri, işbu Kısımda belirtilen yetki ve usullerin esas alınması suretiyle bazı cezaî soruşturma ve işlemlerin yapılabilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
2. Madde 21'de aksi özellikle belirtilen durumlar hariç olmak üzere, Taraflardan her biri, paragraf 1'de değinilen yetki ve usulleri aşağıdakilere ilişkin olarak uygulamaya koyacaktır:
 - a. İşbu Konvansiyonda Madde 2 ila 11'de tanımlanan cezaî suçlar;
 - b. Bir bilgisayar sistemi aracılığıyla işlenen diğer cezaî suçlar;
 - c. Cezaî bir suça ilişkin olarak elektronik ortamda delil toplanması.

- 3.a. Taraflardan her biri Madde 20'de belirtilen önlemleri, kendisi tarafından belirlenecek suçlara ya da suç kategorilerine ilişkin olarak uygulama hakkını saklı tutar. Ancak, ilgili Tarafça söz konusu önlemlerin uygulandığı suçlar ya da suç kategorileri, yine ilgili Tarafın Madde 21'de belirtilen önlemleri uyguladığı suçlardan daha sınırlı bir çerçevede olmayacaktır. Taraflardan her biri, suç ya da suç kategorilerinin, Madde 20'de belirtilen önlemin en geniş şekilde uygulanabilecek olmasını sağlamak üzere en geniş şekilde belirlenmesi gerektiğini göz önünde bulunduracaktır.
- b. İşbu Konvansiyonun kabul edildiği dönemde yürürlükte bulunan ulusal mevzuatındaki sınırlamalar dolayısıyla işbu Madde 20 ve 21'de belirtilen önlemleri herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak uygulayamayan herhangi bir Taraf,
- i. söz konusu sistemin belirli bir kullanıcı grubunun menfaatine işletiliyor olması,
 - ii. söz konusu sistemin halka açık iletişim şebekelerini kullanmıyor olması ve halka açık

ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması,

halinde, söz konusu aktarıma ilişkin olarak bu önlemleri uygulamama hakkını saklı tutar.

Taraflardan her biri, Madde 20 ve 21'de belirtilen önlemlerin en geniş şekilde uygulanabilecek olmasını sağlayacak şekilde görüş bildirilmesi gerektiğini göz önünde bulunduracaktır.

Madde 15 - Şartlar ve Önlemler

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

hakkaniyet ilkesinin tesis edilmesini sağlayacaktır.

2. Yukarıda belirtilen şartlar ve önlemler, ilgili yetki ya da usulün niteliği göz önüne alındığında uygun olduğu ölçüde, söz konusu yetki ya da usulün kapsamı ve süresine ilişkin adli ya da başka nitelikli bağımsız gözetim, gerekçelerin haklılığına ilişkin başvuru işlemi, ya da sınırlama yapılmasını da, diğer hususlarla birlikte, içerecektir.
3. Kamu yararının, özellikle de adaletin sağlıklı şekilde yürütülmesinin söz konusu olduğu durumlarda, Taraflar, işbu Kısımda belirtilen yetki ve usullerin, üçüncü şahısların yetki, sorumluluk, ve meşru menfaatleri üzerindeki etkisini göz önünde bulunduracaktır.

BAŞLIK - 2
Saklanan Bilgisayar Verilerinin Korunmasının
Kolaylaştırılması

Madde 16 - Saklanan Bilgisayar Verilerinin
Korunmasının Kolaylaştırılması

1. Taraflardan her biri, yetkili mercilerinin bir bilgisayar sistemi aracılığıyla saklanan bazı bilgisayar verilerinin, bu çerçevede trafik bilgilerinin, korunmasının kolaylaştırılması yönünde talimat vermeleri ya da söz konusu hususu benzer şekilde temin etmelerini sağlamak amacıyla, özellikle bilgisayar verilerinin kaybedilmesinin ya da değiştirilmesinin söz konusu olabileceğine dair gerekçelerin mevcut bulunduğu durumlarda, gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
2. Herhangi bir Tarafın, bir kişinin mülkiyetinde ya da kontrolünde bulunan saklı bazı bilgisayar verilerinin korunması amacıyla ilgili kişiye talimat vermek suretiyle yukarıdaki paragraf 1 hükmünü yürürlüğe sokması halinde, söz konusu Taraf, ilgili kişinin bu bilgisayar verilerinin doğruluğunu azami 90 gün olmak üzere gereken süre boyunca korumasını temin etmek ve bu suretle

yetkili mercilerin bu bilgilerin açıklanmasını isteyebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Taraflardan her biri, bilgisayar verilerini koruması gereken görevlinin ya da başka bir kişinin bu hususa ilişkin usulleri ilgili Tarafın ulusal mevzuatında belirtilen süre boyunca gizli tutması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Madde 17 - Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması

- I. Taraflardan her biri Madde 16 uyarınca korunması gereken trafik bilgilerine ilişkin olarak aşağıdaki hususlara ilişkin olarak gerekli olabilecek yasama işlemlerini ve diğer işlemlerini yapacaktır:
 - a. trafik bilgilerinin korunması işleminin kolaylaştırılması hususunun, söz konusu bilgilerin bir ya da birden daha fazla hizmet

sağlayıcı tarafından iletilmiş olmasına
bakılmaksızın sağlanması;

b. ilgili Tarafın yetkili merciine veya bu merciin
belirlediği bir kişiye, ilgili Tarafın söz
konusu hizmet sağlayıcıları ve bilgilerin
iletildiği yolu belirleyebilmesini sağlayacak
ölçüde açıklama yapılması işleminin
kolaylaştırılması.

2. İşbu maddede sözü geçen yetki ve usuller
Madde 14 ve 15'e tabi olacaktır.

BAŞLIK - 3
Üretim Talimatı

Madde 18 - Üretim Talimatı

1. Taraflardan her biri, yetkili mercilerinin aşağıdaki hususlarda talimat verme konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. Söz konusu Tarafın ulusal sınırlar içinde bulunan bir kişinin, söz konusu kişinin mülkiyetinde ya da kontrolünde bulunan ve bir bilgisayar sisteminde veya bilgisayar verilerini saklamak için kullanılan başka bir cihazda saklanan bazı bilgisayar verilerini vermesi yönünde;
 - b. Söz konusu Tarafın ulusal sınırları içinde hizmet veren bir hizmet sağlayıcının, mülkiyetinde ya da kontrolünde bulunan ve sözü geçen hizmete ilişkin olan abone bilgilerini vermesi yönünde;
2. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.
3. İşbu maddede kullanılan "abone bilgileri" terimi, bilgisayar verisi şeklinde ya da başka şekillerde

saklanan, ve hizmet sağlayıcının elinde bulunan ve verilen hizmetlere ilişkin olan trafik ya da içerikle ilgili bilgilerinin haricindeki bilgiler anlamına gelmektedir. Bu bilgiler kullanılarak;

- a. kullanılan iletişim hizmetinin türü, teknik imkanlar ve hizmet süresi;
- b. abonenin kimliği, posta ya da bulunduğu yerin adresi, telefon numarası ve aboneye ulaşılacak diğer numaralar, hizmet sözleşmesi veya düzenlemesi esas alınarak verilen fatura ve ödeme bilgileri;
- c. hizmet sözleşmesi veya düzenlemesi esas alınarak verilen ve iletişim ekipmanının kurulduğu bölgeye ilişkin olan diğer bilgiler belirlenebilmektedir.

BAŞLIK - 4
Saklanan Bilgisayar Verilerinin Aranması ve
Bunlara El Koyulması

Madde 19 - Saklanan Bilgisayar Verilerinin Aranması
ve Bunlara El Konulması

1. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde aşağıdakileri arama ya da bunlara benzer şekilde erişim sağlama konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. bir bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan bilgisayar verileri; ve
 - b. bilgisayar verilerinin saklandığı cihazlar.
2. Tarafların her biri, yetkili mercilerinin paragraf 1 (a) uyarınca belirli bir bilgisayar sisteminde ya da bu sistemin bir parçasında arama yapması ya da bunlara erişim sağlaması söz konusu olduğunda, ayrıca, aranan verilerin kendi ulusal sınırları içindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçeleri bulunduğunda, söz konusu

mercilerin arama ya da erişim işlemlerini bu sistemi kapsayacak şekilde genişletebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

3. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koyma ya da bunları başka şekillerde koruma altına alınması konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Bu işlemler arasında, aşağıdakilerin yapılabilmesine yönelik yetkilerin sağlanması bulunacaktır:

- a. herhangi bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara el konulması ya da bunların benzer şekilde koruma altına alınması;
- b. bu bilgisayar verilerinin kopyalanıp alıkonulması;
- c. söz konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi; ve

- d. erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez kullanılamaz hale getirilmesi ya da silinmesi.
4. Taraflardan her biri, yetkili mercilerinin ilgili bilgisayar sisteminin işleyişi hakkında ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında bilgi sahibi olan herhangi bir kişiye, paragraf 1 ve 2'de belirtilen işlemlerin yapılabilmesi için gerekli bilgileri makul şekilde vermesi yönünde talimat vermesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
5. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

BAŞLIK - 5
Bilgisayar Verilerini Gerçek Zamanlı
Olarak Toplanması

Madde 20 - Trafik Bilgilerinin Gerçek
Zamanlı Olarak Toplanması

- I. Taraflardan her biri, yetkili mercilerinin aşağıdaki hususlarda yetkili olması için gerekli olabilecek yasal işlemleri ve diğer işlemleri yapacaktır:
 - a. trafik bilgilerinin gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplanması ya da kaydedilmesi, ve
 - b. herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde
 - i. trafik bilgilerini gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplamasının ya da kaydetmesinin, ve
 - ii. trafik bilgilerinin gerçekli zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle işbirliği yapmasının ve

onlara bu hususta yardımcı olmasının temin edilmesi

Söz konusu trafik bilgileri, bir bilgisayar sistemi üzerinden aktarılan ve ilgili Tarafın ulusal sınırları içinde özel iletişim sayılan bilgilerdir.

2. Yerleşik ulusal hukuki düzenlemeler dolayısıyla paragraf I (a)'da belirtilen işlemleri yapamayan herhangi bir Taraf, bunların yerine, kendi ulusal sınırları içinde özel iletişim sayılan trafik bilgilerinin gerçek zamanlı olarak söz konusu sınırlar dahilindeki teknik imkanlar kullanılmak suretiyle toplanması ya da kaydedilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapabilir.
3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu Maddede verilen herhangi bir yetki hakkındaki esasları ve bilgileri gizli tutmakla yükümlü kılmak için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Madde 21 - İçerikle İlgili Bilgilere Müdahale Edilmesi

- I. Taraflardan her biri, yetkili mercilerinin, ulusal yasalarca belirlenecek ciddi nitelikli suçlara ilişkin olarak aşağıdakilerin yapılması hususunda yetkili kılınması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
 - a. İçerikle ilgili bilgilerin gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplanması ya da kaydedilmesi, ve
 - b. herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde
 - i. içerikle ilgili bilgileri gerçek zamanlı olarak, ilgili Tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplamasının ya da kaydetmesinin, ve
 - ii. içerikli ilgili bilgilerin gerçekli zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle işbirliği yapmasının ve onlara bu hususta yardımcı olmasının temin edilmesi

İçerikle ilgili söz konusu bilgiler, bir bilgisayar sistemi üzerinden aktarılan ve ilgili Tarafın ulusal sınırları içinde özel iletişim sayılan bilgilerdir.

2. Yerleşik ulusal hukuki düzenlemeler dolayısıyla paragraf 1 (a)'da belirtilen işlemleri yapamayan herhangi bir Taraf, bunların yerine, kendi ulusal sınırları içinde özel iletişim sayılan içerikli ilgili bilgilerin gerçek zamanlı olarak söz konusu sınırlar dahilindeki teknik imkanlar kullanılmak suretiyle toplanması ya da kaydedilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapabilir.
3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu Maddede verilen herhangi bir yetki hakkındaki esasları ve bilgileri gizli tutmakla yükümlü kılmak için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
4. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

KISIM - 3
Yargı Yetkisi

Madde 22 - Yargı Yetkisi

1. Taraflardan her biri, işbu Konvansiyonda Madde 2 ile 11 arasında tanımlanan suçlara ilişkin olarak yargı yetkisi tesis etmek için gerekli olabilecek yasama işlemlerini ve diğer işlemleri, söz konusu suçların
 - a. İlgili Tarafın ulusal sınırları içinde; ya da
 - b. İlgili Taraf bandırası taşıyan seyir halindeki bir gemide; ya da
 - c. İlgili Tarafın yasaları çerçevesinde kayıtlı bulunan bir uçakta; ya da
 - d. İlgili Tarafın vatandaşlarından biri tarafından işlenmesi, ve söz konusu suçların işlendikleri yerde ceza hukukuna tabi bulunması ya da herhangi bir Ülkenin yargı yetkisine sahip olduğu sınırlar dışında işlenmesi hallerinde

yapacaktır.

2. Taraflardan her biri, işbu maddede ya da herhangi bir bölümünde paragraf (1) b ile (1) d çerçevesinde belirtilen yargı yetkilerini yalnızca belirli durum ve şartlarda uygulama ya da uygulamama hakkını saklı tutar.
3. Taraflardan her biri, ulusal sınırları dahilinde bulunan bir zanlının yalnızca tabiyeti esas alınarak bir iade talebini müteakiben başka bir Tarafa iade edilmemesi durumunda, işbu Konvansiyonda Madde 24 paragraf 1'de belirtilen suçlara ilişkin olarak yargı yetkisi tesis etmek için gerekli olabilecek işlemleri yapacaktır.
4. İşbu Konvansiyon herhangi bir ulusal hukuk çerçevesinde uygulanan cezaî yargı yetkisini kapsam dışı bırakmamaktadır.
5. Herhangi bir suç zannına ilişkin olarak birden fazla Tarafın işbu Konvansiyona göre yargı yetkisine sahip bulunduğunu iddia etmesi halinde, söz konusu Taraflar dava için en uygun yargı merciinin belirlenmesi amacıyla görüş alışverişinde bulunacaklardır.

BÖLÜM - III
Uluslararası İşbirliği

KISIM - I
Genel İlkeler

BAŞLIK - I
Uluslararası İşbirliğine İlişkin Genel İlkeler

Madde 23 - Uluslararası İşbirliğine İlişkin Genel İlkeler

Taraflar, işbu bölüm hükümleri çerçevesinde ve, cezaî meselelerde uluslararası işbirliğine ilişkin uluslararası belgelerin, tek taraflı ya da karşılıklı mevzuata dayalı sözleşmelerin, ve ulusal yasaların bilgisayar sistemlerine ve verilerine ilişkin soruşturma ve davalarda, ya da cezaî suçlara ilişkin olarak elektronik ortamda delil toplanması amacıyla mümkün olan en geniş biçimde kullanılabilecek şekilde uygulanması vasıtasıyla işbirliğine gideceklerdir.

BAŞLIK - 2
İadeye İlişkin İlkeler

Madde 24 - İade

1. a. İşbu madde, Taraflar arasında işbu Konvansiyonda Madde 2 ile 11 çerçevesinde tanımlanan cezaî suçlara ilişkin olan iade işlemleri konusunda, söz konusu suçların, ilgili Tarafların yasaları çerçevesinde en az bir yıl özgürlükten mahrum bırakılması şeklinde ya da daha ağır nitelikli bir ceza ile cezalandırılabilir olması şartıyla, geçerli olacaktır.
- b. Tek taraflı ya da karşılıklı mevzuat ya da iade anlaşması, bu çerçevede Avrupa İade Sözleşmesi (ETS No.24) esas alınmak suretiyle varılan ve iki ya da daha fazla taraf arasında yürürlükte bulunan anlaşmalar çerçevesinde asgari bir cezanın uygulanmasının söz konusu olduğu durumlarda, söz konusu anlaşma ya da sözleşme çerçevesindeki asgari ceza geçerli olacaktır.
2. İşbu Maddede paragraf 1 çerçevesinde tanımlanan cezaî suçlar, iki ya da daha fazla Taraf arasındaki iade anlaşmaları çerçevesinde iadeye konu olabilen suçlar olarak

addedilecektir. Taraflar, bu suçları söz konusu iade anlaşmaları çerçevesinde iadeye konu suçlar olarak addedecekleri yönünde taahhütte bulunmaktadır.

3. İade işlemini bu konuda bir anlaşma olması şartına bağlayan herhangi bir Tarafın, kendisi ile iade anlaşması bulunmayan bir Taraftan iade talebi alması halinde, talebi alan Taraf, işbu Konvansiyonu, işbu maddede paragraf I çerçevesinde tanımlanan herhangi bir cezaî suça ilişkin olarak gerekli hukuki zemin sayabilir.
4. İade işlemini bu konuda bir anlaşma olması şartına bağlamayan Taraflar, işbu maddede paragraf I'de tanımlanan cezaî suçları, birbirleri arasında iade işlemi yapılmasına konu olan suçlar olarak tanıyacaklardır.
5. İade işlemi, bu işlemi gerçekleştirmesi talep edilen Tarafın yasalarındaki şartlara ya da yürürlükte bulunan iade anlaşmalarına, ayrıca iade işlemi gerçekleştirmesi talep edilen Tarafın bu işlemi gerçekleştirmeyi reddetmesine zemin teşkil eden gerekçelere tabi olacaktır.
6. İşbu maddede paragraf I çerçevesinde belirtilen bir cezaî suça ilişkin olarak iade işlemi

gerçekleştirilmesi yönünde bir talebin, yalnızca iadesi istenen kişinin tabiyeti dolayısıyla veya iade işlemi gerçekleştirmesi talep edilen Tarafın söz konusu suça ilişkin olarak yargı yetkisini haiz olduğunu düşünmesi sebebiyle reddedilmesi halinde, iade işlemi gerçekleştirmesi talep edilen Taraf, kendisinden bu işlemi talep eden Tarafın isteği üzerine, meseleyi dava edilmesi amacıyla yetkili mercilerine iletecek ve nihai sonucu iade talebinde bulunan Tarafa gereken şekilde bildirecektir. Bu merciler, kararlarını verirken ve soruşturmalarını sürdürürken, benzer nitelikte bir suçun kendi yasaları çerçevesinde söz konusu olmuş olması durumunda hareket edecekleri şekilde çalışacaklardır.

7. a. Taraflardan her biri, herhangi bir anlaşmanın olmadığı durumlarda iade ya da geçici tutuklama talebini iletecek ya da bu yönde bir talebi alacak yetkili mercilerden her birinin adını ve adresini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.
- b. Avrupa Konseyi Genel Sekreteri, Tarafların yukarıda belirtilen şekilde tespit ettikleri yetkililerin kaydını tutacak ve bu kaydı sürekli

güncelleyecektir. Taraflar, bu kayıta yer alan bilgilerin her zaman doğru olmasını temin edeceklerdir.

BAŞLIK - 3
Yardımlaşmaya İlişkin Genel İlkeler

Madde 25 - Yardımlaşmaya İlişkin Genel İlkeler

1. Taraflar, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlara ilişkin soruşturma ve davaların yürütülmesi ya da cezaî bir suça ilişkin olarak elektronik ortamda delil toplanması konusunda birbirlerine mümkün olan en geniş ölçüde yardımcı olacaklardır.
2. Taraflardan her biri, Madde 27 ila 35 çerçevesindeki yükümlülüklerin yerine getirilmesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaklardır.
3. Taraflardan her biri, acil durumlar söz konusu olduğunda faks ve elektronik posta gibi hızlı iletişim araçlarıyla yardım verilmesi ya da irtibat kurulması talebinde bulunabilir. Ancak, söz konusu araçların güvenlik ve doğruluk açısından gerekli ölçülerde olması (gerektiği takdirde şifreleme kullanarak) ve kendisinden talepte bulunulan Tarafın isteği üzerine resmi teyit mesajı gönderilmesi gerekecektir. Kendisinden talepte bulunulan Taraf, ilgili hızlı iletişim

araçları vasıtasıyla iletilen talebi kabul edecek ve bu talebe gerekli cevabı verecektir.

4. İşbu Bölümdeki Maddelerde açıkça belirtilen durumlar hariç olmak üzere, karşılıklı olarak yardım verilmesi hususu, kendisinden talepte bulunulan Tarafın yasalarındaki şartlara veya karşılıklı olarak yardım verilmesine ilişkin anlaşmaların şartlarına, ayrıca kendisinden yardım talep edilen Tarafın bu talebi reddetmesine gerekçe olabilecek şartlara tabi olacaktır. Kendisinden talepte bulunulan Taraf, Madde 2 ile 11 çerçevesinde belirtilen suçlara ilişkin olarak yardım vermeyi, yalnızca söz konusu suçları mali nitelikli olarak değerlendirdiği gerekçesine dayanarak, reddetme hakkını kullanmayacaktır.
5. Kendisinden talepte bulunulan Tarafın, işbu bölüm hükümlerine uygun olarak, yardım verme hususunu, ilgili suçun işlendiği her iki yerde de cezaî nitelik taşıması şartına bağlayabildiği durumlarda, talep edilen yardıma konu olan söz konusu suça zemin teşkil eden fiilin yardım talep eden Tarafın yasaları çerçevesinde cezaî nitelik taşıması halinde bu şart, kendisinden yardım talep edilen Tarafın bu suçu yardım talep eden

Tarlafla aynı kategoriye koymasına ya da aynı terimlerle tespit etmesine bakılmaksızın, yerine getirilmiş sayılacaktır.

Madde 26 - Anında İletilen Bilgiler

1. Herhangi bir Taraf, ulusal yasalarının sınırları çerçevesinde, kendi yürüttüğü soruşturmalar çerçevesinde edindiğı bilgileri, bunların açıklanmasının söz konusu bilgileri alan Tarafa işbu Konvansiyonda tanımlanan cezaî suçlara ilişkin soruşturma ve davaların başlatılması konusunda yardımcı olacağını ya da ilgili Tarafın işbirliği talebinde bulunmasını temin edeceğini düşündüğü takdirde, başka bir Tarafa önceden izin almaksızın iletebilir.
2. Söz konusu bilgiler verilmeden önce, bu bilgileri veren Taraf bilgilerin gizli tutulmasını ya da belirli şartlarda kullanılmasını talep edebilir. Bilgileri alan Taraf, bu talebin gereğini yerine getiremeyecek olması halinde bilgileri veren Tarafa bildirimde bulunacak, bilgileri veren Taraf da bilgilerin yine de verilir verilemeyeceğini tespit edecektir. Bilgileri alan Tarafın belirli şartlar çerçevesinde kabul ettiğı bilgiler, söz konusu Taraf açısından bağlayıcı olacaktır.

BAŞLIK - 4

***Uluslararası anlaşmaların Yürürlükte Bulunmadığı
Durumlarda Gelen Yardım Taleplerine
İlişkin Usuller***

**Madde 27 - Uluslararası anlaşmaların Yürürlükte
Bulunmadığı Durumlarda Gelen Yardım
Taleplerine İlişkin Usuller**

1. Tek taraflı ya da karşılıklı mevzuata dayalı herhangi bir yardım anlaşması ya da düzenlemesinin söz konusu olmadığı durumlarda işbu maddede paragraf 2 ile 10 çerçevesinde geçen hükümler geçerli olacaktır. Bu tür bir anlaşma ya da düzenlemenin söz konusu olduğu durumlarda, ilgili Taraflar bu anlaşmaların yerine bu madde hükümlerinin bir kısmını ya da tamamını geçerli saymayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.
2. a. Taraflardan her biri yardım taleplerinde bulunmak, bu taleplere cevap vermek, bu taleplerin gereğini yerine getirmek, ya da bunların gereğini yerine getirecek mercilere bu talepleri iletmekle görevli bir merci ya da merciler belirleyecek.

- b. Söz konusu merciler birbirleriyle doğrudan haberleşeceklerdir
 - c. Taraflardan her biri, herhangi bir anlaşmanın olmadığı durumlarda işbu paragraf gereğini yapacak yetkili mercilerden her birinin adını ve adresini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.
 - d. Avrupa Konseyi Genel Sekreteri, Tarafların yukarıda belirtilen şekilde tespit ettikleri yetkililerin kaydını tutacak ve bu kaydı sürekli güncelleyecektir. Taraflar, bu kayıta yer alan bilgilerin her zaman doğru olmasını temin edeceklerdir.
3. İşbu Madde çerçevesindeki karşılıklı yardım talepleri, talepte bulunan Tarafça tespit edilecek usullere göre işleme konacaktır. Kendisinden talepte bulunulan Tarafın yasalarında bu hususa aykırı bir durum varsa bu hüküm geçerli olmayacaktır.
4. Kendisinden talepte bulunulan Taraf, Madde 25 Paragraf (4) çerçevesindeki red gerekçelerine ek

olarak, aşağıdaki hususlar söz konusu olduğunda yardım vermeyi kabul etmeyebilir:

- a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da
 - b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi
5. Kendisinden talepte bulunulan Taraf, herhangi bir talebe ilişkin olarak işlem yapmasının yetkili mercilerince sürdürülmekte olan cezaî soruşturma ya da işlemlere zarar vermesinin söz konusu olabileceği durumlarda, bu talebe ilişkin işlemleri tehir edebilir.
6. Kendisinden talepte bulunulan Taraf, yardım vermeyi red ya da tehir etmeden önce, ve gerekli durumlarda yardım talep eden Tarafla görüş alışverişinde bulunarak, yardımın kısmen verilip verilemeyeceği ya da bazı şartlara tabi olarak verilebileceği hususunu karara bağlar.

7. Kendisinden talepte bulunulan Taraf, yardım talebinin işleme konmasından hasıl olan neticeyi talepte bulunan Tarafa bildirecektir. Talebin reddi ya da tehiri halinde bunlara ilişkin gerekçeler bildirilecektir. Talebin yerine getirilmesini imkansız kılan ya da önemli ölçüde geciktirecek olan gerekçeler de bildirilecektir.
8. Talepte bulunan taraf, kendisinde talepte bulunulan Tarafın, işbu Bölüm çerçevesinde iletilen taleplerin esasına ve içeriğine ilişkin bilgileri, söz konusu talebin karşılanması için bilgilerin gizli tutulmamasının gerekli olduğu durumlar hariç olmak üzere, gizli tutmasını isteyebilir. Kendisinden talepte bulunulan Taraf, bilgilerin gizli tutulmasına ilişkin talebi gerçekleştiremeyecek olması halinde, bu durumu talepte bulunan Tarafa derhal bildirecek, ve talepte bulunan Taraf talebin yine de gerçekleştirilip gerçekleştirilmeyeceği yönünde karar verecektir.
9. a. Acil durumlarda, yardım talepleri ya da bu taleplere ilişkin yazışmalar, doğrudan talep eden Tarafın adli mercileri aracılığıyla kendisinden yardım talep edilen Tarafın adli mercilerine iletilebilir. Bu tür durumlarda, yardım talep eden

Taraf, yapılan yazışmaların bir nüshasını yetkili mercii aracılığıyla kendisinden yardım edilen Tarafın yetkili merciiine gönderecektir.

- b. İşbu paragraf çerçevesinde iletilecek talepler ve sair yazışmalar Interpol aracılığıyla gönderilebilir.
- c. İşbu maddenin (a) paragrafına uygun olarak talepte bulunulması ve ilgili merciiin bu talebe ilişkin olarak işlem yapamıyor olması halinde, söz konusu merci, talebi ulusal düzeyde yetkili olan mercie ileticek ve bu durumu yardım talep eden Tarafa bildirecektir.
- d. İşbu paragraf çerçevesinde iletilen ve zorlayıcı unsurlar içermeyen talepler ya da yazışmalar, talepte bulunan Tarafın yetkili mercilerince kendisinden talepte bulunulan Tarafın yetkili mercilerine doğrudan iletilebilir.
- e. Taraflardan her biri, işbu paragraf çerçevesinde iletilen taleplerin daha etkin şekilde ele alınabilmesi için yetkili mercie iletilmesi gerektiğini Avrupa Konseyi Genel Sekreterine, onay, kabul, tasdik ya da giriş belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde, bildirecektir.

Madde 28 - Kullanımda Gizlilik ve Sınırlama

1. Tek taraflı ya da karşılıklı mevzuata dayalı herhangi bir yardım anlaşması ya da düzenlemesinin söz konusu olmadığı durumlarda işbu madde hükümleri geçerli olacaktır. Bu tür bir anlaşma ya da düzenlemenin söz konusu olduğu durumlarda, ilgili Taraflar bu anlaşmaların yerine bu madde hükümlerinin bir kısmını ya da tamamını geçerli saymayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.
2. Kendisinden talepte bulunulan Taraf, aşağıdaki şartlara bağlı olarak herhangi bir talep karşılığında bilgi ya da malzeme verebilir:
 - a. Hukuki yardım talebinin bu şartın yerine getirilmemesi halinde karşılanamadığı durumlarda söz konusu bilgi ya da malzemelerin gizli tutulması, ya da
 - b. Söz konusu bilgi ya da malzemelerin talepte belirtilenler dışında başka bir soruşturma ya da yasal işlem için kullanılmaması
3. Talepte bulunan Taraf, paragraf 2'de belirtilen şartları yerine getiremeyecek olması halinde,

diğer Tarafı bu konuda bilgilendirecek, diğer Taraf da bilgilerin her halükarda verilmesini isteyip istemediği konusunda karar verecektir. Şartın kabul edilmesi talepte bulunan Taraf açısından bağlayıcı olacaktır.

4. Paragraf 2'de belirtilen şartların yerine getirilmesi kaydıyla bilgi ya da malzeme veren herhangi bir Taraf, diğer Tarafın söz konusu şarta ilişkin olarak bilgilerin ve malzemelerin nasıl kullanıldığı konusunda açıklama yapmasını isteyebilir.

KISIM - 2
Özel Hükümler

BAŞLIK - 1
Geçici Önlemlerin Alınması Konusunda
Yardımlaşma

Madde 29 - Saklanan Bilgisayar Verilerinin
Korunmasının Kolaylaştırılması

1. Taraflardan herhangi biri, başka bir Tarafın ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla saklanan ve talepte bulunan Tarafın araştırma, erişim, el koyma ya da benzer şekilde elde tutma amacıyla yardım talebine konu etmeyi düşündüğü ya da açıklanmasını talep edeceği verilerin korunması işleminin kolaylaştırılmasını söz konusu Taraftan talep edebilir.
2. Paragraf 1 çerçevesinde bilgilerin korunması amacıyla yapılan talepler:
 - a. Verilerin korunmasını isteyen mercii
 - b. cezaî soruşturmaya ya da işleme konu olan suç ve ilgili esasların özetini

- c. saklanan bilgisayar verilerini elinde bulunduran kişiyi ya da bilgisayar sisteminin yerini belirleyebilmek için elde bulunan bilgileri
 - d. verilerin korunmasının gerekliliğini; ve
 - e. ilgili Tarafın saklanan bilgisayar verilerine ilişkin olarak araştırma, erişim, el koyma ya da benzer şekilde elde tutma işlemi ve açıklama yapılması amacıyla yardım talebinde bulunmayı düşünüyor olduğunu belirtici nitelikte olacaktır.
3. Kendisinden talepte bulunulan Taraf, ilgili talebi aldıktan sonra ilgili verileri ulusal yasalarına uygun olarak korunması işleminin kolaylaştırılması için gerekli önlemleri alacaktır. Herhangi bir talebe cevap verilmesinin söz konusu olduğu durumlarda, verilerin korunmasının, ilgili suçun her iki Tarafın sınırları dahilinde de cezaî niteliğinin bulunması şartı aranmayacaktır.
4. İşbu Konvansiyonda Madde 2 ile 11 çerçevesinde tanımlananlar dışındaki suçlara ilişkin olarak verilerin araştırılması, verilere erişim sağlanması, el konulması ya da verilerin

benzer şekilde elde tutulması veya açıklanması amacıyla yardım sağlanması amacına yönelik bir talebe cevap vermek için ilgili suçun her iki Tarafın sınırları dahilinde de cezaî niteliğinin bulunması şartını arayan bir Taraf, söz konusu şartın verilerin açıklandığı tarihte yerine getirilemiyor olduğunu gösteren gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması amacıyla iletilen talepleri reddetme hakkını saklı tutar.

5. Yukarıdakilere ek olarak, verilerin korunması amaçlı bir talep ancak aşağıdaki durumlarda reddedilebilir:

- a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da
- b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi.

6. Kendisinden yardım talep edilen Taraf, verilerin korunması işleminin verilere gelecekte ulaşılmasına sebep olacağını ya da yardım talep eden Tarafın yürüttüğü soruşturmanın gizliliğini zedeleyeceğini ya da buna başka şekillerde zarar vereceğini düşünmesi halinde, bu düşüncesini yardım talep eden Tarafa en kısa sürede bildirecek, talepte bulunan Taraf da yardım talebinin gereğinin her halükarda yapılmasını isteyip istemediği yönünde karar verecektir.
7. Paragraf 1'de belirtilen talebe cevaben yerine getirilen koruma işlemi en az 60 gün sürecek, bu suretle talepte bulunan Tarafın verilerin araştırılması, verilere erişim sağlanması, el konulması ya da verilerin benzer şekilde elde tutulması veya açıklanması amacıyla talepte bulunabilmesi sağlanacaktır. Bu yönde bir talebin alınmasının ardından, veriler söz konusu talep konusunda bir karar verilene dek korunacaktır.

Madde 30 - Korunan Trafik Verilerinin Açıklanması İşleminin Kolaylaştırılması

1. Özel iletişim sayılan trafik verilerinin korunmasına ilişkin olarak Madde 29

çerçevesinde iletilen talebin yerine getirilmesi sırasında, kendisinden yardım talep edilen Tarafın başka bir Ülkedeki bir hizmet sağlayıcının söz konusu iletişimin sağlanmasında dahli bulunduğunu keşfetmesi halinde, söz konusu Taraf, talepte bulunan Tarafa, ilgili hizmet sağlayıcının ve verilerin aktarıldığı yolun belirlenmesi için gerekli olacak ölçüde trafik verisini en kısa sürede açıklayacaktır.

2. Paragraf 1 çerçevesinde trafik verilerinin açıklanması işlemi ancak aşağıdaki durumlarda gerçekleşmeyebilir:

- a. yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; ya da
- b. söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi.

BAŞLIK - 2

Soruşturma Yetkileri Konusunda Yardımlaşma

Madde 31 - Saklanan Bilgisayar Verilerine Erişilmesine İlişkin Yardımlaşma

1. Taraflardan herhangi biri, kendisinde talepte bulunulan Tarafın ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla saklanan verilerin, bu çerçevede Madde 29 uyarınca korunan verilerin, söz konusu Tarafça araştırılması, bunlara erişilmesi, el konulması ya da bunların benzer şekilde elde tutulması ya da açıklanması amacıyla söz konusu Taraftan talepte bulunabilir.
2. Kendisinden yardım talep edilen Taraf, bu talebe, Madde 23'te belirtilen uluslararası belgelerin, düzenlemelerin ve yasaların, ayrıca işbu Bölümün ilgili hükümlerinin uygulamaya konması suretiyle cevap verecektir.
3. Söz konusu talebe cevap verilmesi işlemi aşağıdakiler söz konusu olduğunda daha hızlı gerçekleştirilecektir:

- a. ilgili verilerin kaybolmasının ya da değiştirilmesinin söz konusu olabileceğine dair gerekçeler bulunması; ya da
- b. paragraf 2'de belirtilen belge, düzenleme ve yasaların başka şekillerde hızlı bir işbirliği sağlıyor olması

**Madde 32 - Saklanan Bilgisayar Verilerine İzinli
Şekilde ya da Bu Verilerin Halka Açık
Olduğu Durumlarda Sınır Ötesinden
Erişim Sağlamak**

Herhangi bir Taraf, diğer Tarafın iznini almaksızın:

- a. kullanıma açık (herkesin ulaşabileceği bir kaynaktan gelen) saklı bilgisayar verilerine, bu verilerin coğrafi konumuna bakılmaksızın erişebilir; ya da
- b. ulusal sınırları içinde bulunan bir bilgisayar sistemi aracılığıyla, başka bir Taraf dahilinde bulunan saklı bilgisayar verilerine, bu verileri söz konusu bilgisayar sistemi üzerinden açıklama yetkisini haiz olan kişinin iznini yasal olarak aldıktan sonra erişebilir ya da bunları alabilir.

**Madde 33 - Trafik Verilerinin Gerçek Zamanlı
Olarak Toplanması Konusunda
Yardımlaşma**

1. Taraflar, kendi ulusal sınırları içinde özel iletişim olarak görülen ve bir bilgisayar sistemi üzerinden aktarılan trafik verilerinin gerçek zamanlı olarak toplanması için birbirlerine yardımcı olacaklardır. Paragraf 2'ye tabi olmak kaydıyla, bu yardım ulusal yasalarda belirtilen şartlara ve usuller çerçevesinde gerçekleşecektir.
2. Taraflardan her biri, en azından, ulusal sınırlar içinde trafik verilerinin gerçek zamanlı olarak toplanabilmesini mümkün kılanlara benzer nitelikteki cezaî suçlar konusunda yardım sağlayacaktır.

**Madde 34 - İçerikle İlgili Verilere Müdahale Edilmesi
Konusunda Yardımlaşma**

Taraflar, bir bilgisayar sistemi aracılığıyla aktarılan özel iletişimlere ilişkin içerik bilgilerinin gerçek zamanlı olarak toplanması veya kaydedilmesine ilişkin olarak, ulusal yasalarının izin verdiği ölçüde birbirlerine yardımcı olacaklardır.

BAŞLIK - 3
24 Saat 7 Gün Boyunca Elverişli Ağ

Madde 35 - 24/7 Ağı

- I. Taraflardan her biri, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlar konusundaki soruşturma ve davaların yürütülmesi ya da cezaî bir suça ilişkin olarak elektronik ortamda delil toplanabilmesi işlemlerine ilişkin olarak en kısa sürede yardım temin edilmesini sağlamak üzere haftanın 7 günü 24 saat boyunca elverişli olan bir irtibat noktası belirleyecektir. Söz konusu yardım, aşağıdakilerin kolaylaştırılması ya da ulusal yasa ve uygulamaların uygun görmesi halinde doğrudan yapılması ile olacaktır:
 - a. teknik görüş verilmesi;
 - b. Madde 29 ve 30 uyarınca verilerin korunması; ve
 - c. Delil toplanması, yasal bilgilerin verilmesi, şüphelilerin yerlerinin bulunması.
2. a. Tarafların irtibat noktaları hızlı iletişim sağlanmasına elverişli nitelikte olacaktır.

- b. Herhangi bir Tarafın belirlediği irtibat noktasının, ilgili Tarafın uluslararası yardımlardan ya da iadede sorumlu merciinin ya da mercilerinin bir parçası olmaması durumunda, söz konusu irtibat noktasının ilgili merci ya da mercilerle hızlı bir şekilde koordinasyon sağlayabilecek nitelikte olması gerekmektedir.
3. Taraflardan her biri, ağı rahat biçimde işletilmesini sağlayacak eğitimi ve teçhizatı haiz personel bulunmasını temin edecektir.

BÖLÜM - IV
Diğer Hükümler

Madde 36 - İmza ve Yürürlük

1. İşbu Konvansiyon, Avrupa Konseyine üye Ülkelerin ve bu belgenin hazırlanmasında payı bulunan üye olmayan Ülkelerin imzasına açık olacaktır.
2. İşbu Konvansiyon, tasdik edildikten, kabul edildikten ve onaylandıktan sonra yürürlüğe girecektir. Tasdik, kabul ve onay evrakı Avrupa Konseyi Genel Sekreterine teslim edilecektir.
3. İşbu Konvansiyon, en az üçü Avrupa Konseyi üyesi olan beş Ülkenin, işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.
4. İşbu Konvansiyon, Konvansiyonun bağlayıcılığını kabul eden Ükelere ilişkin olarak, söz konusu Ülkelerin işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten

sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 37 - Konvansiyona Katılım

1. İşbu Konvansiyonun yürürlüğe girmesinin ardından Avrupa Konseyi Bakanlar Kurulu, Konvansiyonu İmza Eden Ülkelerle görüş alışverişinde bulunup onların oybirliğiyle ilgili karara varmalarının ardından, Konsey üyesi olmayan ve işbu Konvansiyonun hazırlanmasında payı bulunmayan herhangi bir Ülkeyi Konvansiyona katılmaya davet edebilir. Bu konudaki karar, Avrupa Konseyi Yasası Madde 20 (d)'de belirtilen çoğunluk tarafından ve Bakanlar Kurulunda bulunmaya yetkili İmza Eden Ülkelerin yetkili temsilcilerinin oybirliğiyle alınacaktır.
2. İşbu Konvansiyon, paragraf 1 çerçevesinde Konvansiyona katılan herhangi bir Ülkeye ilişkin olarak, söz konusu Ülkenin işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettiği tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 38 - Belirli Bölgelerde Yürürlük

1. Ülkelerden herhangi biri, tasdik, kabul, onay ya da katılım belgesini imza ettiğinde ya da bu belgeyi teslim ettiğinde işbu Konvansiyonun hangi bölge ya da bölgelerde yürürlükte bulunacağını belirleyebilir.
2. Taraflardan herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılı beyanda bulunmak suretiyle, işbu Konvansiyonun söz konusu beyanda belirtilen bölgelerde de yürürlüğe girmesini temin edebilir. İşbu Konvansiyon, söz konusu bölgelerde, Genel Sekreterin belirtilen beyanı teslim aldığı tarihten sonraki üç ayın ardından gelen ayın ilk gününde yürürlüğe girecektir.
3. Yukarıdaki iki paragraf çerçevesinde iletilen herhangi bir yazılı beyan, bu beyanda belirtilen bölgelere ilişkin olarak, Avrupa Konseyi Genel Sekreterine hitaben gönderilecek bir bildirimle geri çekilebilir. Söz konusu beyanın geri çekilmesi işlemi, bu bildirimin Genel Sekreter tarafından teslim alındığı tarihten sonraki üç ayın ardından gelen ayın ilk gününde yürürlük kazanacaktır.

Madde 39 - Konvansiyonun Sonuçları

1. İşbu Konvansiyon, Taraflar arasında yürürlükte bulunan çok taraflı ya da ikili anlaşmaları ya da düzenlemeleri, ve bu çerçevede aşağıdakilerin hükümlerini, desteklemek amacına yöneliktir:
 - 13 Aralık 1957 tarihinde Paris'te imzaya açılan Avrupa İade Konvansiyonu (ETS No. 24)
 - 20 Nisan 1959 tarihinde Strazburg'ta imzaya açılan Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonu (ETS No. 30)
 - 17 Mart 1987 tarihinde imzaya açılan Cezaî Meselelerde Yardımlaşma Hakkında Avrupa Konvansiyonuna İlişkin Ek Protokol (ETS No. 99)
2. İki ya da daha fazla sayıda Tarafın işbu Konvansiyonda ele alınan konulara ilişkin olarak daha önceden yapmış bulundukları bir anlaşma olduğu veya bu konuları başka şekillerde karara bağlamış oldukları takdirde, veya bunların gelecekte söz konusu olmaları halinde, ilgili Taraflar bu sözleşme ya da anlaşmaları da

uygulama veya ilişkilerini bunlara uygun olarak düzenleme hakkını haiz olacaklardır. Ancak, Tarafların işbu Konvansiyonda, ele alınan hususlara ilişkin meseleleri işbu Konvansiyonda belirtilen şekilde karara bağlamamış olmaları halinde, bu Tarafların hususa ilişkin olarak alacakları kararlar işbu Konvansiyonun amaç ve ilkeleriyle tutarsız olmayacaktır.

3. İşbu Konvansiyon içeriği, Taraflardan herhangi birine ilişkin diğer haklar, sınırlamalar, yükümlülükler ve sorumlulukları etkilemeyecektir.

Madde 40 - Yazılı Beyanlar

Ülkelerden herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılan bir bildirim vasıtasıyla, tasdik, kabul, onay ve katılım belgesini imzaladığında ya da teslim ettiğinde, Madde 2, Madde 3, Madde 6, paragraf 1 (b), Madde 7, Madde 9, paragraf 3 ve Madde 27, paragraf 9 (e) çerçevesinde belirtilen şekilde ek unsurlar talep edebileceğini beyan edebilir.

Madde 41 - Federal Ükelere İlişkin Hüküm

1. Federal bir Ülke, işbu Konvansiyonda Bölüm II çerçevesinde belirtilen yükümlülükleri, merkezi hükümeti ile federal Ülkeyi oluşturan Eyaletler

- ve benzer nitelikteki idari bölgeler arasındaki ilişkilerin dayandığı esaslarla tutarlı şekilde kabul etme hakkını, Bölüm III çerçevesinde işbirliğine gidebilecek olmak şartıyla, saklı tutar.
2. Söz konusu hakkı Paragraf I'de belirtilen şekilde saklı tutan bir federal Ülke, bu hakkın saklı tutulmasına ilişkin şartları, Bölüm II'de belirtilen işlemlerin yapılmasına ilişkin yükümlülüklerden hariç tutulacak ya da bu yükümlülükleri önemli ölçüde azaltacak şekilde uygulayamaz.
3. Federal hükümet, işbu Konvansiyonun, federal Ülkeyi oluşturan ve federasyonun anayasal sistemi gereği yasama işlemleri yapması gerekmeyen Eyaletlerin ya da diğer idari birimlerin yargı yetkisine tabi bulunarak uygulanan hükümlerine ilişkin olarak, söz konusu Eyaletlerin yetkili mercilerini federal hükümetin tercih ettiği görüşü de ileterek bilgilendirecek ve bu mercileri söz konusu hükümlerin gereğini yapmaları hususunda teşvike çalışacaktır.

Madde 42 - Hakların Saklı Tutulması

Ülkelerden herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben yazılan bir bildirim vasıtasıyla,

tasdik, kabul, onay ve katılım belgesini imzaladığında ya da teslim ettiğinde, Madde 4, paragraf 2, Madde 6, paragraf 3, Madde 9, paragraf 4 ve Madde 10, paragraf 3, Madde 11, paragraf 3, Madde 14 paragraf 3, Madde 22, paragraf 2, Madde 29, paragraf 4, ve Madde 41, paragraf 1 çerçevesinde belirtilen hakları saklı tutabileceğini beyan edebilir. Bunların dışında saklı tutulabilecek başka bir hak bulunmamaktadır.

**Madde 43 - Saklı Tutulan Hakların Durumu ve
Hakların Saklı Tutulması İşleminde
Vazgeçilmesi**

1. Madde 42 çerçevesinde herhangi bir hakkı saklı tutan bir Taraf, söz konusu hakkı saklı tutma fiilinden, Genel Sekretere hitaben yazılı bildirimde bulunmak suretiyle kısmen ya da tamamen vazgeçebilir. Vazgeçme işlemi, ilgili bildirimin Genel Sekreter tarafından alındığı tarihte yürürlük kazanacaktır. Söz konusu bildirimde, vazgeçme işleminin bildirim dahilinde belirtilen tarihte yürürlük kazanacağını belirtilmesi ve bu tarihin bildirimin Genel Sekreter tarafından alındığı tarihten sonrasına denk düşmesi halinde,

vazgeçme işlemi daha sonraki tarihte yürürlük kazanacaktır.

2. Herhangi bir hakkı Madde 42'de belirtilen şekilde saklı tutan herhangi bir Taraf, söz konusu saklı tutma fiilinden şartlar elverdiğinde vazgeçecektir.
3. Avrupa Konseyi Genel Sekreteri, Madde 42'de belirtilen şekilde bir ya da birkaç hakkı saklı tutan Taraflarla, söz konusu saklı tutma fiilinden vazgeçmelerinin temini amacıyla belirli aralıklarla gerekli görüşmelerde bulunabilir.

Madde 44 - Değişiklikler

1. Herhangi bir Taraf işbu Konvansiyonda değişiklik yapılması amacıyla teklifte bulunabilir. Söz konusu değişiklikler Avrupa Konseyi Genel Sekreteri tarafından Avrupa Konseyine üye Ükelere, işbu Konvansiyonun hazırlanmasında payı bulunan üye olmayan Ükelere, ayrıca, Madde 37'ye uygun olarak işbu Konvansiyona katılan ya da katılmaya davet edilen herhangi bir Ülkeye bildirilecektir.
2. Herhangi bir tarafın yapılmasını teklif ettiği değişiklikler, Suçlarla İlgili Problemler Hakkında

Avrupa Komisyonuna bildirilecek, bu Komisyon da teklif edilen değişikliğe ilişkin görüşünü Bakanlar Kuruluna sunacaktır.

3. Bakanlar Kurulu, yapılması teklif edilen değişikliği ve Suçlarla İlgili Problemler Hakkında Avrupa Komisyonunun bu konudaki görüşünü değerlendirdikten ve üye ülke olmayan Taraflarla görüş alışverişinde bulunduktan sonra değişikliği kabul edebilir.
4. Bakanlar Kurulunun işbu maddedeki paragraf 3 çerçevesinde kabul ettiği değişikliğe ilişkin metin, kabul edilmesi amacıyla Taraflara gönderilecektir.
5. İşbu Maddedeki Paragraf 3 çerçevesinde yapılması kabul edilen herhangi bir değişiklik, Tarafların tamamının söz konusu değişikliği kabul ettiklerini Genel Sekretere bildirdikleri tarihten sonraki otuzuncu günde yürürlüğe girecektir.

Madde 45 - Anlaşmazlıkların Çözümü

1. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, İşbu Konvansiyonun yorumlanması

ve uygulanmasına ilişkin olarak sürekli şekilde bilgilendirilecektir.

2. Taraflar arasında işbu Konvansiyonun yorumlanması ya da uygulanmasına ilişkin olarak herhangi bir anlaşmazlık doğması halinde, Taraflar bu anlaşmazlığı görüşme yoluyla ya da kendilerinin tercih edeceği başka bir barışçıl yolla gidermeye çalışacaklardır. Bu çerçevede söz konusu anlaşmazlığın, ilgili Tarafların üzerinde anlaşacağı şekilde, Suçlarla İlgili Problemler Hakkında Avrupa Komisyonuna, kararları Tarafları bağlayıcı bir tahkim heyetine, ya da Uluslararası Adalet Divanına iletilmesi söz konusu olabilecektir.

Madde 46 - Tarafların Görüş Alışverişinde Bulunmaları

1. Taraflar, gerekli durumlarda, aşağıdaki hususların kolaylaştırılması amacıyla görüş alışverişinde bulunacaklardır:
 - a. işbu Konvansiyondan verimli bir şekilde kullanıma konması ve uygulanması, bu çerçevede bu hususlara ilişkin problemlerin ve işbu Konvansiyon çerçevesinde iletilen

beyanlara ya da saklı tutulan haklara ilişkin neticelerin belirlenmesi;

b. siber suçlara ilişkin olan önemli hukuki, siyasi ya da teknolojik gelişmeler ve elektronik ortamda bilgi toplanması konularında bilgi alışverişinde bulunulması;

c. Konvansiyonun başka belgelerle desteklenmesi ya da Konvansiyonda değişiklik yapılması.

2. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, paragraf 1'de belirtilen görüş alışverişlerinden hasil olan neticeler konusunda belirli aralıklarla sürekli bilgilendirilecektir.

3. Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, gerekli durumlarda, paragraf 1'de belirtilen şekilde görüş alışverişinde bulunulmasını kolaylaştıracak ve Taraflara, işbu Konvansiyonun başka belgelerle desteklenmesi ya da Konvansiyonda değişiklik yapılması konusunda yardım etmek üzere gerekli işlemleri yapacaktır. İşbu Konvansiyon yürürlüğe girdikten sonra en geç üç yıl içinde Suçlarla İlgili Problemler Hakkında Avrupa Komisyonu, Taraflarla işbirliğine giderek Konvansiyon

- hükümlerinin gözden geçirecek ve gerekli değişikliklere ilişkin teklifte bulunacaktır.
4. Masrafların Avrupa Konseyince üstlenildiği durumlar hariç olmak üzere, paragraf 1 hükümlerinin yerine getirilmesi için yapılan harcamalar Taraflarca kendilerinin belirleyeceği şekilde karşılanacaktır.
5. Avrupa Konseyi Sekreterliği, Taraflara, işbu Madde çerçevesindeki işlemlerin yapılması konusunda yardımcı olacaktır.

Madde 47 - Konvansiyondan Ayrılma

1. Taraflardan herhangi biri, Avrupa Konseyi Genel Sekreterine hitaben bildirimde bulunmak suretiyle işbu Konvansiyondan dilediği zaman ayrılabilir.
2. Konvansiyondan ayrılma işlemi, ilgili bildirimin Genel Sekreter tarafından alınmasından sonraki üç ayın bitiminden sonraki ayın ilk gününde yürürlük kazanacaktır.

Madde 48 - Bildirimler

Avrupa Konseyi Genel Sekreteri, Avrupa Konseyine üye Ülkelere, işbu Konvansiyonun

hazırlanmasında payı bulunan üye olmayan Ülkelere, ayrıca, işbu Konvansiyona katılan ya da katılmaya davet edilen Ülkelere aşağıdaki hususlarda bildirimde bulunacaktır:

- a. herhangi bir belgenin imza edilmesi;
- b. herhangi bir tasdik, kabul, onay ya da katılım belgesinin teslim edilmesi;
- c. işbu Konvansiyonun Madde 36 ve 37 uyarınca yürürlüğe girdiği herhangi bir tarih;
- d. Madde 40 ve 41 çerçevesinde iletilen herhangi bir beyan ya da Madde 42 çerçevesinde herhangi bir hakkı saklı tutma fiili;
- e. İşbu Konvansiyona ilişkin başka işlemler, bildirimler ve sair muhaberat.

Aşağıda imzaları bulunan yetkili kişiler işbu Konvansiyonu imza etmişlerdir.

İşbu Konvansiyon ... şehrinde ... 2001 tarihinde her ikisi de asıl metin kabul edilen İngilizce ve Fransızca tek nüsha şeklinde imza edilmiş olup, bu nüsha Avrupa Konseyi arşivlerinde saklanacaktır. Avrupa Konseyi Genel Sekreteri, Avrupa Konseyine

78 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

üye Ükelere, işbu Konvansiyonun hazırlanmasında payı bulunan üye olmayan Ükelere, ayrıca işbu Konvansiyona katılmaya davet edilen Ükelere işbu Konvansiyonun tasdikli nüshalarını gönderecektir.

AÇIKLAYICI RAPOR TASLAĞI

I. GİRİŞ

1. Bilgi teknolojilerinde yaşanan devrim, toplum üzerinde köklü bir değişim yaratmıştır ve bu değişimin yakın gelecekte sürmesi muhtemeldir. Birçok işlem daha kolay hale gelmiştir. Başlangıçta, toplumun sadece belirli bazı kesimleri bilgi teknolojileri yardımıyla çalışma prosedürlerini akılcı hale getirebilirken, artık bu değişimden etkilenmeyen hemen hemen hiçbir kesim kalmamıştır. Bilgi teknolojisi, çeşitli biçimlerde, insanların neredeyse bütün faaliyetlerine nüfuz etmiştir.
2. Bilgi teknolojisinin en belirgin özelliklerinden biri, telekomünikasyon teknolojisinin evrimi üzerinde şu ana kadar yaptığı ve ileride yapacağı etkidir. İnsan sesinin iletilmesine yönelik klasik telefon teknolojisinin yerini ses, metin, müzik, hareketsiz ve hareketli resim şeklindeki çok büyük miktarlarda verinin alışverişini mümkün kılan sistemler almıştır. Bu alışveriş artık sadece insanlar arasında değil, aynı zamanda insanlar ve bilgisayarlar ya da bilgisayarların kendi aralarında da olabilmektedir. Çevrim anahtarlı bağlantıların

(Circuit-switched connection) yerini Paket Anahtarlama Ağı almıştır. Artık doğrudan doğruya bağlantı kurulması önemli değildir; verilerin belli bir adrese gidecek ya da isteyen herkes tarafından erişilecek şekilde bir bilgi ağına girilmesi yeterlidir.

3. Elektronik posta kullanımının yaygınlaşması ve İnternet üzerinden çok sayıda web sitesine ulaşılabilmesi bu gelişmelere örnektir. Bu gelişmeler toplumumuzu köklü bir değişime uğratmıştır.
4. Bilgisayar sistemlerindeki bilgilere erişimin ve bu bilgileri araştırmanın kolaylığı, bilgilerin coğrafi mesafelerden bağımsız olarak alışverişi ve yayımı konusundaki neredeyse sınırsız olanaklarla birleşince, mevcut bilgilerin miktarının ve bunlardan üretilebilecek bilgi birikiminin katlanarak büyümesine yol açmıştır.
5. Bu gelişmeler benzeri görülmemiş ekonomik ve toplumsal değişimlere yol açmıştır, ancak, konunun yeni suç türlerinin ortaya çıkması ve eski suçların yeni teknolojiler aracılığıyla gerçekleştirilmesi gibi bir de karanlık tarafı vardır: Ayrıca, suçların sonuçları eskiye göre çok

daha geniş alanlara yayılabilmektedir çünkü artık bu suçlar coğrafi kısıtlamalara ve ulusal sınırlara tabi olmaktan çıkmıştır. Son zamanlarda zararlı bilgisayar virüslerinin bütün dünyaya yayılması bu gerçeği kanıtlamaktadır. Bilgisayar sistemlerini korumaya yönelik teknik önlemler, suçu önlemeye ve caydırmaya yönelik hukuki önlemlerle bir arada uygulanmalıdır.

6. Yeni teknolojiler mevcut hukuki kavramların geçerliliğini tehdit etmektedir. Artık bilgi akışı ve iletişim dünya genelinde daha kolay gerçekleştirilmektedir. Sınırlar artık bu akışı sınırlandırmamaktadır. Suçluların, eylemlerini, bunların sonuçlarının ortaya çıktığı yerlerden farklı yerlerde gerçekleştirmesi, giderek daha fazla rastlanan bir olgu haline gelmiştir. Ancak yerel yasalar genellikle spesifik bir bölgeyle sınırlıdır. Bu yüzden yaşanan sorunlara getirilen çözümler uluslararası hukuk çerçevesinde yer almalıdır. Bu ise, uygun uluslararası hukuki araçların benimsenmesini gerekli kılar. Bu Konvansiyon ile, yeni Bilgi Toplumunda insan haklarına gerekli önem gösterilerek bu güçlüğün aşılması hedeflenmektedir.

II. HAZIRLIK ÇALIŞMALARI

7. Avrupa Suç Sorunları Komitesi (CDPC), CDPC/103/211196 sayılı kararla, Kasım 1996'da siber suçlarla ilgilenecek bir uzmanlar komitesi kurmaya karar vermiştir. CDPC, kararını şu gerekçeye dayandırmıştır:
8. "Bilgi teknolojisi alanındaki hızlı gelişmeler, modern toplumun bütün kesimlerini doğrudan etkilemiştir. Telekomünikasyon ve bilgi sistemlerinin bütünleşmesi, her türlü iletişimin mesafeden bağımsız olarak saklanması ve aktarılmasını mümkün kılarak birçok yeni olanak yaratmıştır. Dünyanın neresinde olduğundan bağımsız olarak hemen hemen herkesin her türlü elektronik bilgi hizmetine erişimini mümkün kılan İnternet gibi bilgi otobanlarının ve ağlarının ortaya çıkışı, bu gelişmeleri hızlandırmıştır. İletişim ve bilgi hizmetlerine bağlanan kullanıcılar "siber uzay" adı verilen, meşru amaçlar için kullanılan, ancak kötü kullanıma da açık olan, ortak bir uzay yaratmışlardır. Söz konusu "siber uzay suçları", bilgisayar sistemlerinin ve telekomünikasyon ağlarının bütünlüğüne, ulaşılabilirliğine ve gizliliğine karşı işlenebileceği gibi, geleneksel

suçların işlenmesinde bu ağların sunduğu hizmetlerin kullanılmasını da içerebilir. Bu suçların sınırlar arası niteliği, örneğin İnternet aracılığıyla işlenebilmesi, ulusal icra makamlarının mülkiliğiyle çelişki halindedir.

9. Bu nedenle ceza hukuku, siber uzayın olanaklarının kötü kullanımı ve meşru çıkarlara zarar vermek için son derece gelişmiş olanaklar sunan bu teknolojik gelişmeleri yakından takip etmelidir. Bilgi ağlarının sınır ötesi yapılarından dolayı bu tür kötü kullanımlarla mücadele etmek için uluslararası düzeyde ortak çalışmalar yürütmek gerekmektedir. (89) 9 sayılı Tavsiye belirli bilgisayar kötü kullanım biçimleriyle ilgili ulusal kavramların birbirlerine yaklaşmasını sağlamıştır ama bu yeni olgularla mücadelede gerekli verimliliğin sağlanması ancak bağlayıcı uluslararası bir araçla mümkün olabilir. Böyle bir araç çerçevesinde, uluslararası işbirliği önlemlerine ek olarak, maddi hukuk ve usul hukukuyla ilgili sorunlar ve bilgi teknolojisinin kullanımıyla yakından bağlantılı konular ele alınmalıdır."

10. Bunlara ek olarak, CDPC -kendi isteği üzerine- Profesör H.W.K. Kaspersen tarafından

hazırlanmış Raporu da dikkate almıştır. Raporda şu sonuca ulaşılmıştır: " ... Konvansiyon gibi Tavsiyeden daha çok yükümlülük getiren bir hukuki araca başvurulmalıdır. Böyle bir Konvansiyonda maddi ceza hukuku konularının yanı sıra ceza usulleriyle ilgili sorunlar ve uluslararası ceza hukuku usulleri ve sözleşmeleri de ele alınmalıdır. (1) Maddi hukukla ilgili R (89) 9 (2) sayılı Tavsiyeye ek Raporda ve bilgi teknolojisiyle bağlantılı usul hukuku sorunlarıyla ilgili R (95) 13 (3) sayılı Tavsiyede de benzer sonuçlara ulaşılmıştır.

11. Yeni komitenin özel görev tanımı şöyledir:

- i. "Bilgisayar suçlarına ilişkin R (89) 9 sayılı ve bilgi teknolojisiyle bağlantılı ceza usulleri hukuku sorunlarına ilişkin R (95) 13 sayılı Tavsiyeleri göz önünde bulundurarak, özellikle aşağıdaki konuları incelemek:
- ii. siber uzay suçları, özellikle İnternet gibi telekomünikasyon ağlarının kullanımı yoluyla işlenen suçlar, örneğin yasadışı para işlemleri, yasadışı hizmetler sunmak,

telif haklarının ihlali ile insan haysiyetini ve küçüklerin korunmasını ihlal eden suçlar;

iii. uluslararası işbirliği için tanımlar, yaptırımlar ve siber uzaydaki, İnternet hizmet sağlayıcılarının da içinde bulunduğu aktörlerin sorumluluğu gibi ortak yaklaşımların gerekli olabileceği diğer maddi ceza hukuku konuları;

iv. teknoloji ortamında cebri kuvvetlerin kullanımı -sınır ötesi kullanım olasılığı da dahil olmak üzere- ve uygulanabilirliği, örneğin telekomünikasyonun önlenmesi ve bilgi ağlarının -örneğin İnternet yoluyla- elektronik olarak izlenmesi, bilgi-işlem sistemlerinde saklanan verilerin aranması ve bunlara el konması (İnternet siteleri de dahil olmak üzere), yasadışı malzemeyi erişilemez yapmak ve hizmet sağlayıcıların özel yükümlülüklerine uymasını sağlamak, bu arada bilgi güvenliğine yönelik şifreleme gibi bazı önlemlerin yaratacağı sorunları da göz önüne almak.

v. bilgi teknolojisi suçlarında yargı yetkisi sorunu, örneğin suçun işlendiği yeri (locus

delicti) ve buna uygun olarak hangi yasanın geçerli olduğunu belirlemek, ayrıca birden çok yargı yetkisinin olduğu durumlarda ne "bis idem" sorunu ve pozitif yargı yetkisi çatışmalarının nasıl çözüleceği ve negatif yargı yetkisi çatışmalarından nasıl kaçınılacağı meselesi;

- vi. siber uzay suçlarının soruşturulmasında Avrupa Konvansiyonlarının Ceza Alanında Uygulanması Uzmanları Komitesiyle (PC-OC) yakın işbirliği içinde uluslararası işbirliği meseleleri.

Komite, i-v. bentler için, mümkün olduğu ölçüde, ve uluslararası sorunlara özel bir önem göstererek, bağlayıcı bir hukuki araç ve uygun olduğu durumlarda özel konularla ilgili ikinci derecede tavsiye taslakları hazırlamalıdır. Komite, teknolojik gelişmeleri göz önünde bulundurarak diğer konularla ilgili öneriler yapabilir."

11. CDPC'nin kararına uygun olarak, Bakanlar Kurulu, Bakan Vekillerinin (4 Şubat 1997 tarihindeki) 583. toplantısında alınan CM/Del/Dec(97)583 sayılı kararla "Siber Uzay

Suçları Uzmanları Komitesi (PC-CY)" adı verilen yeni bir 'komite oluşturdular. PC-CY Komitesi Nisan 1997'de çalışmaya başladı ve siber suçlara ilişkin uluslararası bir konvansiyon taslağı üzerinde görüşmelere başladı. Başlangıçtaki görev tanımına göre Komitenin çalışmalarını 31 Aralık 1999 tarihinde bitirmesi gerekiyordu. Bu tarihte Komite Konvansiyon taslağındaki bazı konularla ilgili görüşmeleri tamamlayacak durumda olmadığı için, Bakan Vekillerinin CM/Del/Dec(99)679 sayılı kararıyla görev tanımı 31 Aralık 2000'e uzatıldı. Avrupa Adalet Bakanları, birincisi ülkelerin ceza hukuku hükümlerinin birbirlerine yaklaştırılması ve bu suçlar için etkili soruşturma yollarının kullanılmasının mümkün kılınması için Bakanlar Kurulunun CDPC'nin siber suçlarla ilgili olarak yürüttüğü çalışmaları desteklemesini tavsiye eden, 21. Konferansta (Prag, Haziran 1997) kabul edilen 1 numaralı Kararla, ikincisi görüşmelere katılan tarafların çalışmalarını mümkün olan en çok sayıda Ülkenin Konvansiyona taraf olmasını sağlayacak uygun çözümleri bulmaya yönelik olarak yürütmesini teşvik eden, ve siber suçlarla mücadelenin özel koşullarını gerektiği gibi ele alan hızlı ve etkin

bir uluslararası işbirliğine duyulan gereksinimi tasdik eden, Avrupa Adalet Bakanlarının 23. Konferansında (Londra, Haziran 2000) kabul edilen 3 numaralı Kararla olmak üzere iki kez görüşmelerle ilgili desteklerini bildirdiler. Avrupa Birliğine Üye Ülkeler Mayıs 1999'da benimsenen bir Ortak Konumla PC-CY'nin çalışmalarını desteklediklerini belirttiler.

12. PC-CY Komitesi, Nisan 1997 ile Aralık 2000 tarihleri arasında 10 genel kurul toplantısı ve açık uçlu Taslak Grubuyla 15 toplantı yaptı. Uzmanlar, uzatılmış görev tanımının bitişinin ardından, CDPC'nin himayesinde, Parlamenterler Asamblesinin görüşü ışığında Açıklayıcı Memorandum taslağını son haline getirmek ve Konvansiyon Taslağını gözden geçirmek üzere üç toplantı daha yaptılar. Bakanlar Kurulu, Ekim 2000'de Asambleden, Nisan 2001'deki genel kurul toplantısının ikinci bölümünde kabul ettiği Konvansiyon taslağı üzerine görüş bildirmesini talep etmişti.

13. PC-CY Komitesinin aldığı bir kararla Konvansiyon taslağının erken bir versiyonu Nisan 2000'de gizli olmaktan çıkarıldı ve yayınlandı. Daha sonra her genel kurulda bir

taslak yayınlanarak görüşmelere katılan Ülkelerin ilgili bütün taraflarla istişareye girmesine imkan tanındı. Bu istişare sürecinin yararlı olduğu görüldü.

14. Gözden geçirilmiş ve son haline getirilmiş Konvansiyon taslağı ve Açıklayıcı Memorandumu Haziran 2001'deki genel kurulunda onaylanmak üzere CDPC'ye sunuldu. Bunun ardından Konvansiyon taslağının metni kabul edilmek ve imzaya açılmak üzere Bakanlar Kuruluna sunuldu.

III. KONVANSİYON

15. Konvansiyonun başlıca amaçları (1) siber suçlar alanında ülkelerin maddi ceza hukuku unsurlarını ve bağlantılı hükümleri uyumlu hale getirmek (2) bu suçların ve bir bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usulleri hukuku yetkilerini sağlamak (3) hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak.
16. Konvansiyon, buna uygun olarak dört bölümden oluşmaktadır: (I) Terimler; (II) Ulusal düzeyde alınacak önlemler - maddi hukuk ve usul hukuku; (III) Uluslararası işbirliği; (IV) Diğer hükümler.
17. Bölüm I'de (maddi hukuk konuları) bilgisayar ya da bilgisayarla ilgili suçlar alanında hem suç sayılmayla ilgili hükümler hem de bağlantılı diğer hükümler yer almaktadır. Önce 4 farklı kategoride gruplanan 9 suç tanımlanmakta, sonra ilave yükümlülükler ve yaptırımlar belirtilmektedir. Konvansiyonda tanımlanan suçlar şunlardır: yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere

müdahale, cihazların kötüye kullanımı, bilgisayarlarla ilişkili sahtecilik fiilleri, bilgisayarlarla ilişkili sahtekarlık fiilleri, çocuk pornografisiyle ilişkili suçlar ve telif hakları ve benzer hakların ihlaline ilişkin suçlar.

18. Bölüm II'de (usul hukuku konuları) - bu bölümün kapsamı bir bilgisayar sistemi aracılığıyla işlenen ya da delilleri elektronik formda bulunan her türlü suç için geçerli olması açısından Bölüm II'de tanımlanan suçlardan daha geniştir - önce bu Bölümdeki usule ilişkin bütün yetkiler için geçerli olan ortak şartlar ve önlemler belirlenmektedir. Daha sonra usule ilişkin şu yetkiler belirtilmektedir: saklanan bilgisayar verilerinin hızlı bir biçimde korunması; trafik verilerinin hızlı bir biçimde korunması ve kısmen açıklanması; üretim talimatı; saklanan bilgisayar verilerinin aranması ve bunlara el konulması; trafik verilerinin gerçek zamanlı olarak toplanması; içerikle ilgili verilere müdahale edilmesi. Bölüm II'nin sonunda yargı yetkisiyle ilgili hükümler yer almaktadır.

19. Bölüm III'te geleneksel ve bilgisayarla işlenen suçlarla ilgili karşılıklı yardımlaşmaya ilişkin hükümler ve iade kuralları yer almaktadır. İki

durumda geleneksel karşılıklı yardımlaşmaya değinilmektedir: taraflar arasında hiçbir hukuki temelin (anlaşma, karşılıklı mevzuat vs.) bulunmadığı durumlar - bu durumda Konvansiyonun hükümleri geçerli olacaktır - ve böyle bir temelin bulunduğu durumlar - bu durumda mevcut düzenlemeler işbu Konvansiyon çerçevesindeki yardımlaşma için de geçerli olacaktır. Bilgisayarla işlenen ya da bilgisayarla ilişkili suçlara özel yardımlaşma her iki durum için de geçerlidir ve ek şartlara da tabi olmak üzere, Bölüm II'de tanımlanan usule ilişkin yetkileri içine almaktadır. Bölüm III'te, ayrıca, saklanan bilgisayar verilerine karşılıklı yardımlaşma gerektirmeyen özel bir tür sınır ötesi erişimle (izinli olarak ya da verilerin herkese açık olduğu durumlarda) ve taraflar arasında hızlı yardımlaşmayı mümkün kılmak için 24 saat ve 7 gün açık durumda olacak bir ağın kurulmasıyla ilgili hükümler bulunmaktadır.

20. Son olarak, Bölüm IV'te -bazı istisnalar dışında- Avrupa Konseyi anlaşmalarındaki standart hükümlerin tekrarlandığı nihai maddeler yer almaktadır.

KONVANSİYONUN MADDELERİYLE İLGİLİ DEĞERLENDİRMELER

BÖLÜM - I *Terimler*

Madde 1 - Tanımlara Giriş

22. Taslağı hazırlayanlar, işbu Konvansiyon çerçevesinde Tarafların Madde 1'de tanımlanan dört kavramı, ülkelerindeki yasalarda bu kavramların işbu Konvansiyonun ilkeleriyle tutarlı bir biçimde kullanılması ve bu yasaların yorum için eşdeğer bir çerçeve sağlaması şartıyla, kelimesi kelimesine bu yasalara aktarılmak zorunda olmayacaklarını kabul etmişlerdir.

Madde 1 (a) - Bilgisayar Sistemi

23. İşbu Konvansiyon çerçevesinde bir bilgisayar sistemi, dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımdan oluşan bir cihazdır. Giriş, çıkış ve saklama özelliklerini de içerebilir. Tek başına çalışabilir ya da benzer cihazlardan oluşan bir ağa bağlı olabilir. "Otomatik" doğrudan insan müdahalesi içermeyen demektir. "Veri işleme" bilgisayar sistemindeki verilerin bir bilgisayar programı

kullanılarak işleme tabi tutulması anlamındadır. "Bilgisayar programı" istenen amaca ulaşmak için bilgisayar tarafından gerçekleştirilebilen bir talimatlar dizisidir. Bir bilgisayar çeşitli programları çalıştırabilir. Bir bilgisayar sistemi işlemci ya da merkezi işlem ünitesi ve çevre birimleri olarak ikiye ayrılacak çeşitli cihazlardan oluşmaktadır. "Çevre birimi" işlem ünitesiyle etkileşim halinde spesifik işlemleri yerine getiren bir cihazdır. Yazıcı, monitör, CD okuyucu/yazıcı ve diğer saklama cihazları bu gruba girer.

24. Ağ, iki ya da daha fazla bilgisayar sisteminin bağlı olmasıdır. Bağlantılar yerden (örneğin tel ya da kablo) ya da kablosuz (örneğin radyo, kızılötesi ya da uydu) olabilir ya da her ikisi birden içerebilir. Bir ağ coğrafi olarak küçük bir bölgede sınırlandırılabilir (yerel bölge ağları) ya da büyük bir bölgeye yayılabilir (geniş bölge ağları), ve bu ağlar da birbirleriyle bağlantılı olabilir. İnternet, hepsi aynı protokolleri kullanan birbiriyle bağlantılı çok sayıda ağdan oluşan küresel bir ağdır. İnternet'e bağlı olan ya da olmayan, bilgisayar sistemleri arasında bilgisayar verisi iletilmesini sağlayan başka tür ağlar da

mevcuttur. Bilgisayar sistemleri son nokta olarak ya da ağdaki iletişime yardım etmek üzere ağa bağlı olabilirler. Önemli olan nokta ağ üzerinden veri alışverişi yapılıyor olmasıdır.

Madde 1 (b) - Bilgisayar Verileri

25. Bilgisayar verisinin tanımı ISO'nun veri tanımına dayanmaktadır. Bu tanımda "işlenmeye uygun nitelikte" ifadesi kullanılmıştır. Bu, verilerin, bilgisayar sistemi tarafından doğrudan işlenebilecek bir biçimde olduğu anlamına gelir. Bu Konvansiyonda bahsedilen verilerin elektronik ya da diğer doğrudan işlenebilir biçimlerde olduğunu açıkça belirtmek için "bilgisayar verisi" kavramı kullanılmıştır. Otomatik olarak işlenen bilgisayar verileri bu Konvansiyonda tanımlanan ceza hukukuna tabi suçlardan birinin hedefi ve bu Konvansiyonda tanımlanan soruşturmaya yönelik önlemlerden birinin uygulanmasının nesnesi olabilir.

Madde 1 (c) - Hizmet Sağlayıcı

26. "Hizmet sağlayıcı" terimi $\hat{=}$ bilgisayar sistemlerinde verilerin iletişimi ya da işlenmesiyle ilgili belli bir role sahip kişilerden oluşan geniş

bir kategoriye içine almaktadır (Kısım 2 üzerine yapılan değerlendirmelerle karşılaştırın). Tanımın (i) şikkında kullanıcılara birbirleriyle iletişim kurma imkanı sağlayan hem kamu hem de özel sektör tüzel kişilerinin dahil edildiği açıkça belirtilmiştir. Bu nedenle, kullanıcıların kapalı bir grup oluşturması ya da sağlayıcının hizmetlerini kamuoyuna sunması, hizmetlerin bedava ya da ücretli olması önemli değildir. Kapalı gruba örnek olarak kurumsal ağ üzerinden hizmet alan belli bir özel sektör kuruluşunun çalışanları gösterilebilir.

27. Tanımın (ii) şikkında, "hizmet sağlayıcı" teriminin (i)'de belirtilen kişiler adına verileri saklayan ya da başka biçimlerde işleyen kişi ya da kuruluşları da içine aldığı açıkça belirtilmiştir. Terim, ayrıca, (i)'de belirtilen kişilerin hizmetlerinin kullanıcıları adına verileri saklayan ya da başka biçimlerde işleyen kişi ya da kuruluşları da içine almaktadır. Örneğin, bu tanım çerçevesinde hizmet sağlayıcı, hem barındırma (*hosting*) ve *caching* hizmetleri sağlayan hizmetleri, hem de bir ağa bağlantı sağlayan hizmetleri kapsamaktadır. Ancak, iletişim veya benzer veri işleme hizmetleri de sağlamakta olmayan bir içerik

sağlayıcı (örneğin web sitesinin barındırılması için bir web barındırma şirketiyle anlaşmış bir kişi) bu tanım kapsamına alınmamıştır.

Madde 1 (d) - Trafik Verileri

28. İşbu Konvansiyonun amaçları açısından, Madde 1'in d şikkında tanımlandığı şekilde trafik verisi, spesifik bir hukuki rejime tabi olan bir bilgisayar verisi kategorisidir. Bu veriler, bir iletişimi başlangıç noktasından varış noktasına göndermek için iletişim zincirindeki bilgisayarlar tarafından üretilir. Bu nedenle iletişim için yardımcı niteliktedir.

29. Bir bilgisayar sistemiyle bağlantılı olarak işlenen ceza hukukuna tabi bir suçun soruşturulmasında, yeni deliller toplanması için bir başlangıç noktası ya da suçun delillerinin bir parçası olarak iletişimin kaynağının saptanması için trafik verilerine ihtiyaç duyulmaktadır. Trafik verileri çok kısa süreli olarak tutuluyor olabilir; bu yüzden hemen koruma altına alınması gerekebilir. Dolayısıyla, silinmeden önce yeni deliller toplamak ya da bir şüpheliyi teşhis etmek üzere bir iletişimin izlediği yolu bulmak için bu verilerin hemen açıklanması gerekli olabilir. Bu

nedenle bilgisayar verilerinin toplanmasında ve açıklanmasında kullanılan normal prosedürler yetersiz kalabilir. Ayrıca, bu verilerin toplanmasının ilke olarak özel hayatı daha az zedeleyici olduğu düşünülmektedir, çünkü böylece iletişimin daha hassas olduğu düşünülen içeriği açığa vurulmamaktadır.

30. Tanımda işbu Konvansiyonda spesifik bir rejim olarak ele alınan trafik verilerinin kategorileri ayrıntılı olarak sayılmıştır: iletişimin başlangıç noktası, varış noktası, izlediği yol, saat, tarih, boyutlar süre ve bu iletişimde kullanılan hizmet tipi. Bu kategorilerin tamamı daima teknik açıdan elde edilebilir, bir hizmet sağlayıcı tarafından üretilebilir ya da belli bir suçun soruşturulmasında gerekli değildir. "Başlangıç noktası", bir hizmet sağlayıcının hizmet verdiği iletişim aracını tanımlayacak bir telefon numarası, İnternet Protokol (IP) adresi ya da benzer bir bilgi olabilir. "Varış noktası" iletişimin aktarıldığı iletişim aracına ait benzer bir bilgidir. "İletişimde kullanılan hizmet tipi" terimi, ağ içerisinde kullanılan hizmetin tipi -örneğin dosya transferi, elektronik posta ya da anında mesaj-anlamına gelmektedir.

31. Tanım, trafik verilerinin yasal korunmasında verinin hassaslığına bağlı olarak farklılıklar getirme yetkisini ulusal yasama organlarına tanımaktadır. Bu bağlamda, Madde 15 Tarafların insan hak ve özgürlüklerinin korunması için gerekli şart ve önlemleri sağlamasını şart koşturmaktadır. Bu, başka şeylerin yanı sıra, soruşturma yetkisi için geçerli olacak maddi ölçütlerin ve usullerin verilerin hassasiyetine bağlı olarak değişebileceği anlamına gelir.

BÖLÜM - II

Ulusal Düzeyde Alınacak Önlemler

32. Bölüm II'de (Madde 2 - 22) üç kısım yer almaktadır: maddi ceza hukuku (Madde 2 - 13), usul hukuku (Madde 14 - 21) ve yargı yetkisi (Madde 22).

KISIM - I

Maddi Ceza Hukuku

33. Konvansiyonun 1. Kısımının (Madde 2 - 13) amacı, bilgisayarla işlenen ya da bilgisayarla ilişkili suçlar için ortak bir minimum standart oluşturarak bu suçları önleyecek ve zapt edecek önlemleri geliştirmektir. Bu tür bir uyumlulaştırma bu suçlarla hem ulusal hem de uluslararası düzeyde yapılan mücadeleyi güçlendirir. Ulusal mevzuatların uyumlu olması, kötü kullanımların daha önce düşük bir standartta olan Taraflara geçmesini önleyebilir. Sonuçta belirli vakaların ele alınmasında edinilen yararlı ortak deneyimlerin paylaşımı da geliştirilebilir. Çifte suçluluk şartları gibi konulardaki uluslararası işbirliği (özellikle iade ve hukuki yardımlaşma) kolaylaşır.
34. Dahil edilen suçlar listesi minimum bir uzlaşmayı temsil etmekte ve ulusal mevzuatlardaki eklemeleri içermemektedir. Listede büyük ölçüde Avrupa Konseyi'nin bilgisayarla ilişki suçlara ilişkin R (89) 9 sayılı Tavsiyesiyle bağlantılı olarak geliştirilmiş olan talimatlara ve diğer kamusal ve özel uluslararası kuruluşların (OECD, BM, AIDP) çalışmalarını esas alınmış,

ama genişleyen telekomünikasyon ağlarının kötü kullanımlarıyla ilgili daha modern deneyimleri de göz önünde bulundurulmuştur.

35. Kısım beş Başlığa ayrılmıştır. Başlık 1'de bilgisayarla ilişkili temel suçlar, bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne kullanıma açıklığına yönelik suçlar ele alınmıştır. Bu suçlar, bilgisayar ve veri güvenliğiyle ilgili tartışmalarda belirlenen, elektronik veri işleme ve iletme sistemlerinin karşı karşıya bulunduğu temel tehditleri temsil etmektedir. Başlıkta ele alınan suç türlerinin sistemlere, programlara ve verilere izinsiz erişim ve bunları tahrif olduğu belirtilmiştir. Başlık 2 - 4'te, uygulamada daha çok rastlanan ve genellikle ceza hukukunun geleneksel yollarla yapılan saldırılara karşı zaten korumakta olduğu belirli yasal haklara karşı yapılan saldırılarda bilgisayar ve telekomünikasyon sistemlerinin kullanılmasının söz konusu olduğu diğer "bilgisayarla ilişkili suç" türleri ele alınmıştır. Başlık 2'de ele alınan suçlar (bilgisayarla ilişkili sahtecilik ve sahtekarlık), Avrupa Konseyi'nin R (89) 9 sayılı Tavsiyesinde yer alan, aşağıda belirtilen öneriler doğrultusunda eklenmiştir. Başlık 3, günümüzün en tehlikeli modi operandi'lerinden biri olan

*Ankara Barosu
Bilgi İşlem Merkezi Yayınları*

"bilgisayar sistemleri yoluyla yasadışı çocuk pornografisi üretimi ve dağıtımıyla ilgili bilgisayar ilişkili suçlar"ı ele almaktadır. Konvansiyon taslağını hazırlayan komitede, ırkçı propagandanın bilgisayar sistemleri yoluyla dağıtımı gibi başka içerikle ilişkili suçların da dahil edilmesi üzerine tartışılmıştır. Ancak komite bu fiillerin suç sayılması üzerine tam bir uzlaşmaya varamamıştır. Bunun da ceza hukukuna tabi bir suç olarak dahil edilmesi yönünde güçlü bir destek olmakla birlikte, bazı temsilciler böyle bir hükmün dahil edilmesi konusunda ifade özgürlüğü açısından kaygılı olduklarını belirtmişlerdir. Konunun karmaşıklığı göz önüne alınarak, komitenin işbu Konvansiyona ek bir Protokol hazırlaması için Avrupa Suç Sorunları Komitesi'ne (CDPC) başvurmasına karar verilmiştir. Başlık 4'te "telif haklarının ve benzer hakların ihlaline ilişkin suçlar" belirtilmiştir. Telif hakkı ihlallerinin bilgisayarla işlenen ya da bilgisayarla ilişkili suçların en yaygın biçimlerinden biri olması ve bu ihlallerdeki artışın uluslararası düzeyde kaygıya yol açması nedeniyle bu konu da Konvansiyona dahil edilmiştir. Son olarak, Başlık 5'te teşebbüste bulunmak ve yardım ya da

yataklık etmek, yaptırımlar ve önlemler, ve son dönemdeki uluslararası araçlara uygun olarak kurumsal yükümlülük ele alınmıştır.

36. Maddi hukuk hükümleri bilgi teknolojileri kullanılarak işlenen suçlara ilişkin olmakla birlikte, maddi ceza hukuku suçlarının hem bugünkü hem de gelecekteki teknolojiler için geçerli olması amacıyla Konvansiyonda teknolojiye bağımsız bir dil kullanılmıştır.
37. Konvansiyon taslağını hazırlayanlar Tarafların küçük ya da önemsiz suçları Madde 2-10'da tanımlanan suçların uygulamasından çıkarabileceğini kabul etmişlerdir.
38. Dahil edilen suçların bir özelliği söz konusu fiilin "haksız biçimde" yapılmış olmasının açık bir şart olarak belirtilmiş olmasıdır. Bu, tanımlanan fiilin her zaman başlı başına cezalandırılabilir olmadığı; rıza, kendini müdafaa ya da zorunluluk gibi klasik hukuki savunmaların geçerli olduğu durumlarda yasal ya da haklı olabileceği gibi, başka ilke ve hakların da cezai yükümlülüğün ortadan kalkmasına yol açabileceği şeklinde bir düşüncüyü yansıtmaktadır. "Haksız biçimde" ifadesinin

anlamı kullanıldığı bağlamdan çıkmaktadır. Dolayısıyla, Tarafların kavramı kendi ulusal mevzuatlarında nasıl uygulayacaklarına sınırlama getirilmeksizin, izinsiz (yasama, yürütme, idare, yargı, sözleşme ya da rıza açısından) olarak gerçekleştirilen ya da ulusal mevzuat çerçevesinde belirlenmiş hukuki savunma, mazeret, gerekçe ya da benzer ilkeler kapsamına girmeyen fiiller anlamında kullanılabilir. Dolayısıyla Konvansiyon meşru hükümet yetkisiyle gerçekleştirilen fiilleri kapsamına almamaktadır (örneğin Tarafın hükümeti kamu düzenini sürdürmek, ulusal güvenliği korumak, ya da ceza hukukuna tabi suçları soruşturmak amacıyla bir eylemde bulunduğu). Ayrıca, ağların tasarımının ayrılmaz bir parçası olan meşru ve yaygın faaliyetler ya da meşru ve yaygın işletmeyle ilgili ve ticari uygulamalar suç olarak tanımlanamaz. Bu tür suç olarak tanımlanamayacak durumlarla ilgili spesifik örnekler aşağıda, Açıklayıcı Memorandumun ilgili bölümünde spesifik suçlarla ilişkili olarak verilmiştir. Bu tür muafiyetlerin ulusal hukuk sistemlerinde nasıl uygulanacağını (ceza hukuku çerçevesinde ya da başka şekilde) belirlemek Taraflara bırakılmıştır.

39. Cezai yükümlülüğün geçerli olabilmesi için Konvansiyonda ele alınan bütün suçların "kasıtlı" olarak işlenmesi gereklidir. Bazı durumlarda ilave spesifik bir kasıt unsuru suçun bir bölümünü oluşturur. Örneğin, bilgisayarla ilişkili sahtekarlığa ilişkin Madde 8'de ekonomik bir kazanç elde etmeye yönelik kasıt suçun teşkil edici unsurlarından birdir. Konvansiyon taslağını hazırlayanlar "kasıtlı olarak" ifadesinin kesin anlamının ulusal yoruma bırakılmasına karar vermişlerdir.
40. Kısımdaki bazı Maddeler, Konvansiyonun ulusal mevzuatta uygulanmasında bazı kısıtlayıcı şartların ilave edilmesine izin vermektedir. Bazı durumlarda hakların saklı tutulması olanağı bile tanınmıştır (bkz Madde 40 ve 42). Suç olarak tanımlamaya yönelik bu tür çeşitli daha kısıtlayıcı yaklaşımlar, söz konusu davranışın tehlike düzeyiyle ve ceza hukukunu bir karşı tedbir olarak kullanma ihtiyacıyla ilgili farklı değerlendirmeleri yansıtmaktadır. Bu yaklaşım hükümetlere ve meclislere bu alandaki cezai politikalarını belirleme esnekliği tanımaktadır.
41. Bu suçları belirleyen yasalar, cezai yaptırımlara yol açacak fiil türlerinin yeterince tahmin

edilebilir olmasını sağlamak amacıyla mümkün olduğunca açık ve spesifik bir dille kaleme alınmalıdır.

42. Taslağı hazırlayanlar, kaleme alma sürecinde, Madde 2-11'de tanımlananlar dışındaki bazı fiillerin suç olarak tanımlanmasının yerindeliğini değerlendirmişlerdir. Siber işgalcilik adı verilen, mevcut olan ve genellikle çok tanınan bir kişi ya da kuruluşun adını ya da bir ürün ya da firmanın ticari ismini ya da ticari markasını alan adı olarak kaydettirme fiili de buna dahildir. Siber işgalciler söz konusu alan adlarını aktif olarak kullanmayı düşünmemekte ve ilgili kişi ya da kuruluşu dolaylı olarak da olsa bu alan adının mülkiyetinin transferi için para ödemeye zorlayarak mali avantaj elde etmeye çalışmaktadırlar. Şu an için bu fiil ticari markalarla ilgili bir sorun olarak ele alınmaktadır. Ticari marka ihlalleri bu Konvansiyonda ele alınmadığı için, taslağı hazırlayanlar bu tür fiilleri suç olarak tanımlama konusunu değerlendirmenin uygun olmadığı sonucuna ulaşmışlardır.

BAŞLIK - I

*Bilgisayar Veri ve Sistemlerinin Gizliliğine,
Bütünlüğüne ve Kullanıma Açıklığına
Yönelik Suçlar*

43. Madde 2-6'da tanımlanan ceza hukukuna tabi suçlarla bilgisayar sistem ve verilerinin gizliliğini, bütünlüğünü ve kullanıma açıklığını korumak amaçlanmış, ağların tasarımının ayrılmaz bir parçası olan meşru ve yaygın faaliyetlerin ya da meşru ve yaygın işletmeyle ilgili ya da ticari uygulamaların suç olarak tanımlanması amaçlanmamıştır.

Madde 2 - Yasadışı Erişim

44. "Yasadışı erişim" terimi bilgisayar sistem ve verilerinin güvenliğine (yani gizlilik, bütünlük, kullanıma açıklık) yönelik tehlikeli tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Koruma ihtiyacı, kuruluş ve kişilerin sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme ihtiyaçlarını yansıtmaktadır. Sadece izinsiz girme, yani korsanlık ("hacking"), "zarar verme amacıyla girme" ("cracking") ya da "bilgisayara izinsiz girme" ("computer trespass") ilke olarak başlı başına yasadışı olmalıdır. Bu durum, sistemlerin

ve verilerin meşru kullanıcılarının engellenmesine ve düzeltilmesi yüksek maliyet getiren değişiklik ve tahribata yol açabilir. Bu tür izinsiz girmeler gizli verilere (şifreler, hedeflenen sistemle ilgili bilgiler dahil olmak üzere) ve sırlara erişilmesine, sistemin ücretsiz kullanılmasına yol açabilir, hatta korsanları bilgisayarla ilişkili sahtecilik ve sahtekarlık gibi daha tehlikeli bilgisayarla ilişkili suç türlerine teşvik edebilir.

45. İzinsiz erişimi önlemenin en etkin yolu şüphesiz ki etkin güvenlik önlemlerinin geliştirilmesi ve uygulanmaya başlanmasıdır. Ancak kapsamlı bir önlem paketi ceza hukukuna ilişkin önlemleri kullanma tehdidini ve bu önlemlerin kullanımını da içermelidir. İzinsiz erişimin cezai yollarla engellenmesi sistem ve veriler için ek bir koruma getirebilir ve yukarıda sayılan tehlikelerin erken bir aşamada önlenmesini sağlayabilir.

46. "Erişim", bilgisayar sisteminin tamamına ya da bir parçasına (donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler) girilmesi anlamındadır. Ancak, sisteme sadece bir e-posta mesajı ya da dosya gönderilmesini kapsamaz. "Erişim", kamusal telekomünikasyon ağları yoluyla ya da

bir kuruluşun yerel ağı (LAN) ya da İntranet'i gibi bir ağ üzerindeki başka bir bilgisayar sistemine girmeyi içine alır. İletişim yöntemi (örneğin kablosuz bağlantılar da dahil olmak üzere uzaktan ya da yakın mesafeden) önemli değildir.

47. Fiilin "haksız biçimde" işlenmiş olması da gerekmektedir. Bu ifade, yukarıda verilen açıklamalara ek olarak, sistemin ya da bir parçasının sahibi ya da başka hak sahiplerinin izniyle yapılan erişimin (örneğin ilgili bilgisayar sisteminin izinli olarak test edilmesi ya da korunması amacıyla) suç olarak tanımlanamayacağı anlamına gelmektedir. Ayrıca, kamunun ücretsiz ve açık erişimine izin veren bilgisayar sistemlerine erişim suç olarak tanımlanamaz. Bu tür erişimler "haklı biçimde" yapılmaktadır.

48. Spesifik teknik araçların uygulanması, iletişim amacıyla bilginin yerinin saptanması ve elde edilmesi için doğrudan ya da görünmeyen bağlantılar ("*deep-link*") ya da "çerez" ya da "robot yazılımlar"ın ("*bot*") uygulanması da dahil olmak üzere- "hiper-metin" bağlantıları yoluyla bir web sayfasına erişim gibi Madde 2'de belirtilen türde bir erişime yol açabilir. Bu

araçların uygulanması tek başına "haksız biçimde" erişim kapsamına girmez. Kamuya açık bir web sitesinin işletilmesi, web sitesinin sahibinin siteye herhangi başka bir web kullanıcısının erişmesine izin verdiği anlamına gelir. Yaygın olarak uygulanan iletişim protokol ve programlarında sunulan standart araçların uygulanması, özellikle de "cookie" örneğinde olduğu gibi, erişilen sistemin hak sahibinin ilk yüklemeyi reddetmeyerek ya da daha sonra uygulamayı kaldırmayarak bunların uygulanmasını kabul ettiğinin düşünülebileceği durumlarda, tek başına "haksız biçimde" işlenmiş bir fiil değildir.

49. Birçok ulusal mevzuatta halihazırda korsanlık suçlarıyla ilgili hükümler bulunmaktadır, ama kapsam ve teşkil edici unsurlar önemli ölçüde değişiklik göstermektedir. Madde 2'nin ilk cümlesindeki geniş suç olarak tanımlama yaklaşımı tartışma konusudur. Yalnızca izinsiz girme fiilinin hiçbir tehlike yaratmadığı ve hatta hacking olaylarının sistemlerin güvenliğindeki boşluk ve zayıflıkların saptanmasını sağladığı durumlar muhalif görüşlerin doğmasına yol açmaktadır. Bu durum, bazı ülkelerde ek kısıtlayıcı şartlar getiren daha dar bir yaklaşımın

benimsenmesine neden olmuştur. (89) 9 sayılı Tavsiyede ve OECD Çalışma Grubunun 1985 tarihli önerisinde de bu yaklaşım benimsenmiştir.

50. Taraflar geniş yaklaşımı benimseyerek Madde 2'nin ilk cümlesine uygun biçimde sadece korsanlık fiilini de suç olarak tanımlayabilirler. Diğer bir seçenek Tarafların ikinci cümledeki kısıtlayıcı unsurların bazılarını ya da hepsini kabul etmeleridir: Güvenlik önlemlerinin ihlal edilmesi, bilgisayar verilerinin elde edilmesi amacı, ceza hukukuna tabi suç oluşturacak dürüst olmayan başka amaçlar, suçun uzaktaki başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişki olarak işlenmiş olması şartı. Son seçenek Tarafların bir kişinin başka bir bilgisayar sistemini kullanmaksızın bağımsız bir bilgisayara fiziksel erişimini kapsam dışı bırakmalarına izin verir. Taraflar suçu ağ oluşturan bilgisayar sistemleriyle (telekomünikasyon hizmetlerinin sağladığı kamusal ağlar ve Intranet ya da Ekstranet gibi özel ağlar dahil olmak üzere) sınırlı tutabilirler.

Madde 3 - Yasadışı Müdahale

51. Bu hükümle veri iletişiminin gizliliği hakkının korunması amaçlanmaktadır. Suç, kişiler

arasındaki sözlü telefon görüşmelerinin geleneksel yöntemlerle dinlenmesi ve kaydedilmesindeki iletişimin gizliliğinin ihlalini temsil etmektedir. İletişimin gizliliği hakkı Avrupa İnsan Hakları Konvansiyonunun 8. Maddesinde kutsal bir hak olarak gösterilmiştir. Madde 3'te tanımlanan suç bu ilkenin telefon, faks, e-posta ya da dosya transferi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmasıdır.

52. Hükmün metni büyük ölçüde (89) 9 sayılı Tavsiyede belirtilen "izinsiz müdahale" suçundan alınmıştır. İşbu Konvansiyonda söz konusu iletişimlerin aşağıda belirtilen şartlarda "bilgisayar verilerinin iletimi" ve elektromanyetik radyasyonla ilgili olduğu açıkça belirtilmiştir.

53. "Teknik yöntemler" kullanarak müdahale, iletişimin içeriğinin dinlenmesi, denetlenmesi ya da izlenmesi, ve verilerin içeriğinin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizlice dinleme cihazlarının yardımıyla dolaylı olarak elde edilmesi ile ilgilidir. Müdahaleye kaydetmek de dahildir. Teknik yöntemler, iletim hatlarına takılan teknik cihazlarla birlikte kablosuz iletişimi elde etmekte ve kaydetmekte kullanılan cihazları

da kapsar. Bu yöntemler yazılım, şifre ve kodların kullanımını da kapsayabilir. Teknik yöntemler kullanma şartı, gereğinden fazla fiili suç olarak tanımlamaktan kaçınmak için getirilmiş kısıtlayıcı bir şarttır.

54. Suç "kamuya açık olmayan" bilgisayar verilerinin iletimi için geçerlidir. "Kamuya açık olmayan" terimi iletilen verilerin yapısını değil, iletimin (iletişimin) yapısını nitelemektedir. İletilen veriler herkesin ulaşabileceği bilgiler olabilir, ama taraflar bunu gizlice iletmeyi isteyebilirler. Ya da ücretli televizyonlarda olduğu gibi, veriler hizmetin ücreti ödeninceye kadar ticari amaçlarla gizli tutulmak istenebilir. Bu nedenle, "kamuya açık olmayan" terimi tek başına kamusal ağlar üzerinden gerçekleştirilen iletişimleri dışarıda bırakmamaktadır. "Bilgisayar verilerinin kamuya açık olmayan iletimi" kapsamına giren personel arasındaki iletişim, ticari amaçla olup olmamasından bağımsız olarak, Madde 3 çerçevesindeki haksız biçimde müdahaleye karşı koruma altındadır (bkz. örneğin Halford-Birleşik Krallık davasındaki 25 Haziran 1997 tarihli ve 20605/92 sayılı Avrupa İnsan Hakları Mahkemesi kararı).

55. Bilgisayar verilerinin iletimi biçimindeki iletişim tek bir bilgisayar sisteminin içinde (örneğin merkezi işlem ünitesinden ekran ya da yazıcıya akış), aynı kişiye ait iki bilgisayar sistemi arasında, birbiriyle iletişim halindeki iki bilgisayar ya da bir bilgisayar ile bir kişi (örneğin klavye yoluyla) arasında olabilir. Ancak Taraflar, birbirlerine uzaktan bağlı bilgisayar sistemleri arasındaki iletişimin iletimi için ek bir unsura gerek duyabilirler.
56. "Bilgisayar sistemi" kavramının radyo bağlantılarını da içine almasının, "kamuya açık olmayan" bir iletim de olsa, görece açık ve kolaylıkla erişilebilir bir şekilde yapılan ve bu nedenle, örneğin amatör radyocular tarafından, müdahale edilebilen bir radyo iletimini suç olarak tanımlamak konusunda Taraflara bir zorunluluk getirmediğine dikkat edilmelidir.
57. "Elektromanyetik dalgalar yayınlanması"yla bağlantılı olarak suçun oluşması kapsamı genişletmektedir. Elektronik dalgalar normal işleyişi sırasında bir bilgisayar tarafından yayınlanabilir. Madde I'de verilen tanım göre bu tür yayınlar "veri" olarak kabul edilmemektedir. Ancak, veriler bu yayınlar kullanılarak yeniden oluşturulabilir. Bu nedenle, bir bilgisayar

sisteminin elektromanyetik dalgalarındaki verilere müdahale bu hüküm çerçevesinde suç olarak tanımlanmıştır.

58. Cezai yükümlülük getirmesi için yasadışı müdahalenin "kasıtlı olarak" ve "haksız biçimde" gerçekleştirilmiş olması gerekmektedir. Örneğin müdahale eden kişi bunu yapma hakkına sahipse, iletimin taraflarının talimatları doğrultusunda ya da izinleriyle bunu yapıyorsa (tarafların izin verdiği test etme ve koruma faaliyetleri dahil olmak üzere), ya da izleme ulusal güvenlik ya da soruşturma mercilerinin suçları araştırma çalışmaları çerçevesinde yasal yetkiyle gerçekleştiriliyorsa, fiil haklıdır. "Cookie"lerin kullanımı gibi yaygın ticari uygulamaların da suç olarak tanımlanmamasına, "haksız biçimde" gerçekleştirilmiş bir müdahale olarak değerlendirilmemesine karar verilmiştir. Madde 3 çerçevesinde korunan, personel arasındaki kamuya açık olmayan iletişime (bkz. yukarıda paragraf 54) yapılan meşru müdahaleler için ulusal mevzuatta bir zemin bulunabilir. Madde 3 çerçevesinde bu durumlardaki müdahale "haklı biçimde" gerçekleştirilmiş olarak kabul edilmektedir.

59. Bazı ülkelerde müdahale, bir bilgisayar sistemine izinsiz erişim suçuyla yakından ilişkili olarak görülebilir. Yasanın yasaklayıcılığının ve uygulamasının tutarlı olmasını sağlamak için, dürüst olmayan amaçları ya da Madde 2'ye uygun biçimde fiilin başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmesini şart koşan ülkeler, bu Maddedeki cezai yükümlülüğe de benzer sınırlayıcı unsurlar getirebilir. Bu unsurlar, "kasıtlılık" ve "haksız biçimde" işlenme gibi suçun başka unsurlarıyla bağlantılı olarak yorumlanmalı ve uygulanmalıdır.

Madde 4 - Verilere Müdahale

60. Bu hükmün amacı, bilgisayar verilerini ve bilgisayar programlarını da, fiziksel nesneler gibi, kasıtlı hasar verme girişimlerine karşı koruma altına almaktır. Burada koruma altına alınan yasal hak, saklanan bilgisayar veri ya da bilgisayar programlarının bütünlüğü ve uygun biçimde çalışmaları ve kullanımıdır.
61. Paragraf 1'de, örtüşen fiiller olarak "tahrip etmek" ve "bozmak", özellikle veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz biçimde değiştirilmesiyle ilişkilidir.

Verilerin "silinmesi", fiziksel bir cismin imhasına eşdeğerdir. Veriler imha edilir ve tanınmaz hale getirilir. Bilgisayar verilerinin erişilmez kılınması, verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişi için verilerin ulaşılabilirliğini önleyen ya da sona erdiren herhangi bir fiil anlamındadır. "Değiştirme" terimi mevcut verilerin farklı bir hale getirilmesi anlamındadır. Virüs ve Truva atı gibi kötü amaçlı kodların sisteme sokulması da, bu nedenle, verilerin sonuçta farklı bir hale gelmesi gibi, bu paragrafın kapsamındadır.

62. Yukarıdaki fiiller ancak "haksız biçimde" gerçekleştirildiği takdirde cezalandırılabilir. Ağların tasarımının ayrılmaz bir parçası olan yaygın faaliyetler veya işletmeyle ilgili ya da ticari yaygın uygulamalar -örneğin bir bilgisayar sisteminin güvenliğinin sahibi ya da işletmecisinin izniyle test edilmesi ya da korunması, ya da sistemin işletmecisi yeni bir yazılım edindiğinde (örneğin İnternet'e erişim sağlayan, daha önce yüklenmiş benzer programları çalışmaz hale getiren bir yazılım) bilgisayarın işletim sisteminin konfigürasyonunun değişmesi- haksız biçimde gerçekleştirilmektedir ve dolayısıyla bu Madde çerçevesinde suç olarak tanımlanmamaktadır. Anonim iletişimleri

kolaylaştırmak amacıyla trafik verilerinin farklı bir hale getirilmesi (örneğin anonim yeniden postalama sistemleri), ya da güvenli iletişim amacıyla verilerin farklı bir hale getirilmesi (örneğin şifreleme), ilke olarak gizliliğin meşru bir koruması olarak görülmeli ve haklı biçimde yapılmış oldukları kabul edilmelidir. Ancak, Taraflar, anonim iletişimle ilgili belli suiistimalleri, örneğin suçlunun kimliğini gizlemek için paket başlık bilgilerinin değiştirildiği durumları suç olarak tanımlamak isteyebilirler.

63. Ayrıca, failin "kasıtlı olarak" hareket etmiş olması gerekmektedir.
64. Paragraf 2, Tarafların ciddi zararlar sonuçlanan fiillerle ilgili olarak haklarını saklı tutmalarına izin vermektedir. Bu ciddi zararları neyin teşkil ettiğinin yorumu ulusal mevzuata bırakılmıştır, ama Taraflar bu haklarını saklı tutma imkanından yararlanırlarsa yorumlarını Avrupa Konseyi Genel Sekreteri'ne bildirmelidirler.

Madde 5 - Sistemlere Müdahale

65. (89) 9 sayılı Tavsiyede bundan bilgisayar sabotajı olarak söz edilmektedir. Hükmün amacı telekomünikasyon olanakları da dahil olmak

üzere bilgisayar sistemlerinin yasalara uygun şekilde kullanımının bilgisayar verileri kullanılarak ya da bu veriler etkilenecek uluslararası düzeyde engellenmesi fiilinin suç olarak tanımlanmasıdır. Korunan yasal hak, bilgisayar ya da telekomünikasyon sistemlerinin işletmeci ve kullanıcılarının bu sistemleri uygun biçimde işletme haklarıdır. Metin her tür işleyiş biçiminin koruma altına alınmasını sağlamak için tarafsız bir dille kaleme alınmıştır.

66. "Engelleme" terimi, bilgisayar sisteminin uygun işleyişine müdahale eden fiiller için kullanılmıştır. Bu engelleme, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak yoluyla yapılmış olmalıdır.
67. Cezai yaptırıma yol açması için engellemenin ayrıca "ciddi ölçüde" olması gerekir. Taraflardan her biri engellemenin "ciddi ölçüde" sayılması için hangi ölçütlerin gerçekleşmesi gerektiğine kendisi karar verecektir. Örneğin, Taraflardan biri engellemenin ciddi ölçüde sayılması için minimum düzeyde tahribatın oluşmasını yeterli görebilir. Taslağı kaleme alanlar, verilerin belli bir sisteme, sahibinin ya da işletmecisinin sistemi

kullanma ya da diğer sistemlerle iletişim kurma yeteneği üzerinde önemli ölçüde zararlı bir etkisi olan bir biçim, hacim ya da sıklıkta gönderilmesini "ciddi ölçüde" olarak değerlendirmektedirler (örneğin "hizmetin reddi" saldırıları geliştiren programlar, sistemin işleyişini önleyen ya da önemli ölçüde yavaşlatan virüs gibi kötü amaçlı kodlar, ya da bir alıcıya sistemin iletişim işlevlerini engellemek üzere çok büyük miktarlarda elektronik posta gönderen programlar yoluyla).

68. Engelleme "haksız biçimde" yapılmış olmalıdır. Ağların tasarımının ayrılmaz bir parçası olan yaygın faaliyetler ya da işletmeyle ilgili ya da ticari yaygın uygulamalar haklı biçimde yapılmaktadır. Bunlar arasında, örneğin, bir bilgisayar sisteminin güvenliğinin sahibi ya da işletmecisinin izniyle test edilmesi ya da korunması, ya da sistemin işletmecisi daha önce yüklenmiş benzer programları çalışmaz hale getiren yeni bir yazılım edindiğinde bilgisayarın işletim sisteminin konfigürasyonunun değişmesi bulunmaktadır. Dolayısıyla, bu fiiller, ciddi ölçüde engellemeye yol açsalar da bu Madde çerçevesinde suç olarak tanımlanmamaktadır.

69. Ticari ya da başka amaçlarla istenmeyen e-postaların gönderilmesi, özellikle büyük miktarlarda ve çok sık bir biçimde gerçekleştirildiğinde istenmeyen e-postalar ("spamming") alıcıyı rahatsız edebilir. Taslağı kaleme alanlara göre, bu fiil ancak iletişimi kasıtlı olarak ve ciddi ölçüde engellediğinde suç olarak tanımlanmalıdır. Ancak, Tarafların mevzuatlarında engelleme için farklı yaklaşımlar bulunabilir. Örneğin belli müdahale fiilleri idari suçlar olarak tanımlanabilir ya da başka şekillerde yaptırıma tabi kılınabilir. Metin, mevzuatlarında idari ya da cezai yaptırımı gerektirecek zarar eşiğine ulaşmak için sistemin işleyişinin ne dereceye kadar -kısmen ya da tamamen, geçici ya da kalıcı olarak- engellenmesi gerekeceğini belirlemeyi Taraflara bırakmaktadır.

70. Suç kasıtlı olarak işlenmiş olmalı, yani fail ciddi ölçüde engelleme kastıyla hareket etmiş olmalıdır.

Madde 6 - Cihazların Kötüye Kullanımı

71. Bu hükümle belli cihazlarla ilgili spesifik yasadışı fiillerin kasıtlı olarak işlenmesi ya da bilgisayar sistemleri ve verilerinin gizliliği, bütünlüğü ve

kullanıma açıklığına karşı yukarıda tanımlanan suçları işlemek üzere verilere erişilmesi ayrı ve bağımsız bir cezai suç olarak tanımlanmaktadır. Bu suçları işlemek genellikle erişim araçlarının "korsanlık araçları" ya da başka araçların bulundurulmasını gerektirdiği için, bu araçları suç işlemek üzere elde etmeye yönelik, üretim ve dağıtımları alanında bir tür karaborsanın doğmasına yol açabilecek, güçlü bir eğilim vardır. Bu tehlikelerle daha etkin bir biçimde mücadele edebilmek için, ceza hukuku tehlike potansiyeli taşıyan spesifik fiilleri, Madde 2 - 5'te tanımlanan suçların işlenmesinden önce, kaynağında yasaklamalıdır. Bu açıdan hüküm, Avrupa Konseyi'ndeki (şartlı erişime dayalı olan ya da şartlı erişim içeren hizmetlere yasal koruma üzerine Avrupa Konvansiyonu - 178 sayılı ETS) ve Avrupa Birliği'ndeki (Avrupa Parlamentosu'nun ve 20 Kasım 1998 tarihli Konseyin şartlı erişime dayalı olan ya da şartlı erişim içeren hizmetlere yasal koruma üzerine 98/84/EC sayılı Direktifi) bazı yeni gelişmelere ve bazı ülkelerdeki ilgili hükümlere dayanmaktadır. Kalpazanlık üzerine 1929 Cenevre Konvansiyonunda benzer bir yaklaşım benimsenmiştir.

72. Paragraf 1(a)'de bilgisayar programları da dahil olmak üzere işbu Konvansiyonun 2 ila 5. Maddelerinde tanımlanan suçlardan herhangi birini işlemek amacıyla tasarlanmış ya da bu amaca uygun hale getirilmiş bir cihazın üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilebilir hale getirilmesi suç olarak tanımlanmıştır. "Dağıtım" verileri aktif olarak başkalarına iletmek, "elde edilebilir hale getirmek" online cihazları başkalarının kullanımına sunmak anlamında kullanılmıştır. Bu terimin, bu tür cihazlara erişimi kolaylaştırmak için hiper-metinler yaratmayı ya da derlemeyi de içine alması amaçlanmıştır. "Bilgisayar programı"yla, örneğin virüs programları gibi verileri değiştirmeye hatta imha etmeye ya da sistemlerin işletimine müdahale etmeye yönelik ya da bilgisayar sistemlerine erişim sağlamak için tasarlanmış ya da bu amaca uygun hale getirilmiş programlar kastedilmiştir.

73. Konvansiyon taslağını kaleme alanlar, cihazların münhasıran ya da spesifik olarak suç işlemek üzere tasarlanmış cihazlarla sınırlı tutulması ve dolayısıyla çift kullanımlı cihazların kapsam dışı bırakılması konusunu ayrıntılı olarak tartışmışlardır. Bunun aşırı dar bir kapsam

olacağı düşünülmüştür. Bu yaklaşım hükmü pratikte uygulanamaz ya da sadece nadir durumlarda uygulanabilir hale getirerek ceza davalarında üstesinden gelinemeyecek delil bulma güçlüklerine yol açabilir. Alternatif olarak, yasal olarak üretilmiş ve dağıtılmış bile olsa bütün cihazları kapsam dahiline almak görüşü de reddedilmiştir. Bu durumda, ceza vermek konusunda yalnızca bilgisayar suçu işlemeyi amaçlamak gibi öznel bir unsur belirleyici olacaktı. Bu yaklaşım kalpazanlık alanında da benimsenmemiştir. Konvansiyon, makul bir uzlaşma noktası olarak, kapsamını cihazların öncelikli olarak suç işlemek için tasarımı olduğu ya da bu amaca uygun hale getirildiği durumlarla sınırlı tutmuştur. Tek başına bu hüküm genellikle çift kullanımlı cihazları kapsam dışı bırakmaktadır.

74. Paragraf 1(a)2'de bir bilgisayar sisteminin tamamına veya bir kısmına erişim sağlayan bilgisayar şifreleri, erişim kodları veya benzeri verilerin, üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı ya da başka surette elde edilebilir hale getirilmesi suç olarak tanımlanmıştır.

75. Paragraf 1(b), paragraf 1(a)1 ve 1(a)2'de belirtilen unsurların bulundurulması suçunu belirlemektedir. Paragraf 1(b)'nin son cümlesiyle, Tarafların yasalarında söz konusu unsurlardan belli bir sayıda bulundurması şartı getirmelerine izin verilmiştir. Bulundurulan unsurların sayısı doğrudan suç işleme amacını ispatlayacaktır. Cezai yükümlülük doğması için gerekli unsurların sayısına karar vermek taraflara bırakılmıştır.
76. Suçun kasıtlı olarak ve haksız biçimde işlenmiş olması gerekmektedir. Cihazların, bilgisayar sistemlerine karşı saldırılar düzenlemek gibi, meşru amaçlarla üretildiği ve piyasaya sunulduğu durumları da suç olarak tanımlama tehlikesinden kaçınmak için suçu sınırlandıracak başka unsurlar da eklenmiştir. Genel amaç şartı dışında, cihazın işbu Konvansiyonun 2-5. Maddelerinde belirtilen suçları işlemek amacıyla kullanıldığını gösteren spesifik (yani doğrudan) bir amaç da bulunmalıdır.
77. Bir bilgisayar sisteminin izinli olarak test edilmesi veya korunması amacıyla yaratılan araçların hükmün kapsamı dışında olduğu Paragraf 2'de açıkça belirtilmiştir. Bu kavram "haksız şekilde" ifadesinde belirtilmiştir.

Örneğin, sektör tarafından bilgi teknolojisi ürünlerinin güvenilirliğini kontrol etmek ya da sistem güvenliğini test etmek için tasarlanmış olan test cihazları, "zarar verme amaçlı giriş cihazları" ve ağ analiz cihazları meşru amaçlarla üretilmiştir ve "haklı biçimde" kullanıldıkları kabul edilmektedir.

78. "Cihazların kötüye kullanımı" suçunun Madde 2-5'te belirtilen farklı türlerdeki bütün bilgisayar suçlarına uygulanması ihtiyacıyla ilgili farklı değerlendirmelerden dolayı, paragraf 3'te, hakkın saklı tutulması temelinde (bkz Madde 42) ulusal mevzuatlarda suçu sınırlamaya izin verilmiştir. Ancak, Taraflar, paragraf 1 (a) 2'de belirtildiği gibi, en azından bilgisayar şifreleri ve erişim verilerinin satış, dağıtım ve elde edilebilir hale getirilmesini suç olarak tanımlamak zorundadır.

BAŞLIK 2
Bilgisayarlarla İlişkili Suçlar

79. Madde 7 - 10, sık sık bir bilgisayar sistemi kullanılarak işlenen sıradan suçlarla ilgilidir. Çoğu Ülke bu sıradan suçları suç olarak tanımlamış durumdadır ve bu Ülkelerin mevcut mevzuatı bilgisayar ağlarını içine alacak kadar geniş olabilir ya da olmayabilir (örneğin, bazı ülkelerin mevcut çocuk pornografisi yasaları elektronik görüntülere uygulanabilir değildir). Bu nedenle, Ülkeler, bu Maddeleri uygulama sürecinde, mevcut mevzuatlarını inceleyerek bilgisayar sistem ve ağlarının söz konusu olduğu durumlara uygulanıp uygulanamayacaklarına karar vermelidirler. Mevcut suçlar halihazırda bu fiilleri içine alıyorsa, mevcut suçlar üzerinde değişiklik yapmak ya da yeni suçlar tesis etmek gerekli değildir.

80. "Bilgisayarlarla ilişkili sahtecilik fiilleri" ve "Bilgisayarlarla ilişkili sahtekarlık fiilleri", bilgisayarlarla ilişkili belirli suçları, yani bilgisayarlarla ilişkili sahtecilik ve bilgisayarlarla ilişkili sahtekarlığı, bilgisayar sistemlerinin ve bilgisayar verilerinin manipülasyonunun iki spesifik türü olarak ele almaktadır. Bu suçların

kapsam dahiline alınması, bazı geleneksel yasal hakların birçok ülkede yeni müdahale ve saldırı biçimlerine karşı yeterince korunmadığı gerçeğini yansıtmaktadır.

Madde 7 - Bilgisayarlarla İlişkili Sahtecilik Fiilleri

81. Bu Maddenin amacı, somut belgelerle ilgili sahteciliğe paralel bir suç tesis etmektir. Ceza hukukundaki, bir belgedeki ifadelerin ya da beyanların görsel olarak okunabilirliğini şart koşan ve elektronik olarak saklanan verilere uygulanamayan geleneksel sahtecilikle ilgili boşlukların doldurulması amaçlanmaktadır. Delil teşkil eden bu tür verilerin manipülasyonu, üçüncü bir şahsın yanlış yönlendirilmesine neden oluyorsa geleneksel sahtecilikle aynı ciddi sonuçlara yol açabilir. Bilgisayarlarla ilişkili sahtecilik, verilerde içerilen bilgilerin doğruluğuna dayalı hukuki işlemler sırasında verilerin delil olarak değerlerini değiştirmek üzere izinsiz olarak veri yaratılması ya da saklanan verilerin değiştirilmesi yoluyla kandırmaya yöneliktir. Korunan yasal hak, hukuki ilişkiler açısından önemli olabilecek elektronik verilerin güvenliği güvenilirliğidir.

82. Ulusal sahtecilik kavramlarının büyük değişiklik gösterdiği göz ardı edilmemelidir. Bir kavram belgenin yazarının sahliliğini esas alırken, diğlereri belgede yer alan ifadenin doğruluğunu esas alır. Ancak, sahlilik konusunda kandırma, verilerin içeriğinin doğruluğu ya da ya da gerçekliğinden bağımsız olarak verileri yayınlayanla ilgilidir. Taraflar daha ileriye de gidebilir ve "sahlil" teriminin çerçevesine verilerin hakikiliğı de sokabilirler.
83. Bu hüküm, yasal geçerliliğı olan kamusal ve özel belgenin eşdeğeri olan verileri ele almaktadır. Doğru ve yanlış verilerin izinsiz olarak "ilave edilmesi", sahte bir belgenin üretilmesine karşılık düşmektedir. Daha sonraki değıştirmeler (farklı hale getirme, farklı biçimlerini üretme, kısmi değışiklik), silme (verilerin veri ortamından çıkarılması) ve erişilemez kılma (verilerin gizli tutulması, saklanması) genel olarak hakiki bir belgenin tahrifine karşılık düşmektedir.
84. "Hukuki açıdan" terimi hukuki olarak ilgili hukuki işlemleri ve belgeleri de kapsamaktadır.
85. Hükümün son cümlesi Tarafların suçu ulusal mevzuatlarına uygularken cezai yükümlülüğün

ortaya çıkmasını hile veya benzeri bir sahtekarlık niyetinin mevcut olması şartına bağlamalarına izin vermektedir.

Madde 8 - Bilgisayarlarla İlişkili Sahtekarlık Fiilleri

86. Teknoloji devrimiyle birlikte kredi kartı sahtekarlıkları da dahil olmak üzere sahtekarlık gibi ekonomik suçları işleme fırsatları arttı. Bilgisayar sistemlerinde temsil edilen ya da yönetilen varlıklar (elektronik fonlar, banka parası) geleneksel mülkiyet biçimleri gibi manipülasyon hedefi haline geldiler. Bu suçların başlıcaları bilgisayara yanlış verilerin girildiği veri ekleme manipülasyonları, program manipülasyonları ve veri işleme sürecine yapılan diğer müdahalelerdir. Bu Maddenin amacı mülkiyeti yasadışı biçimde nakletmek amacıyla veri işleme sürecine yapılan kanunsuz manipülasyonları suç olarak tanımlamaktır.

87. Bütün olası ilgili manipülasyonları kapsam dahiline almak için Madde 8(a)'daki "yeni veriler ekleme", "değiştirme", "silme" veya "erişilmez kılma" şeklindeki teşkil edici unsurlara Madde 8(b)'deki "bir bilgisayar programı ya da sisteminin işleyişine müdahale" şeklindeki genel

fiil eklenmiştir. "Veri ekleme, değiştirme, silme ve veya erişilmez kılma" unsurları, bir önceki Maddedekiyle aynı anlamdadır. Madde 8(b), donanım manipölasyonları gibi fiilleri, yazıcı çıktılarını erişilmez kılmaya yönelik fiilleri ve verilerin kaydedilmesini ya da akışını ya da programların çalışma sırasını etkilemeye yönelik fiilleri kapsamaktadır.

88. Bilgisayar sahtekarlığı manipölasyonları, başka bir kişinin mülkiyetinin doğrudan ekonomik ya da zilyetlik kaybına yol açıyorsa ve fail kendisi ya da bir başkasına kanunsuz ekonomik kazanç sağlamayı amaçladıysa suç olarak tanımlanır. Geniş bir kavram olan "mülkiyetin kaybı" terimi, paranın, ekonomik değeri olan maddi ve gayrimaddi varlıkların kaybını kapsar.
89. Suç "haksız biçimde" işlenmiş ve haksız maddi menfaat sağlanmış olmalıdır. Şüphesiz, maddi menfaat sağlamayı amaçlayan meşru yaygın ticari uygulamaların bu Maddede tanımlanan suça dahil edilmeleri düşünülmemiştir, çünkü bu uygulamalar haklı biçimde gerçekleştirilmektedir. Örneğin, etkilenen kişilerle yapılmış geçerli bir sözleşmeye uygun olarak yürütülen faaliyetler haklı olarak gerçekleştirilmektedir (örneğin

sözleşme hükümlerine uygun biçimde bir web sitesini çalışmaz hale getirmek).

90. Suç "kasıtlı" olarak işlenmiş olmalıdır. Genel kasıt unsuru bir başkasının mülkiyetinin kaybına yol açan bilgisayar manipülasyonu, ya da müdahale anlamındadır. Suç ayrıca işleyenin kendisi ya da bir başkasına maddi ya da başka tür menfaat sağlamak amacıyla spesifik bir hile ya da başka tür bir sahtekarlık niyetinin varlığını da şart koşturmaktadır. Bu nedenle, örneğin, piyasa rekabeti çerçevesinde yürütülen, bir kişiye maddi zarar ve bir başkasına kazanç sağlayan, ama hile ya da başka tür bir sahtekarlık niyetiyle gerçekleştirilmiş olmayan ticari faaliyetlerin bu Maddede tanımlanan suça dahil edilmeleri amaçlanmamıştır. Örneğin, İnternet'te karşılaştırmalı alışveriş için kullanılan bilgi toplama programlarının ("bot") kullanımı, "bot"un ziyaret ettiği siteden izin alınmamış olsa bile suç olarak tanımlanmamıştır.

BAŞLIK - 3
İçerikle İlişkili Suçlar

Madde 9 - Çocuk Pornografisiyle İlişkili Suçlar.

91. Çocuk pornografisiyle ilgili olan Madde 9'da ceza hukuku hükümlerini, çocuklara karşı işlenen cinsel suçlarda bilgisayar sistemlerinin kullanımını daha iyi kapsayacak şekilde modernleştirerek, cinsel sömürüye karşı korunmaları da dahil olmak üzere çocuklarla ilgili koruyucu önlemler güçlendirilmeye çalışılmıştır.
92. Bu hüküm, Avrupa Konseyi Devlet ve Hükümet Başkanlarının 2. zirvesinde (Strasbourg, 10 - 11 Ekim 1997) hazırlanan Eylem Planında (madde III.4) belirtilen kaygılara cevap olarak hazırlanmıştır ve çocuk hakları, çocukların satışı, çocuk fuhuşu ve çocuk pornografisine ilişkin BM Konvansiyonunun Seçmeli Protokolünün kısa bir süre önce benimsenmesinde ve Avrupa Komisyonunun kısa bir süre önce başlattığı çocukların cinsel sömürüsü ve çocuk pornografisiyle mücadele girişiminde (COM2000/854) görülen çocuk pornografisini

134 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

yasaklamaya yönelik uluslararası trendle de uyumludur.

93. Bu hükümle çocuk pornografisinin elektronik üretimi, bulundurulması ve dağıtımının çeşitli yönleri suç olarak tanımlanmıştır. Çoğu Ülkenin çocuk pornografisinin geleneksel üretimini ve fiziksel dağıtımını suç olarak tanımlamış durumda olmasına rağmen, bu tür malzemelerin alışverişinde başlıca araç olarak İnternet'in kullanımının giderek artması karşısında çocukların bu yeni cinsel sömürü ve tehdit biçimine karşı savunulması için uluslararası hukuki bir araca spesifik hükümlerin yerleştirilmesinin temel önemde olduğu kuvvetle hissedilmiştir. Bu malzemelerin ve pedofillerin fikir, fantezi ve tavsiye değiş tokuşunda bulunmaları gibi online uygulamaların çocuklara karşı işlenen cinsel suçları desteklemekte, teşvik etmekte veya kolaylaştırmakta rol oynadığı, yaygın olarak paylaşılan bir görüştür.

94. Paragraf 1(a)'da bir bilgisayar sistemi üzerinden dağıtılmak amacıyla çocuk pornografisi üretmek suç olarak tanımlanmıştır. Yukarıda tanımlanan tehlikelerle kaynağında mücadele etmek için bu hükmün gerekli olduğu düşünülmüştür.

95. Paragraf 1(b)'de bir bilgisayar sistemi üzerinden çocuk pornografisi "sunmak" suç olarak tanımlanmıştır. "Sunmak" kelimesinin çocuk pornografisi elde etmek amacıyla başka kişilere başvurmayı da kapsamı amaçlanmıştır. Bu, malzemeyi sunan kişinin onu gerçekten sağlayabileceği anlamına gelmektedir. "Erişim sağlamak" ifadesinin, örneğin bir çocuk pornografisi sitesi oluşturarak, başkalarının kullanımı için çocuk pornografisini online erişime sunmayı kapsamı amaçlanmıştır. Bu paragrafta, çocuk pornografisine erişimi kolaylaştırmak için çocuk pornografisi sitelerine hiper-metinlerin yaratılması ve derlenmesinin de kapsanması amaçlanmaktadır.
96. Paragraf 1(c)'de bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ve yaymak suç olarak tanımlanmıştır. "Dağıtım" malzemenin aktif olarak yayınlanmasıdır. Bir bilgisayar sistemi üzerinden başka bir kişiye çocuk pornografisi göndermek, çocuk pornografisi "yayma" suçu olarak ele alınacaktır.
97. Paragraf 1(d)'deki "kendisi ya da başkası için temin etmek" terimi, örneğin bilgisayarına

indirme yoluyla, aktif olarak çocuk pornografisi elde etmek anlamındadır.

98. Bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda, örneğin bir disket ya da CD-Rom'da, çocuk pornografisi bulundurmak paragraf 1(e)'de suç olarak tanımlanmıştır. Çocuk pornografisi bulundurmak bu tür malzeme için talebi canlandırır. Üretimden bulundurmaya kadar zincirin bütün parçalarının fiilleri için cezai sonuçlar getirmek, çocuk pornografisi üretimini azaltmanın etkin bir yoludur.
99. Paragraf 2'deki "pornografik malzemeler" terimi, malzemelerin müstehcen, kamu ahlakına aykırı ve benzer biçimde ahlak dışı şeklinde sınıflandırılması açısından ulusal standartlara tabidir. Bu nedenle, sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan malzemeler pornografik olmayan malzemeler olarak görülebilir. Görsel teşhir, bilgisayar disketi ya da başka elektronik saklama ortamlarında saklanan, görsel malzemeye dönüştürülebilen verileri de içine alır.

100. "Cinsel anlamda müstehcen eylem" gerçek ya da simülasyon olarak en az şunları içine almaktadır: a) cinsel organ-cinsel organ, oral-cinsel organ, anal-cinsel organ veya oral-anal olmak üzere, reşit olmayan kişiler arasındaki, bir yetişkin ve bir reşit olmayan kişi arasındaki, aynı ya da farklı cinsiyetler arasındaki cinsel ilişki; b) hayvanlarla cinsel ilişki; c) mastürbasyon; d) cinsel anlamda sadistik ya da mazoşistik kötü muamele; ya da e) reşit olmayan bir kişinin cinsel organlarının ya da cinsel bölgesinin şehvet uyandırıcı biçimde teşhiri. Fiilin gerçek ya da simülasyon olması önemli değildir.

101. Paragraf 2'de tanımlanan, paragraf 1'de belirtilen suçları işlemek amacıyla üretilen üç tür malzeme, gerçek bir çocuğun cinsel olarak kötü muameleye uğramasının teşhirini (2a), reşit görünmeyen bir kişinin cinsel anlamda müstehcen bir eyleme katılımını gösteren pornografik görüntüleri (2b), ve son olarak "gerçekçi" olmakla birlikte gerçek bir çocuğun cinsel anlamda müstehcen bir eyleme katılımını içermeyen görüntüleri (2c) kapsamaktadır. Son örnekte gerçek insanların üzerinde oynanmış görüntüleri gibi değiştirilmiş, hatta tamamen bilgisayarda üretilmiş resimler söz konusudur.

102. Paragraf 2'de ele alınan üç durumda korunan yasal haklar biraz değişiktir. Paragraf 2(a)'da çocukları kötü muameleden koruma daha doğrudan doğruya ele alınmıştır. Paragraf 2(b) ve 2(c)'de, malzemedeki gösterilen "çocuğa" gerçekten zarar verilmese ve gerçek bir çocuk söz konusu olmasa bile, çocukları bu tür fiillere teşvik edebilecek ya da ayartabilecek ve böylece çocuklara kötü muameleye izin veren bir alt kültürün oluşmasına katkıda bulunabilecek bir davranışa karşı koruma sağlamak amaçlanmıştır.

103. "Haksız biçimde" terimi, özel şartlar altında bir kişiyi sorumluluktan kurtaracak yasal savunmaları, mazeretleri ve ilgili benzer ilkeleri hariç tutmamaktadır. Dolayısıyla, "haksız biçimde" terimi Tarafların düşünce, ifade ve özel hayat özgürlüğü gibi temel hakları göz önünde bulundurmasına izin vermektedir. Ayrıca, Taraflar sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan "pornografik malzeme"yle ilgili fiiller hakkında bir savunma sağlayabilirler. "Haksız biçimde" terimi, paragraf 2(b)'yle ilgili olarak da, örneğin Tarafların gösterilen kişinin bu hükümde kullanılan anlamda reşit olmayan bir kişi olmadığını saptanması durumunda kişinin cezai

sorumluluktan kurtulmasını sağlamalarına da izin verebilir.

104. Paragraf 3'te "reşit olmayan kişi" terimi, çocuk pornografisiyle ilgili olarak, BM Çocuk Hakları Konvansiyonundaki "çocuk" tanımına (Madde 1) uygun biçimde, genel olarak 18 yaşından küçük herkes şeklinde tanımlanmıştır. Yaş konusunda tek bir uluslararası standart belirlemek önemli bir politika olarak görülmüştür. Burada söz edilen yaşı (gerçek ya da kurgusal) çocukların cinsel nesne olarak kullanılmasıyla ilgili olduğu ve cinsel ilişki için izin yaşıdan farklı olduğu göz önünde bulundurulmalıdır. Ancak, belli ülkelerin çocuk pornografisiyle ilgili ulusal mevzuatlarında bir alt yaş sınırı getirdiği göz önüne alınarak, paragraf 3'ün son cümlesinde, Tarafların, 16'dan küçük olmamak şartıyla, farklı bir yaş sınırı getirmelerine izin verilmiştir.

105. Bu Maddede, Tarafların, çocuk pornografisiyle ilgili olarak, Madde 2-8'de olduğu gibi "kasıtlı" işlendiyse suç olarak tanımlamak zorunda oldukları yasadışı fiil türleri sıralanmıştır. Bu standarda göre, çocuk pornografisi sunmak, erişim sağlamak, dağıtmak, yaymak, üretmek ya da bulundurmak konusunda bir niyet taşımayan

bir kişi, yükümlü tutulamaz. Taraflar daha spesifik bir standart benimseyebilirler. (bkz., örneğin, hizmet sağlayıcı yükümlülükleriyle ilgili geçerli Avrupa Topluluğu yasası) ve bu durumda bu standart geçerli olur. Örneğin, yayılan ya da saklanan bilgi üzerinde "bilgi ve kontrol" mevcutsa yükümlülük doğabilir. Örneğin bir hizmet sağlayıcısının, ulusal mevzuatta bu konuyla ilgili gerekli niyet olmaksızın bir taşıyıcı işlevi üstlenmesi ya da bu tür malzemeler içeren bir web sitesi ya da haber odasını barındırması yeterli değildir. Ayrıca, bir hizmet sağlayıcı cezai yükümlülükten kurtulmak için fiilleri denetlemek zorunda değildir.

106. Paragraf 4'te Taraflara paragraf 1(d) ve (e) ile paragraf 2(b) ve (c) ile ilgili haklarını saklı tutma izni vermektedir. Hükmün bu kısımlarını uygulamama hakkı kısmen ya da tamamen kullanılabilir. Bu tür bütün saklı tutmalar, Madde 42 uyarınca, imza sırasında ya da Tarafın onay, kabul, tasdik ya da katılım araçlarını tevdi etmesi sırasında Avrupa Konseyi Genel Sekreterine beyan edilmelidir.

BAŞLIK - 4
*Telif Haklarının ve Benzer Hakların İhlaline
İlişkin Suçlar*

**Madde 10 - Telif Haklarının ve Benzer Hakların
İhlaline İlişkin Suçlar**

107. Fikri mülkiyet haklarının, özellikle de telif haklarının ihlali, İnternet'te en yaygın olarak işlenen suçlar arasındadır; ve bu durum hep telif hakkı sahipleri hem de bilgisayar ağları üzerinde profesyonel olarak çalışan kişiler için rahatsızlık yaratmaktadır. Koruma altındaki eserlerin, telif hakkı sahibinin onayı olmadan İnternet üzerinde yeniden üretimi ve yayımı son derece yaygındır. Koruma altındaki eserler arasında edebiyat, fotoğraf, müzik eserleri, görsel-ışitsel eserler ve diğer eserler bulunmaktadır. Dijital teknolojiler aracılığıyla izinsiz kopya çıkarmanın kolaylığı ve elektronik ağlarda yeniden üretim ve yayımın boyutları ceza hukuku hükümleri eklemeyi ve bu alandaki uluslararası işbirliğini genişletmeyi zorunlu hale getirmiştir.

108. Taraflardan her biri, telif haklarının ve bazen benzer haklar olarak anılan ilgili hakların kötü niyetli ihlallerini, Maddede sayılan anlaşmalar

uyarınca, bir bilgisayar sistemi aracılığıyla ve ticari ölçekte yapıldığında suç olarak tanımlamak zorundadır. Paragraf 1'de, bir bilgisayar sistemi aracılığıyla gerçekleştirilen telif hakları ihlallerine karşı cezai yaptırımlar getirilmiştir. Telif hakkı ihlali hemen hemen bütün ülkelerde halihazırda suç kapsamındadır. Paragraf 2'de ilgili hakların bir bilgisayar sistemi aracılığıyla ihlal edilmesi ele alınmaktadır.

109. Hem telif haklarının hem de ilgili hakların ihlali Taraflardan her birinin mevzuatları ve belirli uluslararası araçlarla ilişkili olarak Tarafların üstlenmiş olduğu yükümlülükler çerçevesinde tanımlanmıştır. Bütün Taraflar bu ihlalleri cezai suç olarak tanımlamak zorunda olmakla birlikte, ulusal mevzuatlarda bu ihlallerin tanımlanma biçimlerinin detayları ülkeler arasında farklılık gösterebilir. Ancak, Konvansiyon çerçevesinde suç olarak tanımlama zorunlulukları Madde 10'da açıkça belirtilenler dışındaki fikri mülkiyet ihlallerini kapsamamakta ve dolayısıyla patent ya da ticari markayla ilgili ihlalleri dışarıda bırakmaktadır.

110. Paragraf 1'de anılan sözleşmeler, Edebi ve Sanatsal Eserlerin Korunmasına Yönelik Bern

Konvansiyonu çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme (TRIPS) ve Dünya Fikri Mülkiyet Kuruluşu (WIPO) Telif Hakları Anlaşması'dır. Paragraf 2'de anılan uluslararası araçlar, Oyuncuların, Fonogram Yapımcılarının ve Yayın Kuruluşlarının Korunması Hakkında Uluslararası Konvansiyon (Roma Konvansiyonu), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme (TRIPS) ve Dünya Fikri Mülkiyet Kuruluşu (WIPO) Oyunculuk ve Fonogramlar Anlaşması'dır. Her iki paragrafta da "üstlendiği yükümlülükler uyarınca" teriminin kullanımı, işbu Konvansiyonu imzalayan Tarafların anılanlar arasında Tarafı olmadıkları sözleşmelere uymakla yükümlü olmadıklarını açıkça ortaya koymaktadır, ve ayrıca, Taraflar bu sözleşmelerden birinde izin verilen bir haklarını saklı tutmuş ya da bir beyanda bulunmuşlarsa bu saklı tutma bu Konvansiyon çerçevesindeki yükümlülüklerinin kapsamını sınırlandırabilir.

111. WIPO Telif Hakları Anlaşması ve WIPO Oyunculuk ve Fonogramlar Anlaşması, işbu Konvansiyonun tamamlanması sırasında henüz yürürlüğe girmemişti. Ancak, fikri mülkiyetin

uluslararası düzeyde korunmasını önemli ölçüde güncelleştirdikleri (özellikle koruma altındaki malzemelerin "talep üzerine" İnternet üzerinden "erişilebilir kılınması"na ilişkin yeni hakla ilgili olarak) ve dünya çapında fikri mülkiyet hakları ihlalleriyle mücadele yollarını geliştirdikleri için bu anlaşmalar büyük önem taşımaktadır. Bu anlaşmalar Taraflar için yürürlüğe girinceye kadar anlaşmalarda ele alınan hak ihlallerinin işbu Konvansiyon çerçevesinde suç olarak tanımlanmasına gerek olmadığına karar verilmiştir.

112. Uluslararası araçlar çerçevesinde üstlenilen yükümlülükler uyarınca telif hakkı ve ilgili hakların ihlallerini suç olarak tanımlama yükümlülüğü söz konusu araçlar tarafından verilen ahlaki haklar için geçerli değildir (örneğin Bern Konvansiyonu Madde 6-bis- ve WIPO Telif Hakları Anlaşması Madde 5).

113. Cezai yükümlülüğün doğması için telif hakkı ve ilgili haklarla ilişkili suçların "kötü niyetli olarak" işlenmesi gerekmektedir. İşbu Konvansiyondaki bütün diğer maddi hukuk hükümlerinden farklı olarak, paragraf 1 ve 2'de "kasıtlı olarak" yerine "kötü niyetli olarak" terimi kullanılmıştır. Telif

hakkı ihlallerini suç olarak tanımlama yükümlülüğü getiren TRIPS Sözleşmesinde (Madde 61) bu terim kullanılmıştır.

114. Hükümlerde "ticari ölçekte" ve bir bilgisayar sistemi aracılığıyla gerçekleştirilen ihlallere karşı cezai yaptırımlar getirilmesi amaçlanmıştır. Bu, telif hakları meselelerinde cezai yaptırımları yalnızca "ticari ölçekte korsanlık" durumunda şart koşan TRIPS Sözleşmesi Madde 61'le uyumludur. Ancak Taraflar "ticari ölçek" eşiğini aşmayı ve başka tür telif hakkı ihlallerini de suç olarak tanımlamayı tercih edebilirler.

115. "İhlal" terimi telif haklı malzemenin izinsiz kullanımı anlamına geldiği için bu Maddenin metninde "haksız biçimde" terimine gerek görülmemiştir. "Haksız biçimde" teriminin yokluğu, tersinden yorumlanarak, Konvansiyonun başka yerlerinde geçen "haksız biçimde" terimiyle bağlantılı cezai yükümlülük hariç bırakmalarını düzenleyen ceza hukuku savunmalarının, geçerli sebeplerinin ve ilkelerinin uygulanmasını dışlamaz.

116. Paragraf 3'te Tarafların "belirli durumlarda" (örneğin paralel ithalat, kiralama hakları), medeni

ve/veya idari önlemler gibi başka etkin çözümler bulunması şartıyla paragraf 1 ve 2 çerçevesindeki cezai yükümlülükleri ihdas etmemelerine izin verilmiştir. Bu hüküm, temelde, Taraflara, önceden mevcut minimum suç olarak tanımlama şartı olan TRIPS Sözleşmesi Madde 61 çerçevesindeki zorunlulukları terk etmemek şartıyla, cezai yükümlülük ihdas etme konusundaki zorunlulukları için sınırlı bir muafiyet tanımaktadır.

117. Bu Madde hiçbir şekilde, yazarlara, film yapımcılarına, oyunculara, fonogram yapımcılarına, yayın kuruluşlarına ya da başka hak sahiplerine tanınan korumayı, ulusal mevzuat ve uluslararası sözleşmeler çerçevesinde gerekli ölçütlere uymayan kişilere de uygulanacak şekilde yorumlanamaz.

BAŞLIK - 5
İlave Yükümlülük ve Yaptırımlar

Madde 11 - Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek

118. Bu Maddenin amacı, işbu Konvansiyonda tanımlanan suçların işlenmesine teşebbüs ve yardım ya da yataklık etmekle ilişkili ek suçları tanımlamaktır. Aşağıda tartışıldığı gibi, Tarafların işbu Konvansiyonda tanımlanan suçların her birini işlemeye teşebbüsü suç olarak tanımlamaları zorunlu değildir.

119. Paragraf 1'de, Tarafların, Madde 2-10'da tanımlanan suçların herhangi birinin işlenmesine yardım ve yataklık etmeyi cezai bir suç olarak tanımlamaları şart koşulmuştur. Konvansiyonda tanımlanan bir suçu işleyen birine yine suçun işlenmesine niyet etmiş biri tarafından yardım edilirse yardım ve yataklıkla ilgili yükümlülük doğar. Örneğin, zararlı içerik verilerinin ya da kötü amaçlı kodların İnternet üzerinden iletimi taşıyıcı olarak hizmet sağlayıcılarının yardımını gerektirmekle birlikte, cezai niyet taşımayan bir hizmet sağlayıcısı bu Kısım çerçevesinde yükümlülük altına girmemektedir. Dolayısıyla, bu

hüküm çerçevesinde cezai yükümlülükten kaçınmak için içeriği aktif olarak denetlemek hizmet sağlayıcısının görevi değildir.

120. Teşebbüsle ilişkili paragraf 2'yle ilgili olarak, Konvansiyonda tanımlanan bazı suçlar ya da bu suçların unsurları için teşebbüsün kavramsal olarak güç olduğu düşünülmüştür (örneğin çocuk pornografisini sunmak ve buna erişim sağlamak unsurları). Ayrıca, bazı hukuk sistemleri teşebbüsün cezalandırılabilirdiği suçları sınırlamıştır. Dolayısıyla, sadece Madde 3, 4, 5, 7, 8, 9(1)(a) ve 9(1)(c)'de tanımlanan suçlarla ilgili olarak teşebbüsün suç olarak tanımlanması şart koşulmuştur.

121. Konvansiyonda tanımlanan bütün suçlarda olduğu gibi, teşebbüs ve yardım ya da yataklık kasıtlı olarak işlenmiş olmalıdır.

122. Paragraf 3, Tarafların, farklı mevzuatlardaki büyük bir çeşitlilik gösteren kavramlar yüzünden ve paragraf 2'deki hükmün teşebbüsle ilgili belirli konulara muafiyet getirme çabasına karşın, paragraf 2'yle ilgili olarak yaşayabilecekleri sorunlar düşünülerek eklenmiştir. Taraflar paragraf 2'yi kısmen ya da tamamen

uygulamama hakkını saklı tuttuğunu beyan edebilir. Bu durum, bu hükümle ilgili hakkını saklı tutan herhangi bir Taraf Ülkenin teşebbüsü suç olarak tanımlamak konusunda hiçbir zorunlulukla karşı karşıya olmayacağı, ya da teşebbüsle ilgili olarak cezai yaptırımlar getireceği suç ya da suç bölümlerini seçebileceği anlamına gelmektedir. Hakkın saklı tutulmasının amacı, Tarafların bazı temel hukuki kavramlarını korurken, Konvansiyon için mümkün olan en geniş katılımı sağlamaktır.

Madde 12 - Kurumsal Yükümlülük

123. Madde 12 tüzel kişiliklerin yükümlülükleriyle ilgilidir. Madde, günümüzdeki kurumsal yükümlülüğü tanımaya yönelik hukuki trendle tutarlıdır. Maddenin amacı, bir tüzel kişilikte yönetici konumunda olan bir kişi tarafından, tüzel kişiliğin menfaatine gerçekleştirilmiş suçlar için şirketlere, kuruluşlara ve benzeri tüzel kişiliklere yükümlülük ihdas etmektir. Madde 12'de böyle yönetici konumundaki bir kişinin gözetlememesi ya da kontrol etmemesi sonucunda tüzel kişiliğin bir çalışanı ya da vekilinin işbu Konvansiyonda tanımlanan suçları

işlemesinin kolaylaşması durumunda ortaya çıkan yükümlülük de ele alınmıştır.

124. Paragraf 1'e göre yükümlülüğün ortaya çıkması için dört şartın sağlanması gerekmektedir. Birincisi, Konvansiyonda tanımlanan suçlardan biri işlenmiş olmalıdır. İkincisi, suç tüzel kişiliğin menfaatine işlenmiş olmalıdır. Üçüncüsü, suçu (yardım ve yataklık da dahil olmak üzere) yönetici konumundaki bir kişi işlemiş olmalıdır. "Yönetici konumundaki kişi" terimi, kuruluştaki müdürlük gibi yüksek bir konuma sahip gerçek bir kişi anlamındadır. Dördüncüsü, tüzel kişiliğe yükümlülük doğması için yönetici konumundaki gerçek kişinin kendi yetkileri dahilinde hareket ettiğini gösteren bir yetkiye -temsil etme yetkisi ya da karar alma veya kontrol etme yetkisi- dayanarak hareket etmiş olması gereklidir. Kısaca, paragraf 1 Tarafların sadece bu şekilde yönetici konumundaki kişiler tarafından işlenen suçlar için tüzel kişilikler üzerine yükümlülük getirme yetkisine sahip olmasını şart koşturmaktadır.

125. Ayrıca, paragraf 2, Tarafların, paragraf 1'de tanımlanan yönetici konumundaki kişi tarafından değil, tüzel kişiliğin yetkisi altında faaliyet

gösteren başka bir kişi, yani tüzel kişiliğin kendi yetkileri dahilinde faaliyet gösteren bir çalışanı ya da vekili tarafından suçun işlenmesi durumunda tüzel kişilik üzerine yükümlülük getirme yetkisine sahip olmasını şart koşturmaktadır. Yükümlülük doğması için şu şartlar sağlanmalıdır: (1) suç tüzel kişiliğin bir çalışanı ya da vekili tarafından işlenmiş olmalıdır, (2) suç tüzel kişiliğin menfaatine işlenmiş olmalıdır; ve (3) suçun işlenmesi yönetici konumundaki kişinin çalışan ya da vekil üzerindeki gözetim görevini yerine getirmemiş olması sonucunda mümkün hale gelmiş olmalıdır. Bu bağlamda, gözetim görevini yerine getirmemiş olmak, çalışanların ya da vekillerin tüzel kişilik menfaatine suç işlemelerini önlemeye yönelik uygun ve makul önlemleri almamış olmayı da içerecek şekilde yorumlanmalıdır. Uygun ve makul önlemler, işin türü, hacmi, standartlar ya da yerleşik en iyi iş yapma uygulamaları vs. gibi çeşitli etkenlerce belirlenebilir. Bu durum, çalışan iletişimleri üzerinde bir gözetim rejimini şart koşturmak olarak yorumlanmamalıdır (bkz. paragraf 54). Sisteminde bir müşteri, kullanıcı ya da herhangi bir üçüncü şahıs tarafından suç işlenmesi hizmet sağlayıcı için yükümlülük

doğurmaz, çünkü "yetkisi altında faaliyet gösteren" terimi münhasıran kendi yetkileri dahilinde hareket eden çalışan ve vekiller için geçerlidir.

126. Bu Madde çerçevesindeki yükümlülük cezai, medeni ya da idari olabilir. Taraflardan her biri, Madde 13, paragraf 2'de belirtilen yaptırım ya da önlemin "etkin, adil ve caydırıcı" olması ve parasal yaptırımları içermesi ölçütlerine sadık kalmak şartıyla kendi hukuk ilkelerine uygun olarak bu yükümlülük biçimlerinden bazılarını ya da hepsini getirmeyi seçme esnekliğine sahiptir.

127. Paragraf 4, kurumsal yükümlülüğün bireysel yükümlülüğü dışlamadığı noktasına açıklık getirmektedir.

Madde 13 - Yaptırımlar ve Önlemler

128. Bu Madde ceza hukuku çerçevesinde cezalandırılabilir hale getirilmesi gereken bilgisayar suçlarının veya bilgisayarla bağlantılı suçların tanımlandığı Madde 2-11'le yakından bağlantılıdır. Bu Maddelerde getirilen zorunluluklara uygun olarak bu hüküm, Konvansiyonu imzalayan Tarafların bu suçların ciddiyetiyle ilgili sonuçlar çıkararak "etkin, adil

ve caydırıcı" ve gerçek kişiler söz konusu olduğunda hapis cezası olasılığını da içeren cezai yaptırımlar getirmelerini şart koşturmaktadır.

129. Yükümlülükleri Madde 12'de saptanmış olan tüzel kişilikler de cezai, idari ya da medeni nitelikte olabilecek "etkin, adil ve caydırıcı" yaptırımlara tabi olmalıdır. Konvansiyonu imzalayan Taraflar, paragraf 2 çerçevesinde tüzel kişiliklere parasal yaptırımlar getirme olasılığını yaratmak zorundadırlar.

130. Maddede, suçların ciddiyetine bağlı olarak başka yaptırım ve önlem olasılıklarını açık bırakılmaktadır; örneğin, önlemler ihtiyati tedbir ve hakkın düşmesini de içerebilir. Mevcut ulusal hukuk sistemleriyle uyumlu bir cezai suç ve yaptırımlar sistemi yaratmak konusunda takdir yetkisi Taraflara bırakılmaktadır.

KISIM - 2

Usul Hukuku

131. Bu Kısımdeki Maddelerde, Kısım I'de tanımlanan suçların cezai soruşturması, bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlar ve cezai bir suça ilişkin olarak elektronik ortamda delil toplanması amacıyla ulusal düzeyde alınacak belli usul tedbirleri tanımlanmaktadır. Madde 39, paragraf 3 uyarınca, bu Konvansiyonun hiçbir hükmünde Taraflar Konvansiyonda içerilenler dışında herhangi bir yetki ya da usul tesis etmeye zorlanmamakta ya da davet edilmemekte, ayrıca Tarafların bunu yapmaları engellenmemektedir.

132. Çok sayıda iletişim biçimi ve hizmetin ortak iletim ortamları ve taşıyıcılarıyla birbirleriyle bağlantılı ve ilişki içinde olduğu "elektronik otoban"ı da içine alan teknolojik devrim ceza hukuku ve ceza usulleri alanlarını da değiştirdi. Sürekli genişleyen iletişim ağı, hem geleneksel suçlar hem de yeni teknolojik suçlarla ilgili olarak suç niteliğindeki faaliyetler için yeni imkanlar yarattı. Maddi ceza hukuku gibi ceza usulleri hukuku ve soruşturma teknikleri de bu yeni suçlara ayak uydurmalıdır. Aynı şekilde

önlemler de yeni teknolojik ortama ve yeni usul yetkilerine ayak uyduracak şekilde uyarlanmalı ve geliştirilmelidir.

133. Ağ ortamında suçla mücadele etmenin en büyük güçlüklerinden biri faili teşhis etmek ve suç teşkil eden fiilin kapsamını ve etkilerini değerlendirmektir. Bir diğer sorun birkaç saniyede değiştirilebilen, taşınabilen ya da silinebilen elektronik verilerin geçici niteliğidir. Örneğin, verileri kontrolü altında bulunduran bir kullanıcı bir cezai soruşturmaya konu olan verileri bilgisayar sistemini kullanarak silebilir ve böylece kanıtları yok edebilir. Hız ve, bazı durumlarda, gizlilik bir soruşturmanın başarısı için hayati önemde olabilmektedir.

134. Konvansiyon, arama ve el koyma gibi geleneksel usul önlemlerini yeni teknoloji ortamına uyumlu hale getirmektedir. Ek olarak, arama ve el koyma gibi geleneksel delil toplama önlemlerinin her şeyin geçici olduğu teknoloji ortamında etkinliğini sürdürmesini sağlamak için verilerin hızlı bir biçimde korunması gibi yeni önlemler yaratılmıştır. Yeni teknoloji ortamında veriler her zaman durağan olmadığı ve iletişim sürecinde akış halinde olabildiği için, trafik verilerinin

gerçek zamanda toplanması ve içerik verilerine müdahale gibi telekomünikasyonla ilgili diğer geleneksel toplama usulleri de iletişim sürecinde olan elektronik verilerin toplanmasını sağlayacak şekilde uyarlanmıştır. Bu önlemlerin bazıları, Avrupa Konseyi'nin bilgi teknolojisiyle bağlantılı ceza usulleri hukuku sorunlarıyla ilgili R (95) 13 sayılı Tavsiyesinde açıklanmıştır.

135. Bu Kısımda yer alan bütün hükümlerde spesifik ceza soruşturmaları ve takibatlarında kullanmak amacıyla veri elde edilmesine ve toplanmasına izin vermek amaçlanmıştır. İşbu Konvansiyonu kaleme alanlar, Konvansiyonun hizmet sağlayıcılarına belli bir zaman aralığı için rutin olarak trafik verilerini toplama ve saklama zorunluluğu getirmesinin gerekip gerekmediğini görüşmüşler, fakat uzlaşmaya varılamadığı için böyle bir zorunluluğu Konvansiyona almamışlardır.

136. Usuller, genel olarak, iki biçimde (saklanmış ya da iletişim sürecinde) olabilen, üç spesifik tür bilgisayar verisini (trafik verileri, içerik verileri ve abone verileri) de içine alan her tür bilgisayar verisi ile ilgilidir. Madde 1-18'de bu terimlerin bazılarının tanımları verilmiştir. Bir usulün belli

bir tür ya da biçimde elektronik veriye uygulanabilirliği, her bir Maddede spesifik olarak açıklandığı gibi, verilerin yapısına ve biçimine, ve usulün yapısına bağlıdır.

137. Bu Kısımın hükümlerinde, geleneksel usul yasalarını yeni teknoloji ortamına uyarlarken uygun terminolojinin nasıl olması gerektiği sorunu ortaya çıkmıştır. Seçenekler arasında geleneksel dile sadık kalmak ("arama" ve "el koyma"), konuyla ilgili başka uluslararası forumların (örneğin G8 Yüksek Teknoloji Suçları Altgrubu) metinlerinde benimsendiği gibi yeni ve daha teknolojik bilgisayar terimleri kullanmak ("erişim" ve "kopyalama") ve bunları karıştırarak bir uzlaşma aramak ("arama ya da benzer şekilde erişim" ve "el koyma ya da benzer şekilde güven altına alma") vardı. Elektronik ortamda kavramların evrimini yansıtırken bir yandan da bunların geleneksel kaynaklarını saptama ve koruma ihtiyacı yüzünden ülkelerin isterlerse eski "arama ve el koyma", isterlerse yeni "erişim ve kopyalama" kavramlarını kullanmalarına izin vermek şeklinde esnek bir yaklaşım benimsendi.

138. Kısımdaki bütün Maddelerde "yetkili merciler"den ve spesifik ceza soruşturma ve

takibatlarında kullanmak amacıyla bu mercilere verilecek yetkilerden söz edilmiştir. Bazı ülkelerde delil toplanması ve üretilmesi konusunda talimat verme ve yetkilendirme yetkisi sadece hakimlere tanınırken, bazı ülkelerde bu ya da buna benzer yetkiler savcılara ya da başka icra görevlilerine bırakılmıştır. Dolayısıyla, "yetkili merci", ulusal mevzuatın spesifik ceza soruşturma ve takibatlarında kullanmak üzere delil toplamak ya da üretmek konusunda talimat verme, yetkilendirme ya da usulle ilgili önlemleri icra etme yetkisini verdiği yargı, idare ya da başka tür icra mercii anlamındadır.

BAŞLIK - I
Genel Hükümler

139. Kısım, usul hukukuyla ilgili bütün Maddeler için geçerli genel amaçlı iki hükümle başlamaktadır.

Madde 14 - Usul Hükümlerinin Kapsamı

140. Taraf Ülkelerden her biri, ulusal mevzuatına ve hukuki çerçevesine uygun olarak, bu Kısımda tanımlanan yetki ve usulleri tesis etmek için gerekli olabilecek, "spesifik cezai soruşturma veya takibat"larla ilgili yasama önlemlerini ve diğer önlemleri benimsemek zorundadır.

141. İki istisnai durum dışında, Taraflardan her biri bu Kısma uygun olarak tesis edilen yetki ve usulleri: (i) Konvansiyonun 1. Kısmı uyarınca tesis edilen cezai suçlara; (ii) bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlara, ve (iii) cezai bir suça ilişkin olarak elektronik ortamda delil toplanmasına ilişkin olarak uygulamaya koyacaktır. Dolayısıyla spesifik cezai soruşturma ve takibatlarda kullanılmak üzere, bu Kısımda sözü edilen yetki ve usuller bu Konvansiyon uyarınca tesis edilen suçlara, bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlara ve cezai bir suça ilişkin olarak elektronik

ortamda delil toplanmasına ilişkin olarak uygulamaya konacaktır. Bu durum, bu Kısımda belirlenen yetkiler ve usuller yoluyla herhangi bir cezai suça ilişkin olarak elektronik ortamda delil elde edilebilmesini ve toplanmasını güvence altına almaktadır. Böylece bilgisayar verilerini elde etmek ve toplamak için de elektronik olmayan veriler için geleneksel yetkiler ve usuller çerçevesinde mevcut olanlara eşdeğer ya da paralel imkanlar sağlanmaktadır. Konvansiyonda, Tarafların, kovuşturulan cezai suçun niteliğinden bağımsız olarak, dijital ya da başka elektronik ortamlarda bulunan bilgilerin ceza davalarında delil olarak kullanılmasının mümkün olduğunu mevzuatlarına sokmak zorunda oldukları açıkça belirtilmiştir.

142. Bu uygulama kapsamı için iki istisnai durum mevcuttur. Birincisi, Madde 21'de içerik verilerine müdahale etme yetkisinin ulusal mevzuatın belirlediği bir dizi ciddi suçla sınırlı tutulacağı belirtilmiştir. Çoğu ülke, sesli iletişimin ve telekomünikasyonun gizliliğini ve bu soruşturma önleminin özel yaşama müdahale niteliğini göz önüne alarak, sesli iletişimle ve telekomünikasyona müdahale yetkisini bir dizi ciddi suçla sınırlı tutmuştur. Benzer şekilde, bu

Konvansiyon Tarafların, sadece ulusal mevzuatın belirlediği bir dizi ciddi suçla ilgili olarak belirlenen bilgisayar iletişiminin içerik verilerine ilişkin müdahale yetki ve usulleri tesis etmesini şart koşturmuştur.

143. İkincisi, Taraflar Madde 20'deki önlemleri (trafik verilerinin gerçek zamanlı olarak toplanması) uygulama haklarını, ancak hakkın saklı tutulmasıyla ilgili hükümde belirtilen suçlar ya da suç kategorileri için ve bu suç ya da kategori grubunun, Madde 21'de söz edilen müdahale önlemlerini uyguladığı suç grubundan daha sınırlı olmaması şartıyla saklı tutabilir. Bazı ülkeler trafik verilerinin toplanmasını gizlilik ve özel yaşama müdahale açısından içerik verilerinin toplanmasıyla eşdeğer olarak görmektedir. Hak saklı tutma hakkı bu ülkelerin trafik verilerini gerçek zamanlı olarak toplama önlemlerinin uygulamasını içerik verilerine gerçek zamanlı olarak müdahale yetki ve usullerini uyguladığı suç grubuyla sınırlı tutmalarını sağlayacaktır. Ancak birçok ülke, sadece trafik verilerinin toplanması iletişimin içeriğini toplama ve ifşa etmeye yol açmadığı için, içerik verilerine müdahale ile trafik verilerinin toplanmasını eşdeğer olarak

görmemektedir. Trafik verilerinin gerçek zamanlı olarak toplanması bilgisayar iletişimlerinin başlangıç ve varış noktalarını izlemekte (dolayısıyla suçluları teşhis etmekte) çok önemli olabildiği için, Konvansiyon, haklarını saklı tutmayı seçen Tarafları bu saklı tutmayı trafik verilerinin gerçek zamanlı olarak toplanması için sağlanan yetki ve usullerin en geniş uygulamasına izin verecek şekilde sınırlamaya davet etmektedir.

144. Paragraf (b)'de, Konvansiyonu benimsedikleri tarihte ulusal mevzuatlarında mevcut olan sınırlamalar yüzünden, belirli bir kullanıcı grubunun menfaatine işletilen, kamuya açık iletişim ağlarını kullanmayan ve diğer bilgisayar sistemleriyle bağlantılı olmayan bilgisayar sistemlerindeki iletişime müdahale edemeyen ülkelerin haklarını saklı tutmalarına izin verilmektedir. "Belirli bir kullanıcı grubu" terimiyle, örneğin şirketleri tarafından bir bilgisayar ağı aracılığıyla kendi aralarında iletişim kurmaları sağlanan çalışanlar gibi hizmet sağlayıcıyla bağlantıları açısından sınırlı bir grup kullanıcı kastedilmektedir. "Diğer bilgisayar sistemleriyle bağlantılı olmayan" terimi, Madde 20 ya da 21 çerçevesinde bir talimatın

çıkarıldığı tarihte, kendisine iletişimler iletilen bir sistemin başka bir bilgisayar ağıyla fiziksel ya da mantıksal bir bağlantısı olmaması anlamındadır. "Kamuya açık iletişim ağlarını kullanmayan" terimi, kullanımın kullanıcıların bilgisi dahilinde olup olmamasından bağımsız olarak, kamuya açık bilgisayar ağlarını (İnternet dahil), kamuya açık telefon ağlarını ve diğer kamuya açık telekomünikasyon imkanlarını kullanan sistemleri hariç bırakmaktadır.

Madde 15 - Şartlar ve Önlemler

145. Konvansiyonun bu Kısımında içerilen yetki ve usullerin tesis edilmesi, gerçekleştirilmesi ve uygulanması her bir Tarafın ulusal mevzuatındaki şart ve önlemlere tabi olacaktır. Taraflar belli usul hukuku hükümlerini ulusal mevzuatlarına sokmak zorunda olmakla birlikte, bu yetki ve usulleri hukuk sistemlerinde tesis etme ve gerçekleştirme tarzları ve yetki ve usullerin spesifik durumlara uygulanması, Tarafların ulusal yasalarına ve usullerine bırakılmıştır. Bu ulusal yasa ve usuller, aşağıda daha ayrıntılı olarak tanımlandığı gibi, anayasa, yasama, yargı yoluyla ya da başka bir biçimde sağlanan şart ve önlemleri içerecektir. Tarzlar,

yasaların icra edilme zorunluluğuyla insan hak ve özgürlükleri arasında denge kuran şart ve önlem şeklindeki belirli unsurların eklenmesini içermelidir. Konvansiyona Taraf olan ülkelerin çok farklı hukuk sistemlerine ve kültürlerine sahip olmasından dolayı, her bir yetki ve usul için geçerli olabilecek şart ve önlemleri ayrıntılarıyla açıklamak mümkün değildir. Taraflar, bu şart ve önlemlerin insan hak ve özgürlükleri için yeterli koruma getirmesini sağlayacaklardır. Konvansiyona Taraf olan ülkelerin sadık kalmak zorunda oldukları bazı ortak standartlar ya da minimum önlemler mevcuttur. Bunlar, Tarafların konuyla ilgili uluslararası insan hakları araçları çerçevesinde üstlendikleri yükümlülükler uyarınca ortaya çıkan standartları ve minimum önlemleri içermektedir. Bu araçlar arasında, Taraf olan Avrupa ülkeleri için, 1950 İnsan Haklarının ve Temel Özgürlüklerin Korunması için Avrupa Konvansiyonu ve 1, 4, 6, 7 ve 12. ek Protokolleri (ETS N° 005 (4), 009, 046, 114, 117 ve 177) bulunmaktadır. Ayrıca, dünyanın diğer bölgelerindeki bu araçlara Taraf olan ülkeler için, diğer geçerli insan hakları sözleşmeleri (örneğin 1969 Amerika İnsan

Hakları Konvansiyonu ve 1981 Afrika İnsanların ve Halkların Hakları Sözleşmesi) ile daha evrensel düzeyde kabul gören 1966 Uluslararası Medeni ve Siyasi Haklar Sözleşmesi de bunlar arasındadır. Ayrıca, çoğu ülkenin mevzuatında benzer korumalar mevcuttur.

146. Konvansiyondaki diğer bir önlem de yetki ve usullerin "hakkaniyet ilkesinin tesis edilmesini" sağlayacak olmasıdır. Hakkaniyet her bir Taraf Ülke tarafından ulusal mevzuatındaki ilgili ilkeler uyarınca uygulanacaktır. Avrupa ülkeleri için bu, yetki ve usullerin suçun niteliği ve koşulları açısından hakkaniyetli olmasını öngören 1950 Avrupa Konseyi İnsan Haklarının ve Temel Özgürlüklerin Korunması Konvansiyonu, ilgili hukuk sistemi ve ulusal mevzuat ve hukuk sistemleri çerçevesinde belirlenecektir. Diğer ülkeler ulusal mevzuatlarındaki, üretim talimatlarının aşırı kapsamlı olması üzerine sınırlamalar ve arama ve el koymalar için makul olma şartları gibi ilkeleri uygulayacaktır. Ayrıca, Madde 21'deki müdahale önlemleriyle ilgili zorunlulukların ulusal mevzuatın belirlediği bir dizi ciddi suçla ilişkili olması konusundaki açık sınırlama, hakkaniyet ilkesinin uygulanması için açık bir örnektir.

147. Konvansiyon, uygulanabilir şart ve önlem türlerini kısıtlamaksızın, bu şart ve önlemlerin, yetki ya da usulün niteliğine uygun olarak, adli ya da başka nitelikte bağımsız bir gözetimi, yetki ve usulün uygulanmasını ve bunların kapsamı ve süresiyle ilgili kısıtlamalar için gerekçeler içermesini özel olarak şart koşturmaktadır. Ulusal yasama organları, bağlayıcı uluslararası yükümlülükleri ve yerleşik ulusal ilkeleri uygularken, niteliği açısından hangi yetki ve usullerin özel şart ve önlemleri uygulamayı gerektirecek kadar özel hayata müdahale edici olduğuna karar vermek zorundadır. Paragraf 215'te belirtildiği gibi, Taraflar, özel hayata müdahale edici nitelikte olan iletişime müdahale konusunda bu gibi şart ve önlemleri açık bir biçimde uygulamalıdır. Aynı zamanda, örneğin, verilerin korunması konusunda bu tür önlemler aynı derecede uygulanmak zorunda değildir. Ulusal mevzuat çerçevesinde ele alınması gereken diğer önlemler arasında kendi aleyhine tanıklığa karşı hak, hukuki ayrıcalıklar ve önlemin uygulanmasının konusu olacak kişi ve mekanların belirliliği bulunmaktadır.

148. Paragraf 3'te tartışılan konularla ilgili olarak en önemli husus "kamu yararı", özellikle de

"adaletin sağlıklı şekilde yürütülmesi"nin göz önünde bulundurulmasıdır. Taraflar, kamu yararıyla tutarlı olduğu ölçüde, diğer etkenleri, örneğin yetki ve usullerin hizmet sağlayıcılar da dahil olmak üzere üçüncü şahısların "hak, sorumluluk ve meşru menfaatleri" üzerindeki, icra önlemlerinin sonucunda ortaya çıkan etkisini ve bu etkiyi hafifletmek için uygun yolların kullanılıp kullanılamayacağını değerlendireceklerdir. Özet olarak, adaletin sağlıklı şekilde yürütülmesi ve diğer kamusal menfaatlerle ilgili bir ilk değerlendirme yapılmaktadır (örneğin kamu güvenliği, kamu sağlığı ve kurbanların menfaatleri ve özel yaşama saygı da dahil olmak üzere diğer menfaatler). Kamu yararıyla tutarlı olduğu ölçüde, müşteri hizmetlerinin asgari düzeyde zarar görmesi, bu Bölüm çerçevesinde ifşa ya da ifşayı kolaylaştırma konusunda yükümlülükten korunma ya da mülkiyet haklarının korunması gibi konularda olağan değerlendirmeler yapılacaktır.

BAŞLIK - 2

***Saklanan Bilgisayar Verilerinin
Hızlı Bir Biçimde Korunması***

149. Madde 16 ve 17'deki önlemler, hizmet sağlayıcıları gibi veri saklayıcılar tarafından halihazırda toplanmış ve saklanmış veriler için geçerlidir. Bu önlemler, gelecekteki trafik verilerinin gerçek zamanlı olarak toplanması ve tutulması ya da iletişimlerin içeriğine gerçek zamanlı erişim için geçerli değildir. Bu konular Başlık 5'te ele alınmıştır.

150. Maddede belirtilen önlemler bilgisayar verilerinin halihazırda mevcut olduğu ve şu anda saklanmakta olduğu durumlarda işleyecektir. Birçok nedenle, cezai soruşturmalarla ilgili bilgisayar verileri artık mevcut olmayabilir ya da artık saklanmıyor olabilir. Örneğin, doğru veriler toplanmamış ve tutulmamış ya da toplandıysa bile saklanmamış olabilir. Veri koruma yasaları önemli verilerin ceza davaları için önemleri anlaşılmadan yok edilmesini müspet olarak şart koşmuş olabilir. Bazen, örneğin müşterilerin sabit bir fiyat ödediği ya da ücretsiz hizmetler söz konusu olduğunda verilerin toplanması ve tutulması için ticari bir neden olmayabilir.

Madde 16 ve 17'de bu sorunlar ele alınmamaktadır.

151. "Verileri korumak" ile "verileri tutmak" arasında ayırım yapılmalıdır. Bu terimler gündelik dilde benzer anlamda olmakla birlikte bilgisayarla ilgili olarak farklı anlamlara gelmektedir. Verileri korumak, halihazırda saklanmakta olan verilerin saklanmaya devam edilmesi, mevcut nitelik ya da durumunun değişmesine ya da bozulmasına neden olabilecek etkenlerden korunması anlamındadır. Verileri tutmak ise, halihazırda üretilmekte olan verilerin belli birinin mülkiyetinde gelecek için saklanması anlamına gelir. Verileri tutmak, verilerin şimdi biriktirildiğini ve bunların gelecekte tutulacağını ya da bulundurulacağını ifade eder. Verileri tutmak, verileri saklama sürecidir. Verileri korumak ise, saklanan verileri sağlam ve güvenlikte tutma faaliyetidir.

152. Madde 16 ve 17, verileri tutmakla değil korumakla ilgilidir. Bu maddeler bir hizmet sağlayıcının ya da başka bir kişi ya da kuruluşun faaliyetleri esnasında topladığı verilerin hepsinin, hatta bir kısmının toplanmasını ve tutulmasını emretmemektedir. Koruma önlemleri "bir

bilgisayar sistemi aracılığıyla saklanmış" bilgisayar verileri için geçerlidir; yani verilerin halihazırda mevcut olduğu, halihazırda toplanmış ve saklanmış olduğu varsayılmıştır. Ayrıca, Madde 14'te belirtildiği gibi, Konvansiyonun 2. Kısımında tesis edilmesi gereken bütün yetki ve usuller "spesifik cezai soruşturma ve takibatlar" içindir ve bu hüküm önlemlerin uygulanmasını belirli bir vakadaki soruşturmayla sınırlar. Ek olarak, Taraflar bir talimatla koruma önlemlerini yürürlüğe soktuğunda bu talimat "bir kişinin mülkiyetinde ya da kontrolünde bulunan belirli saklı bilgisayar verileri" (paragraf 2) ile ilişkilidir. Dolayısıyla Maddeler sadece spesifik cezai soruşturma ve takibatlar için mevcut saklı verilerin korunmasını şart koşma yetkisini vermekte, verilerin daha sonra başka yasal yetkiler uyarınca ifşasını askıda tutmaktadır.

153. Verilerin korunmasını sağlama zorunluluğuyla, Tarafların, meşru ticari faaliyetlerin bir parçası olarak trafik ya da abonelik verileri gibi bazı veri türlerini rutin bir biçimde toplayıp tutmayan hizmetlerin sunulmasını ve kullanılmasını sınırlamasını şart koşturmak amaçlanmamıştır. Tarafların örneğin sistemde bir talep ya da

talimata uygun olarak saklanması makul şartlarda mümkün olmayacak kadar kısa bir süre tutulan günlük verileri korumak için yeni teknik imkanlardan yararlanmaları da şart koşulmamaktadır.

154. Bazı Ülkelerde belirli türde saklayıcılar tarafından saklanan belirli türde verilerin, örneğin kişisel verilerin, tutulmaları için ticari bir neden yoksa tutulmamaları ve silinmeleri gerektiğini belirten yasalar mevcuttur. Avrupa Birliği'nde genel ilke 95/46/EC sayılı Direktifle ve telekomünikasyon sektörünün özel bağlamında geçerli ilkeler. 97/66/EC sayılı Direktifle uygulamaya geçirilmiştir. Bu direktiflerde verilerin saklanması gerekli olmaktan çıkar çıkmaz silinmesi zorunluluğu tesis edilmiştir. Ancak üye Ülkeler, cezai suçların önlenmesi, soruşturulması ve takibatı için gerekli olduğunda muafiyet yaratacak yasalar çıkarabilirler. Bu direktifler Avrupa Birliği'ne üye Ülkelerin ulusal mevzuatlarında spesifik soruşturmalar için belirli türde verileri korumaya yönelik yetki ve usuller tesis etmelerini engellememektedir.

155. Verileri korumak birçok ülkenin ulusal mevzuatı için yepyeni bir hukuki yetki ve usuldür. Bilgisayar suçlarını ve bilgisayarla bağlantılı suçları, özellikle de İnternet aracılığıyla işlenen suçları ele almak için yeni ve önemli bir soruşturma aracıdır. Birinci olarak, bilgisayar verilerinin geçiciliğinden dolayı veriler kolaylıkla manipölasyon ve değıştirmeye maruz kalabilmektedir. Dolayısıyla, özensiz işleme ve saklama uygulamaları, delilleri yok etmeye yönelik kasıtlı manipölasyon ve silme ya da artık tutulması gerekmeyen verilerin rutin olarak silinmesi sonucunda bir suçla ilgili değıerli deliller kolaylıkla yok olabilmektedir. Yetkili merciler için verilerin bütünlüğünü korumanın bir yöntemi, verileri aramak ya da benzer şekilde erişmek ve el koymak ya da benzer şekilde güven altına almaktır. Ancak verileri saygın bir işletme gibi güvenilir bir kuruluşun koruduğı durumlarda verilerin bütünlüğü bunları korumaya yönelik bir talimat yoluyla daha hızlı bir şekilde gerçekleştirilebilir. Ayrıca, koruma talimatı, meşru işletmelerin normal faaliyetleri ve saygınlıkları açısından, işyerinde arama ve el koyma işleminin yapılmasından daha az zarar vericidir. İkincisi, bilgisayar suçları ve bilgisayarla

bağlantılı suçlar büyük ölçüde iletişimlerin bilgisayar sistemi aracılığıyla iletilmesi sonucunda gerçekleştirilmektedir. Bu iletişimler, çocuk pornografisi, bilgisayar virüsü ya da verilere ya da bilgisayar sisteminin gerektiği gibi işlemesine müdahaleye yol açabilecek başka talimatlar gibi yasadışı bir içeriğe sahip olabilirler ya da uyuşturucu kaçakçılığı ya da sahtekarlık gibi başka suçlarla ilgili deliller içerebilirler. Geçmişteki bu tür iletişimlerin kaynağını ve varış noktasını belirlemek faillerin kimliğini tespit etmeye yardım edebilir. Kaynaklarını ve varış noktalarını belirlemek üzere bu iletişimleri izlemek için bu iletişimlerle ilgili trafik verileri gerekmektedir (trafik verilerinin önemiyle ilgili daha ayrıntılı açıklama için aşağıdaki Madde 17'ye bkz.). Üçüncüsü, bu iletişimlerin yasadışı içerik ya da suç niteliğindeki faaliyetlerle ilgili delil içerdiği ve kopyalarının hizmet sağlayıcılar tarafından tutulduğu durumlarda -örneğin e-posta- kritik delillerin kaybolmaması açısından iletişimlerin korunması önemlidir. Geçmişteki bu iletişimlerin kopyalarının elde edilmesi (örneğin gönderilmiş ya da alınmış olan saklı e-postalar) suçluluk delillerini ortaya çıkarabilir.

156. Bilgisayar verilerinin hızlı bir biçimde korunması yetkisi bu sorunları çözmeye yöneliktir. Bu nedenle, geçici bir önlem olarak, Tarafların belirlenen bilgisayar verilerini koruma talimatı verme yetkisi getirmeleri şart koşulmaktadır. Böylece veriler, en fazla 90 gün olmak üzere, gerekli olduğu sürece korunacaktır. Taraflar daha sonra talimatın yenilenmesini sağlayabilir. Bu, koruma döneminde verilerin icra mercilerine ifşa edileceği anlamına gelmemektedir. Bunun yapılabilmesi için ilave bir ifşa önlemi ya da arama talimatı verilmelidir. Korunan verilerin icra mercilerine ifşasıyla ilgili olarak bkz. paragraf 152 ve 160.

157. Tarafların kendi sınırları içinde bulunan saklı verilerin hızlı bir biçimde korunması konusunda uluslararası düzeyde birbirlerine yardım edebilmeleri için ulusal düzeyde koruma önlemlerinin varolması da önemlidir. Bu, talebin yapıldığı Taraf Ülkenin verileri elde etmesini ve Talebi yapan Taraf Ülkeye ifşa etmesini sağlayan genellikle vakit alıcı geleneksel karşılıklı hukuki yardım prosedürleri esnasında kritik önemdeki verilerin kaybedilmesini önlemeye yardımcı olacaktır.

**Madde 16 - Saklanan Bilgisayar Verilerinin
Hızlı Bir Biçimde Korunması**

158. Madde 16'da ulusal yetkili mercilerin, spesifik bir cezai soruşturma ya da takibatla bağlantılı belirli saklı bilgisayar verilerinin hızlı bir biçimde korunması yönünde talimat vermelerini ya da bunu benzer bir şekilde temin etmelerini sağlamak amaçlanmaktadır.

159. "Koruma", halihazırda saklanmakta olan verilerin mevcut nitelik ya da durumlarının değişmesi ya da bozulmasına yol açacak herhangi bir etkenden korunması anlamındadır. Korumayla verilerin değiştirilme, bozulma ya da silinmeden korunması amaçlanmaktadır. Koruma zorunlu olarak verilerin "dondurulması" (yani erişilmez hale getirilmesi) ve bunların ya da kopyalarının meşru kullanıcılar tarafından kullanılamaması anlamına gelmez. Talimatın yapıldığı kişi, talimatın tam niteliklerine bağlı olarak, verilere erişmeye devam edebilir. Maddede verilerin nasıl korunması gerektiği spesifik biçimde belirtilmemektedir. Uygun koruma yöntemini ve, uygun olduğu bazı durumlarda, verilerin korunmasının "dondurulmalarını" gerektirip

gerektirmediğini belirlemek Taraflara bırakılmıştır.

160. "Talimat vermek ya da bunu benzer bir şekilde temin etmek" ifadesiyle koruma sağlamak için adli ya da idari talimat ya da direktiflerin (örneğin polis ya da savcıdan) yanı sıra diğer yasal yöntemlerin kullanımına da izin vermek amaçlanmıştır. Bazı ülkelerde usul hukukunda koruma talimatları bulunmamaktadır ve veriler ancak arama ve el koyma ya da üretim talimatıyla korunabilmekte ve temin edilebilmektedir. "Ya da bunu benzer bir şekilde temin etmek" ifadesiyle esneklik sağlanması ve bu ülkelerin bu yöntemleri kullanarak bu Maddeyi uygulamalarına izin verilmesi amaçlanmıştır. Ancak, talimatın verildiği kişinin hızlı hareket etmesi belirli durumlarda koruma önlemlerinin daha hızlı uygulanmasını sağlayabildiği için, ülkelerin talimatın verildiği kişiye gerçekten verileri saklama talimatı verilmesini sağlayacak yetki ve usulleri tesis etmeyi değerlendirmeleri tavsiye edilmektedir.

161. Belirli bilgisayar verilerinin hızlı bir biçimde korunması yönünde talimat verme ya da bunu benzer bir şekilde temin etme yetkisi her tür

saklı bilgisayar verisine uygulanabilir. Bu yetki, talimatta korunması gerektiği belirtilen her tür veriyi içerebilir. Örneğin, işle, sağlıkla ilgili, kişisel ya da başka tür kayıtları içerebilir. Önlemler, Taraf Ülkeler tarafından "özellikle bilgisayar verilerinin kaybedilmesinin ya da değiştirilmesinin söz konusu olabileceğine dair gerekçelerin mevcut bulunduğu durumlarda" kullanılmak üzere tesis edilecektir. Buna verilerin kısa süreli olarak tutulduğu, örneğin belli bir süre sonunda silinmelerinin şirket politikası olduğu ya da saklama ortamının başka verilerin kaydedilmesi için olağan olarak silindiği durumlar dahildir. Verilerin koruyucusunun niteliği ya da verilerin güvenli olmayan biçimde saklanması da söz konusu olabilir. Ancak, koruyucu güvenilir değilse, korumayı uyulması muhtemel olmayan bir talimat yerine arama ve el koyma yöntemiyle gerçekleştirmek daha güvenlidir. Özellikle "trafik verileri"ne uygulanabilir hükümleri vurgulamak için, hizmet sağlayıcı tarafından toplanır ve tutulursa genellikle sadece kısa bir süre için tutulan bu verilerden paragraf I'de özel olarak söz edilmiştir. "Trafik verileri"nden söz edilmesi aynı

zamanda Madde 16 ve 17'deki önlemler arasında bir bağlantı oluşturmaktadır.

162. Paragraf 2'de Tarafların korumayı bir talimat yoluyla yürürlüğe sokması durumunda, koruma talimatının "bir kişinin mülkiyetinde ya da kontrolünde bulunan belirli saklı bilgisayar verileri" ile ilgili olacağı belirtilmiştir. Dolayısıyla saklı veriler gerçekten bir kişinin mülkiyetinde bulunabilir ya da başka bir yerde saklı olmasına karşın bu kişinin kontrolüne tabi olabilir. Talimatı alan kişi "yetkili mercilerin bu bilgisayar verilerinin ifşasını isteyebilmesini sağlamak üzere bu verilerin doğruluğunu, azami 90 gün olmak üzere, gereken süre boyunca korumak ve saklamak" zorundadır. Taraf Ülkenin ulusal mevzuatında verilerin bir talimata tabi olarak korunmak zorunda olduğu azami süre, talimatta ise belirlenen verilerin saklanmak zorunda olduğu kesin süre belirtilmelidir. Süre, azami 90 gün olmak üzere, yetkili mercilerin verilerin ifşasını temin etmek için arama ve el koyma ya da benzer şekilde erişim ve güven altına alma ya da bir üretim talimatı çıkarma gibi başka hukuki önlemleri almasına yetecek kadar uzun olmalıdır. Taraflar daha sonra üretim talimatının yenilenmesini isteyebilir. Bu bağlamda, bir

bilgisayar sistemi yoluyla saklanan verilerin hızlı bir biçimde korunmasını temin etmek üzere, yardımlaşma talebinde bulunmakla ilgili Madde 29'a gönderme yapılmalıdır. Bu Madde uyarınca yardımlaşma talebine cevaben yürürlüğe sokulan koruma işlemi "en az 60 gün sürecek, bu suretle talepte bulunan Tarafın verilerin aranması ya da benzer şekilde bu verilere erişim sağlanması, verilere el konulması ya da benzer şekilde güven altında tutulması ya da ifşa edilmesi amacıyla talepte bulunabilmesi sağlanacaktır."

163. Paragraf 3'te, ulusal mevzuatta belirtilecek bir süre için, korunacak verilerin koruyucusuna ya da verileri koruma talimatı alan kişiye, koruma usullerini yerine getirmekle ilgili bir gizlilik yükümlülüğü getirilmektedir. Bu, Tarafların saklanan verilerin hızlı bir biçimde korunmasıyla ilgili gizlilik önlemleri ve gizlilik dönemiyle ilgili bir zaman limiti getirmelerini şart koşar. Bu önlem icra mercilerinin soruşturmanın şüphelisinin soruşturmadan haberdar olmaması ihtiyacını ve bireylerin gizlilik ihtiyacını karşılamaktadır. İcra mercileri için verilerin hızlı bir biçimde korunması başlangıç soruşturmalarının bir parçasını teşkil eder; ve bu nedenle bu aşamada gizlilik önemli olabilir.

Koruma, verileri elde etme ya da ifşa için başka hukuki önlemler alınmasını askıya alan bir hazırlayıcı önlemdir. Başka kişilerin verileri tahrif etmeye ve silmeye kalkışmaması için gizlilik gereklidir. Talimatın verildiği kişi, verilerin konusu ya da verilerde adı geçen ya da kimliği belirtilen başka kişiler için önlemin uzunluğunu belirleyen açık bir zaman sınırı olmalıdır. Verileri sağlam ve güvende tutmak ve koruma önleminin alınmış olduğunu gizli tutmak şeklindeki ikili zorunluluk, verilerin konusunun ya da verilerde adı geçen ya da kimliği belirtilen başka kişilerin gizliliğini korumaya yardımcı olur.

164. Yukarıda belirtilen sınırlamalara ek olarak, Madde 16'da söz edilen yetki ve usuller Madde 14 ve 15'te belirtilen şartlara ve önlemlere de tabidir.

Madde 17 - Trafik Verilerinin Hızlı Bir Biçimde Korunması ve Kısmen İfşası

165. Bu Maddede Madde 16 çerçevesinde trafik verilerinin korunmasıyla ilgili spesifik zorunluluklar tesis edilmekte ve belirli iletişimlerin iletilmesine diğer hizmet sağlayıcıların da katıldığını belirlemek için bazı trafik verilerinin hızlı bir biçimde ifşası

sağlanmaktadır. "Trafik verileri" Madde 1'de tanımlanmıştır.

166. Geçmişteki iletişimlerle ilişkili saklı trafik verilerinin elde edilmesi geçmişteki bir iletişimin kaynağını ya da varış noktasını belirlemek açısından kritik önemde olabilir. Bu bilgiler, örneğin, çocuk pornografisi dağıtan, bir sahtekarlık eyleminin parçası olarak yalan beyanlar dağıtan, bilgisayar virüsleri dağıtan, bilgisayar sistemlerine yasadışı olarak erişmeye teşebbüs eden ya da bunu başaran ya da bir bilgisayar sistemine sistemdeki verilere ya da sistemin uygun biçimde işleyişine müdahale eden iletişimler ileten kişileri saptamak açısından büyük önem taşımaktadır. Ancak, bu tür verilerin uzun süreli olarak saklanması gizliliği korumak için hazırlanmış yasalarca yasaklandığı ya da piyasa güçleri tarafından teşvik edilmediği için bu veriler genellikle ancak kısa bir süre için saklanmaktadır. Dolayısıyla, bu verilerin bütünlüğünü sağlamak için koruma önlemlerinin alınması büyük önem taşımaktadır (yukarıdaki korumayla ilgili tartışmaya bakınız).

167. Çoğu zaman bir iletişimin iletilmesine birden fazla hizmet sağlayıcı katılabilir. Her bir hizmet sağlayıcı, bu iletişimin iletilmesiyle ilgili,

iletişimin kendi sisteminden geçişi üzerine kendi ürettiği ve tuttuğu ya da diğer hizmet sağlayıcılardan aldığı bazı trafik verilerine sahip olabilir. Bazen trafik verileri, ya da en azından trafik verilerinin bazı türleri, ticari, güvenlikle ilgili ya da teknik amaçlarla, iletişimin iletilmesine katılan hizmet sağlayıcılar arasında paylaşılır. Böyle bir durumda, iletişimin kaynağını ve varış noktasını belirlemek için gereken kritik trafik verileri hizmet sağlayıcılardan herhangi birinin elinde bulunabilir. Ancak, çoğu zaman, hiçbir hizmet sağlayıcı iletişimin gerçek kaynağını ya da varış noktasını belirlemeye yetecek miktarda kritik trafik verisine tak başına sahip değildir. Her bir hizmet sağlayıcı bütünün bir parçasına sahiptir ve kaynak ve varış noktasını belirlemek için bu parçaların her biri incelenmelidir.

168. Madde 17, bir iletişimin iletilmesine bir ya da birden fazla hizmet sağlayıcının katıldığı durumlarda bütün hizmet sağlayıcılar arasında trafik verilerinin hızlı bir biçimde korunmasını sağlamaktadır. Maddede bunun başarılmasını sağlayacak yollar belirtilmemekte, hukuk ve ekonomi sistemiyle tutarlı bir yol belirlemek ulusal mevzuata bırakılmaktadır. Yetkili merciler

için hızlı bir biçimde korumayı sağlamanın bir yolu her bir hizmet sağlayıcıya ayrı bir koruma talimatı tebliğ etmektir. Ancak, ayrı ayrı bir dizi talimatın temin edilmesi gereksiz zaman kaybına yol açabilir. Tercih edilen alternatif yöntem, kapsamı spesifik iletişimin iletimine katıldıkları saptanan bütün hizmet sağlayıcılar için geçerli olacak tek bir talimat temin etmektir. Bu kapsamlı talimat, sırayla, saptanan bütün hizmet sağlayıcılara tebliğ edilebilir. Diğer olası alternatifler hizmet sağlayıcıların katılımını içerebilir. Örneğin, kendisine talimat tebliğ edilen bir hizmet sağlayıcının zincirdeki bir sonraki hizmet sağlayıcıya koruma talimatının varlığını ve hükümlerini bildirmesi şart koşulabilir. Bu bildirim, ulusal mevzuata bağlı olarak, ya diğer hizmet sağlayıcının ilgili trafik verilerini gönüllü olarak korumasına izin vererek verilerin silinmesiyle ilgili bir zorunluluk içermeyecek, ya da ilgili trafik verilerinin korunmasını zorunlu kılacaktır. İkinci hizmet sağlayıcı da benzer bir biçimde zincirde bir sonra yer alan hizmet sağlayıcıya bildirimde bulunabilir.

169. Bir koruma talimatının bir hizmet sağlayıcıya tebliğinde trafik verileri icra mercilerine ifşa

edilmediği (ancak daha sonra, başka hukuki önlemlerin alınmasıyla temin ya da ifşa edildiği) için, bu merciler hizmet sağlayıcının bütün kritik trafik verilerine sahip olup olmadığını ve iletişimin iletildiği zincirde başka hizmet sağlayıcıların bulunup bulunmadığını bilemeyecektir. Bu nedenle, bu Maddede, koruma talimatı ya da benzer bir önlemin tebliğ edildiği hizmet sağlayıcının, yetkili mercilere ya da bu mercilerin belirlediği bir kişiye, yetkili mercinin söz konusu hizmet sağlayıcıları ve iletişimin iletildiği yolu belirleyebilmesine yetecek kadar trafik verisini hızlı bir biçimde ifşa etmesi şart koşulmuştur. Yetkili merciler ifşa edilmesi gereken trafik verisi türünü açıkça belirtmelidir. Bu bilgilerin alınması, yetkili mercilerin başka hizmet sağlayıcılar için koruma önlemi alıp almama konusunda karar vermesini sağlayacaktır. Bu yolla, soruşturmayı yürüten merciler iletişimi geriye doğru kaynağına, ileriye doğru varış noktasına kadar izleyebilecek ve soruşturulmakta olan spesifik suçun fail ya da faillerini belirleyebilecektir. Bu Maddedeki önlemler, Madde 14 ve 15'te belirtilen sınırlama, şart ve önlemlere de tabidir.

BAŞLIK - 3
Üretim Talimatı

Madde 18 - Üretim Talimatı

170. Bu Maddenin 1. paragrafında Taraflardan yetkili mercilerinin kendi sınırları içinde bir kişiyi belirli saklı bilgisayar verilerini açıklamaya ya da kendi sınırları içinde hizmetlerini sunan bir hizmet sağlayıcıyı abonelik bilgilerini teslim etmeye zorlayabilmesini sağlamaları istenmektedir. Söz konusu veriler saklanan ve halihazırda mevcut olan verilerdir ve gelecekteki iletişimlerle ilgili trafik verileri ya da içerik verileri gibi henüz mevcut olmayan verileri içermemektedir. Ülkelerin üçüncü şahıslarla ilgili, verilerin aranması ve bu verilere el konulması gibi, sistematik cebri önlemler uygulamak yerine ulusal mevzuatları çerçevesinde cezai soruşturmalarla ilgili bilgileri temin etmek için daha az müdahaleci yöntemler sağlayan alternatif soruşturma yetkilerine sahip olmaları temel önemdedir.

171. "Üretim talimatı", icra mercilerinin birçok durumda, özellikle daha müdahaleci ya da külfetli önlemler yerine kullanabileceği daha

esnek bir önlem sağlamaktadır. Bu tür bir usul mekanizmasının kullanılması, genellikle kontrollerindeki verileri vererek icra mercilerine gönüllü olarak yardım etmeye hazır olan, ama sözleşmelerden ya da başka nedenlerden doğan herhangi bir yükümlülükten kurtulmak için böyle bir yardımın hukuki bir temeli olmasını tercih eden hizmet sağlayıcıları gibi üçüncü şahıs veri koruyucuları açısından da yararlıdır.

172. Üretim talimatı bir kişi ya da hizmet sağlayıcının mülkiyetinde olan bilgisayar verileri ve abonelik bilgileriyle ilgilidir. Önlem sadece kişi ya da hizmet sağlayıcının bu veri ya da bilgileri tuttuğu durumlar için geçerlidir. Örneğin bazı hizmet sağlayıcılar hizmetlerinin aboneleriyle ilgili kayıt tutmamaktadır.

173. Paragraf 1(a) uyarınca Taraflar, yetkili icra mercilerinin, sınırları içindeki bir kişiye, bu kişinin mülkiyetinde ya da kontrolünde bulunan bir bilgisayar sisteminde ya da veri saklama ortamında saklanan belirli bilgisayar verilerini vermesi yönünde talimat verme yetkisine sahip olmalarını sağlayacaklardır. "Mülkiyetinde ya da kontrolünde" terimi, verilerin talimatı veren Taraf Ülkenin sınırları içinde fiziksel mülkiyet

dahilinde bulunmasını, veya üretilecek verilerin söz konusu kişinin fiziksel mülkiyeti dışında olduğu ama kişinin yine de talimatı veren Taraf Ülkenin sınırları içinden verilerin üretimini serbestçe kontrol edebildiği durumları ifade etmektedir (örneğin, uygulanabilir ayrıcalıklara tabi olmak üzere, kendisine uzaktaki bir online saklama hizmeti yoluyla hesabında sakladığı bilgiler için bir üretim talimatı tebliğ edilen bir kişi bu bilgileri üretmek zorundadır). Aynı zamanda, uzakta saklanan verilere teknik erişebilirlik (örneğin bir kullanıcının bir ağ bağlantısıyla uzakta saklanan, kendi meşru kontrolünde olmayan verilere erişebilmesi) tek başına bu hükümde kastedilen anlamıyla "kontrol" oluşturmayabilir. Bazı ülkelerde mevzuatta "mülkiyet" olarak adlandırılan kavram, bu "mülkiyet ve kontrol" şartını karşılayacak kadar geniş kapsamlı olarak fiziksel ve kanunen varsayılan mülkiyeti kapsamaktadır.

Paragraf 1(b) uyarınca Taraflar hizmetlerini sınırları dahilinde sunan bir hizmet sağlayıcıya da "mülkiyetinde ya da kontrolünde bulunan abonelik bilgilerini verme" talimatı verme yetkisi sağlayacaklardır. Paragraf 1(a)'da olduğu gibi "mülkiyetinde ya da kontrolünde" ifadesiyle

hizmet sağlayıcının fiziksel mülkiyetinde olan ya da uzakta saklanmakta olup hizmet sağlayıcının kontrolünde bulunan abonelik bilgileri kastedilmektedir (örneğin başka bir şirketin sağladığı uzaktaki bir veri saklama imkanı). "Söz konusu hizmetlere ilişkin" ifadesi, yetkinin, talimatı veren Taraf Ülkenin sınırları içinde sunulan hizmetlerle ilgili abonelik bilgilerinin temin edilmesi amacıyla verileceği anlamına gelmektedir.

174. Maddenin 2. paragrafında sözü edilen şart ve önlemler, her bir Taraf Ülkenin ulusal mevzuatına bağlı olarak, ayrıcalıklı veri ya da bilgileri hariç bırakabilir. Taraflar belli kişi ya da hizmet sağlayıcı kategorilerinin tuttuğu belli türde bilgisayar verisi ya da abonelik bilgisinin verilmesi için farklı hükümler, farklı yetkili merciler ve farklı önlemler belirlemek isteyebilir. Örneğin, kamuya açık abonelik bilgileri gibi bazı tür veriler için, Taraflar icra mercilerinin normalde mahkeme emrini gerektirebilecek durumlarda böyle bir talimat çıkarmalarına izin verebilir. Diğer taraftan, bazı durumlarda Taraflar belli veri türlerini temin etmeye yönelik üretim talimatının sadece adli merciler tarafından çıkarılmasını şart koşabilirler ya da

insan hakları önlemleri onları bunu şart koşmaya zorlayabilir. Taraflar, icrayla ilgili nedenlerden dolayı, bu verilerin ifşasını bu bilgilerin ifşasına yönelik adli mercilerin bir üretim talimatı çıkardığı durumlarla sınırlamayı tercih edebilir. Hakkaniyet ilkesi önlemin uygulanmasıyla ilgili olarak da bir parça esneklik sağlamakta; örneğin birçok ülkede önemsiz vakalarda önlem uygulanmamaktadır.

175. Taraflar için değerlendirilecek diğer bir husus gizlilikle ilgili önlemleri dahil etme ihtimalidir. Üretim talimatlarında genellikle gizlilik zorunluluğunun getirilmediği elektronik olmayan dünyayla kurulan paralelliği sürdürmek için hükümde gizlilikten özel olarak bahsedilmemiştir. Ancak, elektronik, özellikle de online dünyada bir üretim talimatı bazen soruşturmada hazırlayıcı bir önlem olarak kullanılıp, daha sonra arama ve el koyma ya da diğer verilere gerçek zamanlı müdahale gibi farklı önlemlere başvurulabilir. Soruşturmanın başarısı için gizlilik temel önemde olabilir.

176. Üretimin tarzı açısından, Taraflar belirli bilgisayar verileri ya da abonelik bilgilerinin talimatta belirtilen biçimde üretilmesi için

sitesi adresi ya da alan adı, e-posta adresi vs.) rezervasyonunun yanı sıra abonenin kullandığı telefon cihazları, çağrı merkezleri ya da LAN'lar (yerel ağ) gibi iletişim teçhizatının sağlanması ve kaydedilmesini içermektedir.

180. Abonelik bilgileri iletişim hizmetinin kullanımıyla doğrudan bağlantılı bilgilerle sınırlı değildir. Aynı zamanda, trafik verileri ya da içerik verileri dışında, kullanıcının kimliğinin, posta adresi ya da bulunduğu yerin adresinin, telefon ve diğer erişim numaralarının, faturalama ve ödeme bilgilerinin saptanmasına yardım eden, aboneyle hizmet sağlayıcı arasındaki hizmet sözleşmesi ya da düzenlemesi esas alınarak elde edilebilen her türlü bilgiyi de içine almaktadır. Ayrıca, trafik verileri ya da içerik verileri dışında, iletişim teçhizatının kurulu olduğu bölge ya da yerle ilgili, hizmet sözleşmesi ya da düzenlemesi esas alınarak elde edilebilen her türlü bilgi de buna dahildir. Bu son bilgi pratik açıdan ancak teçhizatın taşınabilir olmadığı durumlarda önemli olabilir, ancak teçhizatın taşınabilirliği ya da bulunduğu iddia edilen yer (hizmet sözleşmesi ya da düzenlemesine göre elde edilen bilgi esas alınarak) soruşturma için yararlı olabilir.

181. Ancak bu Maddenin hizmet sağlayıcılara abonelerinin kayıtlarını saklama zorunluluğu getirdiği ya da hizmet sağlayıcıların bu bilgilerin doğruluğu için güvence vermelerini şart koştuğu düşünülmemelidir. Dolayısıyla, bir hizmet sağlayıcı önceden ödemeli cep telefonu hizmetleri kartlarının kullanıcılarının kimlik bilgilerini kaydetmek zorunda değildir. Abonelerinin kimliğini doğrulamak ya da hizmetlerin kullanıcılarının takma isim kullanmasına karşı direnmek zorunluluğu da yoktur.

182. Bu Kısımdeki yetki ve usullerde spesifik cezai soruşturma ve takibatlar amaçlandığı için (Madde 14), üretim talimatları, genellikle, belirli abonelerle ilgili tek tek vakalarda kullanılır. Örneğin, üretim talimatında geçen belli bir isim esas alınarak bağlantılı bir telefon numarası ya da e-posta adresi istenebilir. Belli bir telefon numarası ya da e-posta adresi esas alınarak ilgili abonenin isim ve adresi talep edilebilir. Hüküm, Taraflara, hizmet sağlayıcının, örneğin veri madenciliği amacıyla, abone grupları hakkında gelişigüzel miktarlarda abonelik bilgisi ifşa etmesi yönünde hukuki talimatlar çıkarma yetkisi vermemektedir.

kaydedilmiş delillerin toplanmasından oluşur. Soruşturmayı yürütenler bu tür kayıtlı verileri arar ve inceler, ve maddi kayıtlara el koyar ya da bunları fiziksel olarak alıp götürürler. Verilerin toplanması arama döneminde ve o sırada mevcut olan verilerle ilgili olarak gerçekleşir. Ulusal yasalar ve insan hakları önlemlerinde öngörüldüğü gibi, arama gerçekleştirmek için yasal yetki almanın ön koşulu belli bir yerde verilerin varolduğuna ve spesifik bir cezai suça delil teşkil edeceğine inanmak için gerekçelerin bulunmasıdır.

186. Yeni teknoloji ortamında, özellikle de bilgisayar verileriyle ilgili olarak, delil bulma amacıyla yapılan aramalarda da geleneksel aramanın birçok özelliği bulunmaktadır. Örneğin, verilerin toplanması arama esnasında ve o sırada mevcut olan verilerle ilgili olarak gerçekleştirilir. Arama yapmak için yasal yetki temin etme ön koşulu da değişmemektedir. Arama için yasal yetki almak için gereken inanç derecesi, verinin maddi ya da elektronik biçimde olmasına göre farklılık göstermez. Aynı şekilde, inanç ve arama halihazırda mevcut olan ve spesifik bir suça delil teşkil edecek verilerle ilgilidir.

187. Ancak, bilgisayar verileri söz konusu olduğunda, bilgisayar verilerinin maddi bir veri taşıyıcısının aranması ve bu taşıyıcıya el konması kadar etkin bir biçimde temin edilebilmesini sağlamak için ilave usul hükümleri gereklidir. Bunun için çeşitli nedenler mevcuttur: Birincisi veriler maddi biçimde değil, elektromanyetik ortamdadır. İkincisi, veriler bilgisayar teçhizatı yardımıyla okunabilir olmakla birlikte, kağıt üzerindeki bir kayıt gibi verilere el konamaz ve bunlar alıp götürülemez. Maddi olmayan verilerin üzerinde saklandığı fiziksel ortama (örneğin bilgisayar sabit diski ya da disket) el konmalı ve bu ortam götürülmeli, ya da verileri içeren maddi bir ortama el konması ve bu ortamın götürülmesi için verilerin maddi (örneğin bilgisayar yazıcısı çıktısı) ya da fiziksel bir ortam (örneğin disket) üzerine maddi olmayan bir kopyası üretilmelidir. Verilerin kopyasının çıkarıldığı son iki durumda, verilerin bir kopyası bilgisayar sisteminde ya da saklama cihazında kalmaktadır. Ulusal mevzuat bu kopyaları üretmek için yetki veriyor olmalıdır. Üçüncüsü, bilgisayar sistemlerinin birbirlerine bağlanabilme özelliklerinden dolayı veriler doğrudan aramanın yapıldığı bilgisayarda değil, ama o sistemden kolayca erişilebilecek bir

1. The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that proper record-keeping is essential for the transparency and accountability of the organization. This section also outlines the various methods used to collect and analyze data, ensuring that the information is reliable and up-to-date.

2. The second part of the document focuses on the implementation of the proposed changes. It details the steps involved in the transition process, from the initial planning phase to the final execution. This section also addresses the potential challenges that may arise during the implementation and provides strategies to overcome them.

3. The third part of the document discusses the impact of the proposed changes on the organization's overall performance. It highlights the expected benefits, such as increased efficiency and cost savings, and provides a detailed analysis of the potential risks. This section also includes a comparison of the current state of the organization with the proposed changes, showing the expected improvements.

4. The fourth part of the document provides a summary of the key findings and conclusions. It reiterates the importance of the proposed changes and the need for continued monitoring and evaluation. This section also includes a list of recommendations for future actions, ensuring that the organization remains committed to the principles of transparency and accountability.

5. The fifth part of the document is a conclusion, summarizing the main points of the document and expressing the author's confidence in the proposed changes. It also includes a statement of the author's commitment to the organization's success and a final note of appreciation for the support and cooperation of all stakeholders.

saklı bilgisayar verisi olarak mı yoksa aktarım halindeki veri olarak mı değerlendirilmesi gerektiği sorusu ortaya çıkmaktadır. Bazı Taraf Ülkelerin mevzuatında bu e-posta mesajları iletişimin bir parçasıdır ve dolayısıyla içerikleri ancak müdahale yetkisini uygulayarak temin edilebilir. Bazı hukuk sistemlerinde ise bu mesajlar Madde 19'un kapsamına giren saklı veriler olarak görülür. Bu nedenle, Taraflar hangisinin kendi ulusal hukuk sistemlerine uygun olduğunu belirlemek için yasalarını incelemelidir.

191. "Arama ya da benzer şekilde erişim" ifadesi kullanılmıştır. Geleneksel "arama" kelimesinin kullanımı, Devlet tarafından cebri yetkilerin kullanılması fikrine işaret etmekte ve bu Maddede söz edilen yetkinin geleneksel aramaya karşılık düştüğünü göstermektedir. "Arama", verileri bulmaya çalışma, okuma, denetleme ve inceleme anlamındadır. Veriyi arama ve araştırma (inceleme) kavramlarını içine almaktadır. Diğer taraftan "erişim" kelimesi, bilgisayar terminolojisini daha iyi yansıtan, belli bir yargı bildirmeyen bir kelimedir. Geleneksel kavramlarla modern terminolojiyi uzlaştırmak için her iki terim birlikte kullanılmıştır.

192. "Sınırları içinde" ifadesi, bu hükümde, bu Kısımdeki bütün Maddelerde olduğu gibi, sadece ulusal düzeyde alınması gerekli olan önlemlerin ele alındığını hatırlatmak için kullanılmıştır.
193. Paragraf 2'de, soruşturmayı yürüten mercilerin, gerekli verilerin başka bir bilgisayar sisteminde olduğuna inanmak için yeterli gerekçelerin varolduğu durumlarda, arama ya da benzer şekilde erişimlerini bu bilgisayar sistemini ya da onun bir parçasını içine alacak şekilde genişletmelerine izin verilmektedir. Ancak diğer bilgisayar sistemi ya da onun parçası Taraf Ülkenin "ulusal sınırları içinde" bulunmalıdır.
194. Konvansiyonda bir aramanın genişletilmesine nasıl izin verileceği ve bunun nasıl gerçekleştirileceği belirtilmemektedir. Bu husus ulusal yasalara bırakılmıştır. Örnek ihtimaller şunlardır: Spesifik bir bilgisayar sisteminin aranmasına yetki vermiş adli ya da başka tür merciye, aranan spesifik verilerin bağlantılı bilgisayar sisteminde bulunuyor. olabileceğine inanmak için yeterli gerekçe (ulusal mevzuat ve insan hakları önlemlerinin şart koştuğu dereceye kadar) mevcutsa, aramanın ya da benzer şekilde

1. The first step in the process is to identify the problem or issue that needs to be addressed. This involves gathering information and understanding the context of the problem.

2. Once the problem is identified, the next step is to define the objectives and goals of the project. This helps to clarify what needs to be achieved and provides a clear direction for the work.

3. The third step is to develop a plan or strategy to address the problem. This involves breaking down the problem into smaller, manageable tasks and determining the resources and timeline needed to complete them.

4. The fourth step is to implement the plan. This involves putting the strategy into action and monitoring progress to ensure that the project is on track.

5. The final step is to evaluate the results of the project. This involves assessing the outcomes against the objectives and goals and identifying any lessons learned for future projects.

STIGER RELIGIOUS
JEWELRY PARLOR

durumdaki maddi olmayan verilerle ilgili olduğu için yetkili mercilerin verileri güven altına alması için, kopyalanan ya da taşınan verilerin el koyma anında bulundukları durumda tutulmaları ve cezai takibatlar sırasında değişmemiş durumda kalmaları anlamına gelen "verilerin bütünlüğünün korunması" ya da verilerin "koruyuculuk zincirinin" korunması gibi ek önlemler gereklidir. Terim verilerin kontrolünü ele geçirmeyi ya da verileri alıp götürmeyi ifade etmektedir.

198. Verileri erişilmez kılmak verileri şifrelemeyi ya da başka bir biçimde teknolojik olarak kimsenin verilere erişememesini sağlamayı içerebilir. Bu önlemin virüs programları ya da virüs ya da bomba imalatıyla ilgili bilgiler gibi tehlike ya da toplumsal zararın söz konusu olduğu ya da çocuk pornografisi gibi verilerin ya da içeriklerinin yasadışı olduğu durumlara uygulanması yararlı olabilir. "Taşımak" terimi, verilerin taşınmak ya da erişilmez kılınmakla birlikte yok edilmediği, var olmaya devam ettiği fikrini ifade etmek için kullanılmıştır. Şüpheli geçici olarak verilerden mahrum bırakılmaktadır, ama cezai soruşturma ya da takibatın sonucuna bağlı olarak verilerin geri verilmesi mümkündür.

199. Dolayısıyla verilere el koyma ya da onları benzer şekilde güven altına almanın iki işlevi vardır: 1) Örneğin verileri kopyalamak yoluyla delil toplamak, ya da 2) örneğin verileri kopyalamak ve daha sonra orijinal versiyonlarını erişilmez kılmak ya da taşımak yoluyla verileri müsadere etmek. El koymak, el konan verilerin nihai olarak silinmesi anlamına gelmemektedir.

200. Paragraf 4'te bilgisayar verilerinin aranmasını ve bunlara el konmasını kolaylaştıracak cebri bir önlem getirilmektedir. Paragrafta, işlenebilecek ve saklanacak verilerin miktarı, güvenlik önlemlerine başvurulmuş olması ve bilgisayar işlemlerinin niteliği açısından, delil olarak aranan verilere erişimin ve bu verilerin tanınmasının güç olması şeklindeki pratik sorun ele alınmaktadır. Aramanın en iyi şekilde nasıl yürütülebileceğiyle ilgili teknik nitelikler konusunda, bilgisayar sistemlerine ilişkin özel bir bilgiye sahip sistem yöneticilerine danışılmasının gerekebileceği kabul edilmektedir. Dolayısıyla, hüküm, icra mercilerinin bir sistem yöneticisini arama ve el koyma konusunda yardımcı olmaya, makul sınırlar içinde, zorlamasına izin vermektedir.

201. Bu yetki sadece soruşturmayı yürüten mercilerin yararına değildir. Böyle bir işbirliği olmazsa icra mercileri aramanın yapıldığı işyerinde uzun bir süre kalabilir ve bilgisayar sistemine erişimi engelleyebilirler. Bu durum, meşru işletmeler ve bu süre boyunca verilere erişimi engellenen müşteri ve aboneler için ekonomik bir külfet olabilir. Bilgili insanlara işbirliği yapma talimatı verebilme yolunun yaratılması, arama yapmayı hem icra mercileri hem de durumdan etkilenen masum kişiler için daha etkili ve maliyet açısından etkin bir hale getirecektir. Bir sistem yöneticisini yasal olarak yardım etmeye zorlamak, yöneticinin verileri ifşa etmemek yönünde sözleşmelerden kaynaklanan ya da başka tür yükümlülüklerden kurtulmasını da sağlayabilir.

202. Sağlanması için talimat verilebilecek bilgiler arama ve el koymayı ya da benzer şekilde erişim ve güven altına almayı mümkün kılmak için gerekli olan bilgilerdir. Ancak bu bilgilerin sağlanması "makul" olduğu durumlarla sınırlandırılmıştır. Bazı durumlarda, makul bilgi sağlama bir şifrenin ya da başka bir güvenlik önleminin soruşturmayı yürüten mercilere ifşa edilmesini içerebilir. Ancak bazen, örneğin şifre

ya da başka güvenlik önlemlerinin ifşasının diğer kullanıcıların gizliliğini ya da aranması için yetkili olunmayan verileri tehdit ettiği durumlarda bu makul olmayabilir. Bu durumda, "gerekli bilgiler"in sağlanması, yetkili mercilerce aranmakta olan asıl verilerin anlaşılabilir ve okunabilir bir biçimde ifşa edilmesi olabilir.

203. Bu Maddenin 5. Paragrafı uyarınca önlemler, işbu Konvansiyonun 15. Maddesine dayanılarak, ulusal mevzuat çerçevesinde getirilmiş şartlar ve önlemlere tabidir. Bu şartlar şahitlerin ve uzmanların bulunması ve mali bedellerin ödenmesini de içerebilir.

204. İşbu Konvansiyonu kaleme alanlar paragraf 5 çerçevesinde, bir arama prosedürüyle ilgili olarak ilgili tarafların bilgilendirilmesinin gerekip gerekmediği konusunu tartışmışlardır. Online dünyada verilerin aranması ya da bunlara el konması (kopyalanması), el konan nesnelerin fiziksel olarak ortadan kaybolduğu offline dünyadaki bir el koymadan daha az görünür olabilir. Bazı Taraf Ülkelerin yasaları, geleneksel aramada bildirim yapma zorunluluğu getirmemektedir. Konvansiyonun bilgisayar araması için bildirim zorunluluğu getirmesi, bu

Tarafların yasalarında bir tutarsızlık yaratacaktır. Diğer taraftan, bazı Taraf Ülkeler, saklı verilerin aranması (genellikle gizli bir önlem olması amaçlanmaz) ile akış halindeki verilere müdahale (gizli bir önlemdir, bkz. Madde 20 ve 21) arasındaki ayrımı korumak için, bildirim önlemin temel bir özelliği olarak değerlendirebilirler. Dolayısıyla bildirim konusunu belirlemek ulusal mevzuata bırakılmaktadır. Taraflar ilgili kişilere bildirim yapmanın zorunlu olduğu bir sistem getirmeyi düşünüyorlarsa, böyle bir bildirimin soruşturmaya zarar verebileceği de hesaba katılmalıdır. Böyle bir risk mevcutsa, bildirimin ertelenmesi seçeneği değerlendirilmelidir.

BAŞLIK - 5
***Bilgisayar Verilerinin
Gerçek Zamanlı Olarak Toplanması***

205. Madde 20 ve 21, bir bilgisayar sisteminden iletilen belirli iletişimlerle bağlantılı trafik verilerinin gerçek zamanlı olarak toplanması ve içerik verilerine gerçek zamanlı olarak müdahale edilmesi ile ilgilidir. Hükümlerde bu verilerin yetkili merciler tarafından gerçek zamanlı olarak toplanması ve bunlara gerçek zamanlı olarak müdahale edilmesinin yanı sıra hizmet sağlayıcıların toplama ve müdahaleleri ele alınmaktadır. Gizlilik yükümlülüklerine de değinilmiştir.

206. Telekomünikasyonlara müdahale genellikle geleneksel telekomünikasyon ağlarıyla ilgilidir. Bu ağlar, normal ya da optik kablolardan oluşan kablo altyapılarının yanı sıra cep telefonu sistemleri ve mikrodalga iletim sistemleri gibi kablosuz ağların birbirlerine bağlanmalarını da içerebilir. Günümüzde bir özel uydu ağları sistemi de mobil iletişimlere kolaylaştırmıştır. Bilgisayar ağları bağımsız bir sabit kablo altyapısını da içerebilir, ama genellikle telekomünikasyon altyapılarıyla sağlanan

bağlantılarla oluşan sanal bir ağ olarak işlemektedir ve dolayısıyla küresel nitelikli bilgisayar ağlarının ya da ağ bağlantılarının doğması sağlanmaktadır. Telekomünikasyon ve bilgisayar iletişimleri arasındaki ayırım ve bunların altyapılarının ayrılığı, telekomünikasyon ve bilgi teknolojilerinin birbirlerine yakınlaşmasıyla ortadan kalkmaktadır. Bu nedenle, Madde 1'deki "bilgisayar sistemi" tanımında cihazların ya da cihaz gruplarının birbirlerine bağlanma biçimlerine sınırlama getirilmemiştir. Bundan dolayı, Madde 20 ve 21'de, bir bilgisayar sistemi aracılığıyla iletilen, başka bir bilgisayar sistemine ulaşmadan önce telekomünikasyon ağları aracılığıyla da iletilebilen belirli iletişimlere ele alınmaktadır.

207. Madde 20 ve 21'de, mülkiyeti kamusal ya da özel olan telekomünikasyon ya da bilgisayar sistemleri, ya da kamuya ya da kapalı bir kullanıcı grubu ya da özel kişilere sunulan sistemler ve iletişim hizmetleri arasında ayırım yapılmamaktadır. Madde 1'deki "hizmet sağlayıcı" tanımıyla, hizmetlerinin kullanıcılarına bir bilgisayar sistemi aracılığıyla iletişimde bulunma imkanı sağlayan kamusal ve özel kuruluşlar kastedilmiştir.

208. Bu Başlıkta, o anda üretilmekte olan iletişimlerde içerilen, iletişim anında (yani "gerçek zamanlı") gerçekleştirilen delil toplama işlemi ele alınmaktadır. Veriler, maddi olmayan bir biçimdedir (örneğin, ses ya da elektronik sinyallerin iletilmesi biçiminde). Toplama işlemiyle verilerin akışına önemli ölçüde müdahale edilmez ve iletişim ulaşması istenen yere ulaşır. Verilere fiziksel olarak el koymak yerine, iletilmekte olan verilerin bir kaydı (yani kopyası) üretilir. Delil toplama belli bir süre içerisinde gerçekleştirilir. Gelecekteki bir olayla (yani verilerin gelecek bir tarihte iletilmesi) ilgili olarak toplama işlemine izin verecek yasal bir merci aranır.

209. Toplanabilen veriler iki türdür: trafik verileri ve içerik verileri. "Trafik verileri", Madde 1'd'e, bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını ve süresini ya da bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisi olarak tanımlanmıştır. "İçerik verileri" Konvansiyonda

tanımlanmamıştır, ama iletişimin içeriği, yani iletişimin anlamı ve niyeti ya da iletişimle taşınan mesaj ya da bilgi anlamındadır (trafik verileri dışında):

210. Birçok ülkede, hem böyle bir soruşturma önlemine yetki vermek için gerekli yasal ön koşullar hem de kendisiyle ilgili olarak bu önlemin kullanılabileceği suçlar açısından, içerik verilerine gerçek zamanlı müdahale ile trafik verilerinin gerçek zamanlı olarak toplanması arasında bir ayrım yapılmıştır. Birçok ülkede, her iki tür verinin de gizlilikle ilgili çıkarlar içerebileceği kabul edilmekle beraber, iletişim içeriğinin ya da mesajın doğası gereği içerik verileriyle ilgili gizliliğin daha önemli olduğu düşünülmüştür. İçerik verilerinin gerçek zamanlı olarak toplanması ile ilgili olarak trafik verileri için olduğundan daha büyük sınırlamalar getirilebilir. Bu ülkelerdeki ayrımın korunmasına yardımcı olmak amacıyla bu Konvansiyonda, operasyonel olarak her iki durumda da verilerin toplanmakta ve kaydedilmekte olduğu kabul edilmekle birlikte, normatif olarak maddelerin başlıklarında trafik verilerinin toplanmasından "gerçek zamanlı olarak toplanma", içerik

verilerinin toplanmasından "gerçek zamanlı olarak müdahale etme" şeklinde söz edilmiştir.

211. Bazı ülkelerde mevcut mevzuatta, yasada gizlilikle ilgili çıkarlar arasındaki farklara ilişkin bir ayırım yapılmamış olduğu ya da her iki önlem için teknolojik toplama teknikleri çok benzer olduğu için, trafik verilerinin toplanması ile içerik verilerine müdahale edilmesi arasında hiçbir ayırım yapılmamıştır. Dolayısıyla; önlemlerin uygulanmasına yetki vermek için gereken yasal önkoşullar ve kendisiyle ilgili olarak önlemlerin uygulanabildiği suçlar aynıdır. Konvansiyonda, Madde 20 ve 21'in metninde "toplamak ya da kaydetmek" teriminin ortak operasyonel kullanımıyla bu durum da göz önünde bulundurulmuştur.

212. İçerik verilerine gerçek zamanlı olarak müdahale edilmesiyle ilgili olarak, hukukta genellikle önlemin sadece ciddi suçların ya da ciddi suç kategorilerinin soruşturulmasıyla ilgili olarak kullanılabileceği belirtilmektedir. Bu nedenle, bu suçlar, genellikle uygulanabilir suçlar listesinde belirtilerek ya da suça uygulanabilen azami hapis cezasına atıfta bulunulup bu kategoriye dahil edilerek, ulusal yasalarda ciddi olarak

tanımlanmıştır. Dolayısıyla, Madde 21'de, içerik verilerine müdahaleyle ilgili olarak, Taraflara sadece önlemi "ulusal mevzuatın belirlediği bir dizi ciddi suçla ilgili olarak" tesis etmeleri zorunluluğu getirilmiştir.

213. Diğer taraftan, trafik verilerinin toplanmasıyla ilgili olan Madde 20 bu kadar kısıtlı değildir ve ilke olarak bu Konvansiyonda içerilen bütün cezai suçlar için geçerlidir. Ancak Madde 14, paragraf 3'te, Tarafların, önlemi, sadece hak saklı tutma hakkında belirtilen suçlara ya da suç kategorilerine, bu suç ve suç kategorilerinin içerik verilerine müdahale önlemini uyguladıkları suçlardan daha sınırlı olmaması şartıyla, uygulama hakkını saklı tutabileceği belirtilmiştir. Ancak, böyle bir hak saklı tutulduğunda, ilgili Taraf trafik verilerini toplama önleminin en geniş şekilde uygulanmasını mümkün kılmak için bu saklı tutmayı sınırlandırma seçeneğini değerlendirecektir.

214. Bazı Ülkeler için, Konvansiyonda tesis edilen suçlar normalde içerik verilerine müdahale etmeye, hatta bazı durumlarda, trafik verilerini toplamaya izin verecek kadar ciddi görülmeyebilir. Ancak bu teknikler, bilgisayar

sistemlerine yasadışı erişimle ilgili olanlar ve virüslerin ve çocuk pornografisinin dağıtımı gibi, bu Konvansiyonda tesis edilen bazı suçların soruşturmasında büyük önem taşıyabilir. Örneğin, bazı durumlarda trafik verileri gerçek zamanlı olarak toplanmadan tecavüzün ya da dağıtımın kaynağı belirlenemeyebilir. Bazı durumlarda, içerik verilerine gerçek zamanlı olarak müdahale edilmeden iletişimin niteliği keşfedilemeyebilir. Bu suçlar, doğaları gereği ya da iletim yolu açısından bilgisayar teknolojilerinin kullanımını içerirler. Bu nedenle, bu suçları soruşturmak için teknolojik yöntemlerin kullanılmasına izin verilmelidir. Ancak, içerik verilerine müdahale konusu etrafındaki hassasiyetlerden dolayı, Konvansiyon bu önlemin kapsamının belirlenmesini ulusal mevzuatlara bırakmaktadır. Bazı ülkeler trafik verilerinin toplanmasını hukuki olarak içerik verilerine müdahale edilmesiyle kaynaştırdığı için, birinci önlemin uygulanabilirliğini sınırlamak için hak saklı tutmaya izin verilmiştir; ama bu Tarafların içerik verilerine gerçek zamanlı olarak müdahale etme önlemini sınırladığı dereceden daha büyük olmamalıdır. Ancak, Taraflar, bu bilgisayar suçlarının ve bilgisayarla bağlantılı

suçların soruşturulmasına yönelik etkin bir yol sağlamak için, iki önlemi Konvansiyonun I. Kısımında tesis edilen suçlara uygulamayı değerlendirmelidir.

215. İçerik verilerine gerçek zamanlı olarak müdahale edilmesi ve trafik verilerinin gerçek zamanlı olarak toplanmasıyla ilişkili yetki ve usullerle ilgili şartlar ve önlemler Madde 14 ve 15'e tabidir. İçerik verilerine müdahale edilmesi özel hayata son derece müdahale edici bir önlem olduğu için, adaletle ilgili çıkarlar ve bireyin temel hakları arasında uygun bir dengeye ulaşmak için sıkı önlemler gerekmektedir. Müdahale alanında işbu Konvansiyon, içerik verilerine müdahale etme yetkisini ulusal mevzuatta tanımlanan ciddi cezai suçlarla sınırlamak dışında spesifik önlemler getirmemektedir. Bu alanda, ulusal yasalarda uygulanan önemli şart ve önlemler şunlardır: adli ya da başka bağımsız gözetim; müdahale edilecek iletişim ve kişilerin belirliliği; gereklilik, ikincil önemde "tali" yardımlar ("subsidiarity"), hakkaniyet (örneğin önlemin alınmasını gerekçelendiren hukuki yüklemeler; diğer daha az müdahale edici önlemlerin etkili olmaması); müdahalenin süresinin sınırlandırılması; tazminat hakkı. Bu önlemlerin

çoğu Avrupa İnsan Hakları Konvansiyonunu ve sonrasındaki içtihat hukukunu yansıtmaktadır (bkz. Klass (5), Kruslin (6), Huvig (7), Malone (8), Halford (9), Lambert (10) davalarındaki kararlar). Bu önlemlerden bazıları trafik verilerinin gerçek zamanlı olarak toplanması için de geçerlidir.

Madde 20 - Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması

216. Çoğu zaman, izinsiz giren kişi iletişimin izlediği yolu değiştirdiği için, tarihsel trafik verileri elde edilemez ya da yararsız durumdadır. Bu nedenle, trafik verilerinin gerçek zamanlı olarak toplanması önemli bir soruşturma önlemidir. Madde 20'de spesifik cezai soruşturma ve takibatlarda kullanılmak üzere trafik verilerinin gerçek zamanlı olarak toplanması ve kaydedilmesi konusu ele alınmaktadır.

217. Telekomünikasyonlarla (örneğin telefon konuşmaları) ilgili trafik verilerinin toplanması, geleneksel olarak, çeşitli yasadışı iletişim türlerinin (örneğin suç teşkil eden tehdit ve tacizler, suç işlemeye yönelik komplolar, yalan beyanlar) ve geçmiş ya da gelecekteki suçlara

(örneğin uyuşturucu kaçakçılığı, cinayet, ekonomik suçlar vs.) delil sağlayacak iletişimlerin kaynaklarını ya da varış noktalarını (örneğin telefon numaraları) ve ilgili verileri (örneğin saat, tarih ve süre) belirlemek için yararlı bir soruşturma aracı olmuştur.

218. Bilgisayar iletişimleri de aynı tür suçlar teşkil edebilir ya da bu suçlarla ilgili delil sağlayabilir. Ancak, bilgisayar teknolojisi, yazılı metin, görsel imaj ve ses biçiminde çok büyük miktarlarda veriyi iletmeye imkan sağladığı için yasadışı içeriğin (örneğin çocuk pornografisi) dağıtım yoluyla işlenen suçlar için daha büyük bir potansiyele sahiptir. Benzer şekilde, bilgisayarlar çoğu zaman gizlilik içeren, büyük miktarlarda veriyi saklamaya imkan sağladığı için, verilerin bütünlüğüne müdahale edilirse oluşacak ekonomik, sosyal ya da kişisel zarar potansiyeli önemli ölçülere ulaşabilir. Ayrıca, bilgisayar teknolojisi bilimi verilerin işlenmesi üzerine kurulu olduğu için, hem nihai bir ürün hem de operasyonel işlevinin bir parçası (örneğin bilgisayar programlarının çalışması) olarak bu verilere müdahale edilmesi, bilgisayar sistemlerinin uygun işleyişi üzerinde feci sonuçlar doğurabilir. Çocuk pornografisinin

yasadışı dağıtımı, bilgisayar sistemlerine yasadışı erişim ya da bilgisayar sisteminin uygun işleyişine müdahale suçu işlendiği zaman, özellikle suç uzaktan, örneğin İnternet aracılığıyla işlenmişse, iletişimin izlediği yolu geriye, kurbandan faile doğru izlemek gerekli ve önemlidir. Bu nedenle, bilgisayar iletişimleriyle ilgili trafik verilerini toplayabilmek, tamamen geleneksel telekomünikasyonlar için olduğu kadar, hatta belki daha da önemlidir. Bu soruşturma tekniği sayesinde şüphelinin iletişimlerinin saat, tarih, kaynak ve varış noktasıyla kurbanların sistemlerine izinsiz girildiği tarih arasında bağlantı kurulabilir, diğer kurbanlar teşhis edilebilir ya da suç ortakları arasındaki bağlantılar ortaya çıkarılabilir.

219. Bu Madde uyarınca, ilgili trafik verileri Taraf Ülkenin ulusal sınırları içindeki belirli iletişimlerle bağlantılı olmalıdır. Kaynaktaki ya da varış noktasındaki insanları belirlemek için birçok iletişimle ilgili trafik verilerinin toplanması gerekebileceği için belirli "iletişimler" ifadesi çoğuldur (örneğin, birden çok insanın aynı telekomünikasyon imkanlarını kullandığı bir evde çeşitli iletişimlerle kişilerin bilgisayar sistemini kullanma fırsatları arasında bağlantı kurmak

gerekli olabilir). Ancak, kendisiyle ilgili trafik verilerinin toplanabildiği ya da kaydedilebildiği iletişimler belirlenmek zorundadır. Dolayısıyla Konvansiyonda büyük miktarlarda trafik verisinin genel amaçlı ve gelişigüzel bir biçimde toplanması şart koşulmamakta ve buna izin verilmemektedir. Belirli suç vakalarının soruşturulması yerine, suçların keşfedilebileceğinin umulduğu durumlarda, denize olta atmak benzeri girişimlere yetki verilmemektedir. Toplama yetkisini veren adli ya da başka tür talimatlarda trafik verilerinin toplanabileceği iletişimler belirtilmek zorundadır.

220. Paragraf 2'ye tabi olmak üzere, paragraf 1(a) uyarınca Taraflar yetkili mercilerinin trafik verilerini teknik imkanlar yoluyla toplayabilme ve kaydedebilmesini sağlamak zorundadır. Maddede toplamanın teknolojik olarak nasıl gerçekleştirileceği belirtilmemekte ve teknik açıdan hiçbir yükümlülük tanımlanmamaktadır.

221. Ayrıca, paragraf 1(b) uyarınca, Taraflar, yetkili mercilerinin, hizmet sağlayıcıları trafik verilerini toplamaya ya da kaydetmeye ya da bu verilerin toplanması ve kaydedilmesi konusunda yetkili

mercilere işbirliği ve yardım sağlamaya mecbur edebilme yetkisine sahip olmalarını sağlamak zorundadır. Hizmet sağlayıcılarla ilgili bu yükümlülük, ancak bu toplama ve kaydetme ya da işbirliği ve yardım hizmet sağlayıcının mevcut teknik imkanları dahilinde olduğunda geçerlidir. Maddede hizmet sağlayıcılara toplama, kaydetme, işbirliği ya da yardım konusunda teknik yeterliliğe sahip olma yükümlülüğü getirilmemektedir. Hizmet sağlayıcıların yeni teçhizat edinmeleri ya da geliştirmeleri, uzman desteği sağlamaları ya da sistemlerinin konfigürasyonunu yenilemek için masraflı girişimlerde bulunmaları şart koşulmamaktadır. Ancak, Maddede, sistemleri ve personelleri halihazırda böyle bir toplama, kaydetme, işbirliği ya da yardım sağlayacak teknik yeterliliğe sahipse bu yeterliliği kullanmaları için gerekli önlemleri almaları şartı getirilmektedir. Örneğin, sistemin konfigürasyonu buna uygun olabilir, ya da hizmet sağlayıcı halihazırda bu önlemlerin alınmasına izin verecek bilgisayar programlarına sahip olabilir, ama bunlar hizmet sağlayıcının normal çalışması esnasında olağan olarak çalıştırılmaz ya da kullanılmaz. Maddede, yasaların gerektirdiği gibi, hizmet sağlayıcının bu

özellikleri seferber etmesi ya da faaliyete geçirmesi şart koşulmaktadır.

222. Bu ulusal düzeyde uygulanacak bir önlem olduğu için, önlemler ilgili Tarafın ulusal sınırları içindeki belirli iletişimlerin toplanması ve kaydedilmesi için geçerlidir. Dolayısıyla, pratik olarak, yükümlülükler genel olarak hizmet sağlayıcının, başlıca faaliyetlerini yürüttüğü yer ya da merkez ofisi başka yerde olsa da, bu ulusal sınırlar içinde önlemleri gerçekleştirecek fiziksel altyapı ya da teçhizata sahip olduğu durumlar için geçerlidir. İşbu Konvansiyonun amaçları açısından, iletişimde bulunan taraflardan biri (insan ya da bilgisayar) belli bir Taraf Ülkenin ulusal sınırları içindeyse ya da iletişimin geçtiği bilgisayar ya da telekomünikasyon teçhizatı bu sınırlar içinde bulunuyorsa, söz konusu iletişimin ilgili Tarafın ulusal sınırları içinde olduğu kabul edilecektir.

223. Genel olarak, paragraf 1(a) ve (b)'deki iki trafik verisi toplama imkanı birbirlerinin alternatifi değildir. Paragraf 2'de belirtilen husus dışında, Taraflar her iki önlemin de uygulanmasını sağlamalıdır. Bu gereklidir, çünkü bir hizmet sağlayıcı trafik verilerinin toplanmasını ya da

kaydedilmesini üstlenecek teknik yeterliliğe sahip değilse (1(b)), icra mercilerinin bu işi kendi başlarına gerçekleştirebilmeleri için Taraf Ülke bu imkana sahip olmalıdır. Benzer şekilde, yetkili merciler kendi başlarına trafik verilerini toplama ve kaydetme yetkisine sahip değilse paragraf 1(b)(ii) uyarınca trafik verilerinin toplanması ve kaydedilmesi konusunda yetkili mercilere işbirliği ve yardım sunma yükümlülüğü anlamsızdır. Ayrıca, hiçbir hizmet sağlayıcının faaliyette olmadığı bazı yerel ağlar (LAN'lar) söz konusu olduğunda, toplama ve kaydetme işlemlerinin yerine getirilmesinin tek yolu soruşturmayı yürüten mercilerin bu işi kendi başlarına yapmalarıdır. Paragraf 1 (a) ve (b)'deki önlemlerin her ikisinin de her defasında kullanılması zorunlu değildir ama Maddede her iki yöntemin de kullanılabilir durumda olması şart koşulmaktadır.

224. Ancak bu ikili yükümlülük, icra mercilerinin telekomünikasyon sistemlerindeki verilere ancak bir hizmet sağlayıcının yardımı aracılığıyla müdahale edebildiği ya da hizmet sağlayıcının en azından bilgisi olmadan, gizli bir biçimde müdahale edemediği bazı ülkelerde güçlükler yaratmaktadır. Bu nedenle paragraf 2'de böyle

bir durum ele alınmıştır. "Ulusal hukuk sistemindeki yerleşik ilkeler" nedeniyle paragraf 1 (a)'daki önlemleri benimseyemeyen bir Taraf Ülke, başka bir yaklaşım benimseyerek, hizmet sağlayıcıları sadece icra mercilerinin trafik verilerini gerçek zamanlı olarak toplayabilmelerini sağlamak için gerekli teknik imkanları sağlamaya zorlayabilir. Böyle bir durumda, ulusal sınırlar, iletişimlerin belirliliği ve teknik imkanların kullanımıyla ilgili diğer sınırlamalar yine de geçerlidir.

225. İçerik verilerine gerçek zamanlı olarak müdahale etmek gibi, trafik verilerinin gerçek zamanlı olarak toplanabilmesi de ancak soruşturulan kişilerin bilgisi olmadan gerçekleştirildiği zaman etkili olabilir. Müdahale gizlidir ve iletişimin taraflarının algılayamayacakları bir şekilde yürütülmelidir. Bu nedenle, prosedürün gerektiği gibi gerçekleştirilebilmesi için hizmet sağlayıcılar ve bunların müdahaleden haberdar olan çalışanları bir gizlilik yükümlülüğü altındadır.

226. Paragraf 3'te Tarafların, hizmet sağlayıcıları, bu Maddede belirtilen, trafik verilerinin gerçek zamanlı olarak toplanmasıyla ilgili önlemlerden herhangi birinin gerçekleştirildiğini ya da

gerçekleştirilmesiyle ilgili her türlü bilgiyi gizli tutmaya zorlamak için gerekli olabilecek yasamayla ilgili ya da diğer önlemleri benimsemeleri şart koşulmaktadır. Bu hüküm soruşturmanın gizliliğini güvence altına almasının yanı sıra, hizmet sağlayıcıyı da abonelerine kendileriyle ilgili verilerin toplanmakta olduğunu bildirmek konusunda sözleşmelerden kaynaklanan ya da başka tür hukuki yükümlülüklerden kurtarır. Paragraf 3, mevzuatta açık yükümlülüklerin yaratılması yoluyla yürürlüğe konabilir. Diğer taraftan, Taraflar, önlemin gizliliğini önlemi suçlulara haber vererek onlara yardım eden insanlar hakkında adaleti engellediklerinden dolayı dava açma yetkisi gibi diğer ulusal yasa hükümlerine dayanarak da sağlayabilir. Spesifik bir gizlilik şartı (ihlal durumunda etkili bir yaptırımla) tercih edilen bir usul olmakla birlikte, adaleti engelleme suçlarının kullanılması uygun olmayan ifşayı engellemek için alternatif bir yoldur, ve dolayısıyla, bu paragrafı uygulamak için geçerlidir. Açık gizlilik yükümlülükleri yaratılırsa, bu yükümlülükler Madde 14 ve 15'te belirtilen şart ve önlemlere tabi olacaktır. Soruşturma önleminin gizlilik niteliği açısından, bu önlem ve

226 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

şartlar yükümlülüğün süresi için makul zaman dilimleri getirmelidir.

227. Yukarıda belirtildiği gibi, trafik verilerinin toplanmasıyla ilgili olarak gizlilik çıkarının içerik verilerine müdahalede olduğundan daha az önemli olduğu kabul edilmektedir. İletişimin saat, süre ve büyüklüğü, kişiler ve düşünceleri hakkında çok az kişisel bilgi sağlamaktadır. Ancak, iletişimin kaynağı ve varış noktasına (örneğin ziyaret edilen web siteleri) ilişkin verilerle ilgili olarak daha güçlü bir gizlilik sorunu mevcuttur. Bu verilerin toplanması, bazı durumlarda, bir kişinin ilgileri, bağlantıları ve toplumsal konumunun bir profilini çıkarmak için yeterli olabilir. Bu nedenle, Taraflar, Madde 14 ve 15 uyarınca bu önlemleri uygulamak için uygun önlem ve hukuki önkoşulları tesis ederken bu değerlendirmeleri göz önünde bulundurmalıdır.

Madde 21 - İçerikle İlgili Bilgilere Müdahale Edilmesi

228. Geleneksel olarak; telekomünikasyonlarla (örneğin telefon konuşmaları) ilgili içerik verilerinin toplanması, iletişimin yasadışı nitelikte olduğunu belirlemek (örneğin iletişimin suç teşkil eden tehdit ve tacizler, suç işlemeye

yönelik komplolar, yalan beyanlar içermesi) ve geçmişteki ve gelecekteki suçlarla (örneğin uyuşturucu kaçakçılığı, cinayet, ekonomik suçlar vs.) ilgili delil toplamak için yararlı bir soruşturma aracı olmuştur. Bilgisayar iletişimleri de aynı tür suçları teşkil edebilir ya da aynı tür suçlar için delil sağlayabilir. Ancak, bilgisayar teknolojisi, yazılı metin, görsel imaj ve ses biçiminde çok büyük miktarlarda veriyi iletmeye imkan sağladığı için yasadışı içeriğin (örneğin çocuk pornografisi) dağıtımı yoluyla işlenen suçlar için daha büyük bir potansiyele sahiptir. Çoğu bilgisayar suçu verilerin iletim ya da iletişimi yoluyla işlenir; örneğin bir bilgisayar sistemine yasadışı erişim gerçekleştirmek için gönderilen iletişimler ya da bilgisayar virüslerinin dağıtımı. Mesajın içeriğine müdahale etmeden, bu iletişimlerin zararlı ve yasadışı nitelikte olduğunu gerçek zamanlı olarak belirlemek mümkün değildir. Suçluluğu oluşumu sırasında belirleme ve önleme yeteneği olmaksızın, icra mercilerinin tek işlevi zararın halihazırda oluşmuş olduğu geçmiş ve tamamlanmış suçları soruşturmak olur. Dolayısıyla, bilgisayar iletişimlerinin içerik verilerine gerçek zamanlı olarak müdahale etmek, telekomünikasyonlara

gerçek zamanlı olarak müdahale etmek kadar, hatta belki daha da önemlidir.

229. "İçerik verileri" iletişimin iletişim içeriği, yani iletişimin anlamı ya da niyeti, ya da iletişim yoluyla iletilen mesaj ya da bilgi anlamındadır. Trafik verileri dışında iletişime ait olarak iletilen her şey içerik verisidir.

230. Bu Maddenin çoğu unsuru Madde 20'nin unsurlarıyla özdeştir. Bu nedenle, yukarıda belirtilen, trafik verilerinin toplanması ve kaydedilmesi, işbirliği ve yardım yükümlülüğü ve gizlilik yükümlülüğü ile ilgili bütün değerlendirmeler içerik verilerine müdahale için de aynen geçerlidir. İçerik verilerinin gizlilikle ilgili daha büyük çıkarlar içermesinden dolayı, soruşturma önlemi "ulusal mevzuatın belirlediği bir dizi ciddi suç"la sınırlandırılmıştır.

231. Yukarıda, Madde 20 ile ilgili değerlendirmelerde belirtildiği gibi, içerik verilerine gerçek zamanlı olarak müdahale edilmesi için geçerli şart ve önlemler, trafik verilerinin gerçek zamanlı olarak toplanması, ya da saklı verilerin aranması ve bunlara el konması ya da benzer şekilde verilere erişilmesi ya da güven altına alınması için geçerli olanlardan daha sıkı olabilir.

KISIM - 3
Yargı Yetkisi

Madde 22 - Yargı Yetkisi

232. Bu Maddede Konvansiyona Taraf Ülkelerin, Konvansiyonun 2-11. Maddelerinde sıralanan cezai suçlar üzerinde yargı yetkisi tesis ederken uymak zorunda oldukları bir dizi ölçüt tesis edilmiştir.
233. Paragraf 1'in a şıkkı mülkilik ilkesine dayanmaktadır. Tarafların her birinin bu Konvansiyonda tesis edilen suçlardan kendi ulusal sınırları içinde işlenen suçları cezalandırması gerekmektedir. Örneğin, hem bir bilgisayar sistemine saldıran kişi, hem de saldırının kurbanı olan sistem belli bir Taraf Ülkenin sınırları içindeyse, ve saldırgan olmasa da saldırıya uğrayan bilgisayar sistemi bu sınırlar içindeyse, ilgili Taraf Ülke mülki yargı yetkisine sahiptir.
234. Her bir Taraf Ülkenin kendi adına kayıtlı uydularla bağlantılı suçlar üzerinde yargı yetkisine sahip olmasını şart koşan bir hükmün eklenmesi düşünülmüştür. Konvansiyonu kaleme alanlar bunun gereksiz olacağına karar

vermişlerdir; çünkü uydu üzerinden gerçekleştirilen yasadışı iletişimler daima yeryüzünden başlatılmakta ve/veya yeryüzündeki bir noktaya ulaşmaktadır. Bu nedenle, iletim Taraf Ülkenin yargı yetkisi için paragraf 1(a) - (c)'de belirtilen yerlerden birinde başlar ya da biterse yargı yetkisi için bu yer esas alınacaktır. Ayrıca, uydu iletişiminin söz konusu olduğu bir suç belli bir Taraf Ülkenin vatandaşı tarafından herhangi bir Ülkenin yargı yetkisine sahip olduğu sınırlar dışında işlenmesi halinde, paragraf 1(d) yargı yetkisine temel oluşturacaktır. Son olarak, uydu hizmetleri iletim için sadece bir taşıyıcı konumunda olduğu için çoğu durumda işlenen suçla kaydın yapıldığı ülke arasında hiçbir anlamlı bağlantı olmadığını göz önünde bulunduran Konvansiyonu kaleme alanlar kayıtların cezai yargı yetkisi için uygun bir temel oluşturmadığını düşünmüşlerdir.

235. Paragraf 1'in b ve c şıkları mülkilik ilkesinin farklı bir biçimine dayanmaktadır. Bu şıklarda Taraflardan her birinin kendi bandırasını taşıyan gemilerde ve kendi yasaları çerçevesinde kayıtlı bir uçakta işlenen suçlar için cezai yargı yetkisini tesis etmesi şart koşulmaktadır. Bu şekildeki gemi ve uçaklar genellikle ulusal sınırların bir

uzantısı olarak kabul edildiği için, bu yükümlülük birçok ülkenin mevzuatında zaten genel bir husus olarak ele alınmaktadır. Bu tür yargı yetkisi gemi ya da uçak suçun işlenmesi esnasında ulusal sınırlar içinde olmadığı, bunun sonucunda da Paragraf I'in a şıkkının yargı yetkisi iddia etmek için temel oluşturmadığı durumlarda çok yararlıdır. Suç, bayrağın sahibi Taraf Ülkenin ulusal sınırlarının dışında işlenirse bu koşulu engelleyerek yargı yetkisini kullanacak başka bir devlet olmayabilir. Ayrıca, başka bir devletin karasularından ya da hava sahasından geçmekte olan bir gemi ya da uçakta bir suç işlenirse bu devlet yargı yetkisini işletmekte ciddi pratik engellerle karşılaşabilir. Bu nedenle yargı yetkisinin gemi ya da uçağın kayıtlı olduğu Devlete ait olması yararlıdır.

236. Paragraf I'in d şıkkı ulusallık ilkesine dayanmaktadır. Ulusallık teorisi en çok medeni hukuk geleneğini uygulayan devletler tarafından uygulanmaktadır. Bu teoriye göre bir devletin vatandaşları ulusal sınırların dışında olsalar bile ulusal yasalara uymak zorundadırlar. Paragraf I'in d şıkkı uyarınca, Taraflar, bir vatandaşları yurtdışında bir suç işlediğinde, fiil suçun işlendiği ülkenin yasalarına göre de suç

sayılıyorsa ya da herhangi bir devletin yargı yetkisinin dışında gerçekleşmişse, suçu kovuşturabilecek durumda olmalıdırlar.

237. Paragraf 2, Tarafların paragraf 1'in b, c ve d şıklarında belirtilen yargı yetkileriyle ilgili olarak haklarını saklı tutmalarına izin vermektedir. Ancak, a şıkkı uyarınca mülki yargı yetkisi tesis etmekle ya da paragraf 3 uyarınca, "aut dedere aut judicare" (iade et ya da kovuştur) ilkesine uygun düşen, yani bir Taraf Ülkenin bir zanlıyı uyruğu dolayısıyla iade etmeyi reddettiği ve zanlının kendi ulusal sınırları içerisinde bulunduğu durumlarda yargı yetkisi tesis etmekle ilgili olarak ülkelerin herhangi bir hak saklı tutmalarına izin verilmemektedir. İşbu Konvansiyonun 24. Maddesinin 6. paragrafındaki "İade" şartları uyarınca iade talep eden Taraf Ülke tarafından istendiğinde, bu ülkenin vatandaşını iade etmeyi reddeden Taraf Ülkenin soruşturma ve takibatı kendi ülkesinde gerçekleştirmeye yasal yetkisi olmasını sağlamak için Paragraf 3 esas alınarak tesis edilen yargı yetkisi gereklidir.

238. Paragraf 1'de belirtilen yargı yetkisi temelleri münhasır değildir. Bu Maddenin 4. paragrafı

Tarafların kendi ulusal mevzuatlarına uygun biçimde başka türde cezai yargı yetkileri tesis etmelerine de izin vermektedir.

239. Bilgisayar sistemleri kullanılarak işlenen suçlarda, suça iştirak edenlerin bazılarının ya da hepsinin birden fazla Taraf Ülkenin yargı yetkisine tabi olduğu durumlar olabilmektedir. Örneğin, İnternet kullanılarak gerçekleştirilen çoğu virüs saldırısı, sahtekarlık ve telif hakkı ihlali çeşitli ülkelerde bulunan kurbanları hedef almaktadır. Aynı çalışmaların tekrarlanmasından, tanıkların gereksiz şekilde rahatsız edilmesinden ya da ilgili ülkelerin icra görevlileri arasında rekabet yaşanmasından kaçınmak, ya da takibatın etkinliğine ve adilliğine başka şekillerde katkıda bulunmak için, etkilenen Taraflar takibat için uygun yeri belirlemek konusunda birbirleriyle istişare edeceklerdir. Bazı durumlarda, ilgili Ülkeler için en etkin yol takibat için tek bir yer seçmektir; bazı durumlarda ise suça iştirak edenlerin bazılarının bir ülkede, bazılarının başka ülke ya da ülkelerde kovuşturulması en iyi çözüm olabilir. Bu paragrafta her iki duruma da izin verilmiştir. Son olarak, istişare etme yükümlülüğü mutlak değildir ve "uygun olduğu durumlarda"

gerçekleştirilecektir. Bu nedenle, örneğin, Taraf Ülkelerden biri istişarenin gerekli olmadığını biliyorsa (örneğin diğer Taraf Ülkenin harekete geçmeyi planlamadığı bilgisini aldıysa) ya da Taraf Ülke istişarenin soruşturma ya da takibatını bozabileceği kanaatindeyse istişareyi erteleyebilir ya da reddedebilir.

BÖLÜM - III *Uluslararası İşbirliği*

240. Bölüm III'te iade ve Taraf Ülkeler arasında yardımlaşma ile ilgili bir dizi hüküm yer almaktadır.

KISIM - 1
Genel İlkeler

BAŞLIK - 1
Uluslararası İşbirliğine İlişkin Genel İlkeler

**Madde 23 - Uluslararası İşbirliğine İlişkin
Genel İlkeler**

241. Madde 23'te Bölüm III çerçevesindeki uluslararası işbirliği ile ilgili üç genel ilke ortaya konmuştur.

242. İlk olarak, Maddede Taraflar arasındaki uluslararası işbirliğinin "mümkün olan en geniş biçimde" gerçekleştirileceği açıkça belirtilmiştir. Bu ilke uyarınca Tarafların birbirlerine kapsamlı işbirliği sağlamaları, ve bilgi ve delillerin uluslararası akışının düzgün ve hızlı olmasını engelleyen faktörleri en aza indirmeleri şart koşulmuştur.

243. İkinci olarak, Madde 23'te işbirliği yükümlülüğünün genel kapsamı ortaya konmuştur: İşbirliği bilgisayar sistemleri ve verileri ile ilgili bütün cezai suçların (yani Madde 14, paragraf 2, şık a-b'de içerilen suçlar) yanı sıra cezai bir suçun delillerinin elektronik

ortamda toplandığı bütün durumlar için geçerlidir. Başka bir deyişle, suçun bir bilgisayar sistemi kullanılarak işlendiği ya da bir bilgisayar sistemi kullanılarak işlenmeyen sıradan bir suçla (örneğin cinayet) ilgili elektronik delillerin bulunduğu durumlarda Bölüm III'ün hükümleri geçerlidir. Ancak Madde 24 (İade), 33 (Trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma) ve 34'ün (İçerikle ilgili verilere müdahale edilmesi konusunda yardımlaşma) Tarafların bu önlemlerin uygulamasında farklı bir kapsam benimsemelerine izin verdiği de göz önünde bulundurulmalıdır.

244. Son olarak, işbirliği hem "bu bölüm hükümleri çerçevesinde" hem de "cezai meselelerde uluslararası işbirliğine ilişkin uluslararası belgelerin, tek taraflı ya da karşılıklı sözleşmelerin ve ulusal yasaların uygulanması yoluyla" gerçekleştirilecektir. İkinci ifadede Bölüm III'ün hükümlerinin, hukuki yardımlaşma ve iade ile ilgili uluslararası sözleşmelerin hükümlerinin, taraflar arasındaki karşılıklı sözleşmelerin (aşağıda, Madde 27 ile ilgili tartışmada daha ayrıntılı olarak açıklanmıştır) ve ulusal mevzuatın uluslararası işbirliğiyle

bağlantılı ilgili hükümlerinin yerine geçmeyeceği şeklindeki genel ilke ortaya konmaktadır. Bu temel ilke Madde 24 (İade), 25 (Yardımlaşmaya ilişkin genel ilkeler), 26 (Anında iletilen bilgiler), 27 (Uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen yardım taleplerine ilişkin usuller), 28 (Kullanımda gizlilik ve sınırlama), 31 (Saklanan bilgisayar verilerine erişilmesine ilişkin yardımlaşma), 33 (Trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma) ve 34'te (İçerikle ilgili verilere müdahale edilmesi konusunda yardımlaşma) açık bir biçimde pekiştirilmiştir.

BAŞLIK - 2
İadeye İlişkin ilkeler

Madde 24 - İade

245. Paragraf 1'de iade yükümlülüğünün sadece işbu Konvansiyonun 2-11. Maddeleri çerçevesinde tanımlanan, her iki Taraf Ülkenin yasalarında en az bir yıllık azami süreyle özgürlükten mahrum bırakma ya da daha ağır nitelikli bir cezayla cezalandırılabilir olan cezalar için geçerli olduğu belirtilmektedir. Konvansiyonu kaleme alanlar bir eşik ceza getirmeye karar vermişlerdir, çünkü Konvansiyon uyarınca, Taraf Ülkeler bazı suçları daha kısa azami hapis süreleriyle cezalandırabilirler (örneğin Madde 2 - yasadışı erişim - ve Madde 4 - verilere müdahale). Bu açıdan, Konvansiyonu kaleme alanlar Madde 2-11'de tanımlanan suçların her birinin başlı başına iadeye konu olabilen suçlar olarak değerlendirilmesinin şart koşulmasının uygun olacağına inanmamaktadırlar. Dolayısıyla, bir suçun, - Avrupa İade Konvansiyonu'nun (ETS No. 24) 2. Maddesinde öngörüldüğü gibi - bu suç için verilebilecek azami cezanın en az bir yıl hapis olması durumunda iadeye konu olabilen suçlar olarak kabul edilmesi şeklinde genel bir

şart getirilmesi üzerinde anlaşılmıştır. Bir suçun iadeye konu olabilen bir suç olup olmadığının belirlenmesi o an ele alınmakta olan belli bir durumda verilen gerçek cezaya değil, iade talebinde bulunulan ihlal için yasal olarak verilebilecek azami süreye bağlıdır.

246. Paragraf 1'de, aynı zamanda, Bölüm III çerçevesindeki uluslararası işbirliğinin Taraflar arasında yürürlükte olan araçlar uyarınca yürütülmesi şeklindeki genel ilkeye uygun olarak, iki ya da daha fazla Taraf arasında yürürlükte olan ve iade için farklı bir eşik öngören tek taraflı ya da karşılıklı bir iade anlaşması ya da düzenleme mevcutsa (aşağıda Madde 27 ile ilgili değerlendirmelerde bu hükmün açıklamasına bkz.), bu anlaşma ya da düzenlemede öngörülen eşik geçerli olacaktır. Örneğin, Avrupa ülkeleriyle Avrupa dışındaki ülkeler arasındaki birçok iade anlaşmasında bir suçun ancak azami ceza bir yıl haptiden büyükse ya da daha ağır bir ceza mevcutsa iadeye konu edilebileceği kararlaştırılmıştır. Bu gibi durumlarda, bir suçun konu olup olamayacağını belirlemek için uluslararası iade icracıları kendi anlaşma uygulamaları çerçevesindeki normal eşiği uygulamaya devam edeceklerdir. Avrupa

İade Konvansiyonu'nda bile (ETS No. 24) hak saklı tutma hükümlerinde iade için farklı bir asgari ceza belirtilmiş olabilir. İşbu Konvansiyonun Tarafları arasında, böyle bir hak saklı tutmakta olan bir Taraf Ülkeden iade talebinde bulunulduğunda, suçun iadeye konu edilebilir olup olmadığını belirlemek konusunda hak saklı tutma hükmünde belirtilen ceza uygulanacaktır.

247. Paragraf 2'de, paragraf 1 çerçevesinde tanımlanan cezai suçların iki ya da daha fazla Taraf arasındaki iade anlaşmaları çerçevesinde iadeye konu olabilen suçlar olarak addedileceği ve Tarafların kendi aralarında gelecekte yapacakları anlaşmalara dahil edilecekleri belirtilmektedir. Bu, her talep edildiğinde iadeye izin verileceği değil, bu suçlar için kişilerin iade imkanının mevcut olması gerektiği anlamına gelmektedir. Paragraf 5 çerçevesinde Taraflar iade için başka şartlar ileri sürebileceklerdir.

248. Paragraf 3 uyarınca, iade talebinde bulunan Taraf Ülkeyle arasında iade anlaşması olmadığı ya da mevcut anlaşmalar işbu Konvansiyonda tanımlanan suçlarla ilgili bir talebi kapsamadığı için iade işlemini gerçekleştirmeyen bir Taraf

Ülke, buna zorunlu olmamakla birlikte, talep edilen kişiyi iade etmek için bu Konvansiyonu hukuki zemin olarak kullanabilir.

249. Paragraf 4'te, Taraflardan birinin iade işlemini iade anlaşmalarına değil genel bir yasal plana bağladığı durumlarda, iadenin mümkün olduğu suçlara paragraf 1'de tanımlanan suçların da dahil edilmesi şart koşulmuştur.

250. Paragraf 5'te, talebin yapıldığı Tarafın geçerli anlaşma ve yasalardaki bütün hüküm ve şartların yerine getirilmiş olduğu konusunda tatmin olmadığı durumlarda iadeyi gerçekleştirmek zorunda olmadığı belirtilmektedir. Bu durum, Taraflar arasında yürürlükte bulunan geçerli uluslararası araçların, karşılıklı düzenlemelerin ya da ulusal yasaların hükümleri uyarınca işbirliğinin gerçekleştirilmesi ilkesi için diğer bir örnektir. Örneğin, Avrupa İade Konvansiyonunda (ETS No 24) ve Ek Protokollerinde (ETS No 86 ve 98) belirtilen şartlar ve sınırlamalar bu sözleşmelerin tarafları için geçerli olacak ve bunlar esas alınarak iade reddedilebilecektir (örneğin Avrupa İade Konvansiyonu'nun 3. Maddesinde, suçun siyasi nitelikli olduğu düşünüldüğünde ya da iade talebinin söz

konusu kişiyi, başka şeylerin yanı sıra, ırk, din, milliyet ya da siyasi görüşü nedeniyle kovuşturmak ya da cezalandırmak amacıyla yapıldığına karar verildiğinde iadenin reddedileceği bildirilmiştir).

251. Paragraf 6 "aut dedere aut judicare" (iade et ya da kovuştur) ilkesine dayanmaktadır. Birçok ülke kendi vatandaşlarının iadesini reddettiği için, vatandaşları oldukları Taraf Ülkede bulunan suçlular, yerel merciler gerekli işlemleri yapmaya zorlanmazsa, başka bir Taraf Ülkede işlenmiş bir suçun sorumluluğundan kurtulabilirler. Paragraf 6 uyarınca, bir Taraf Ülke bir suçlunun iadesini talep etmişse ve suçlunun talebin yapıldığı Taraf Ülkenin vatandaşı olması gerekçesiyle iade reddedilmişse, talebin yapıldığı Taraf Ülke, talebi yapan Taraf Ülkenin talebi üzerine, kovuşturulmak üzere vakayı ilgili mercilere sevk etmek zorundadır. İade talebi reddedilen Taraf vakanın yerel soruşturma ve takibat için sevkini talep etmezse, talebin yapıldığı Taraf hukuki işlem yapmak zorunda değildir. Ayrıca, iade talebi yapılmadıysa ya da iade uyruk dışındaki nedenlerle reddedildiyse, talebin yapıldığı Tarafın vakayı ulusal kovuşturmaya sevk etmesi

için bu paragrafta bir yükümlülük getirilmemektedir. Ayrıca, paragraf 6'da yerel soruşturma ve takibatın titizlikle yerine getirilmesi; vakanın "karşılaştırılabilir nitelikte başka bir suç durumunda olduğu" kadar ciddi bir şekilde ele alınması şart koşulmaktadır. İlgili Taraf, talebi yapan Tarafa soruşturma ve takibatın sonucunu bildirecektir.

252. Taraflardan her birinin geçici tutuklama ve iade taleplerinin nereye yöneltileceğini bilebilmesi için, paragraf 7'de Tarafların, herhangi bir anlaşmanın olmadığı durumlarda iade ve geçici tutuklama taleplerini yapmak ya da kabul etmekten sorumlu olacak mercilerinin isim ve adreslerini Avrupa Konseyi Genel Sekreteri'ne bildirmeleri şart koşulmaktadır. Bu hüküm ilgili Taraflar arasında yürürlükte iki taraflı ya da çok taraflı bir iade anlaşmasının bulunmadığı durumlarla sınırlandırılmıştır; çünkü taraflar arasında iki taraflı ya da çok taraflı bir iade anlaşmasının (örneğin ETS No. 24) bulunduğu durumlarda, Taraflar bir kayıt yaptırma zorunluluğu olmaksızın iade ve geçici tutuklama taleplerinin kime yapılacağını bileceklerdir. Genel Sekreter'e bildirim imza sırasında ya da Taraf Ülkenin onay, kabul, tasdik ya da giriş

244 *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

belgesi teslim edildiğinde yapılmalıdır. Bir merciin belirlenmesinin diplomatik kanalların kullanılması seçeneğini dışlamadığı göz önünde tutulmalıdır.

BAŞLIK - 3
Yardımlaşmaya İlişkin Genel İlkeler

Madde 25 - Yardımlaşmaya İlişkin Genel İlkeler

253. Yardımlaşma sağlama yükümlülüğüyle ilgili genel ilkeler paragraf 1'de belirtilmiştir. İşbirliği "mümkün olan en geniş şekilde" sağlanacaktır. Dolayısıyla, Madde 23'te ("Uluslararası işbirliğine ilişkin genel ilkeler") belirtildiği gibi yardımlaşma ilke olarak geniş olacak, ve yardımlaşmayı engelleyen unsurlar sıkı bir biçimde sınırlandırılacaktır. İkinci olarak, Madde 23'te belirtildiği gibi, işbirliği yükümlülüğü ilke olarak hem bilgisayar sistemleri ve verileriyle bağlantılı suçlar (yani Madde 14, paragraf 2 şık a-b'nin kapsamına alınan suçlar) hem de elektronik ortamda bir cezai suçun delillerinin toplanması için geçerlidir. Bu geniş suç grubuyla ilgili olarak işbirliği yükümlülüğü getirilmesine karar verilmiştir; çünkü kolay ve elverişli uluslararası işbirliği mekanizmalarına duyulan ihtiyaç bu kategorilerin her ikisi için de mevcuttur. Ancak, Madde 34 ve 35'te Tarafların bu önlemlerle ilgili olarak farklı uygulama kapsamaları belirlemelerine izin verilmiştir.

254. Bu Bölümün diğer hükümlerinde, yardımlaşma sağlama yükümlülüğünün genel olarak geçerli hukuki yardımlaşma anlaşmaları, yasaları ve düzenlemeleri uyarınca yürütüleceğini açıkça belirtilmektedir. Paragraf 2 uyarınca, anlaşmalar, yasalar ve düzenlemelerde halihazırda bu tür hükümler bulunmuyorsa, Taraflardan her birinin Bölümün kalan kısmında açıklanan spesifik işbirliği biçimlerini yerine getirmek için gerekli hukuki temele sahip olması gerekmektedir. Bu mekanizmaların, özellikle de Madde 29-35'te (Özel hükümler - Başlık 1, 2, 3) belirtilenlerin kullanılabilirliği, bilgisayarla bağlantılı cezai konularda etkili işbirliği için hayati önem taşımaktadır.

255. Taraflardan bazıları, paragraf 2'de söz edilen hükümleri uygulamak için herhangi bir uygulama mevzuatına gerek duymayacaktır; çünkü ayrıntılı yardımlaşma rejimleri tesis eden uluslararası anlaşmaların hükümlerinin kendi kendine uygulamaya konabilir nitelikte olduğu kabul edilmektedir. Bu Bölümde tesis edilen yardımlaşma önlemlerini yürütmek için mevcut yardımlaşma mevzuatı uyarınca halihazırda yeterli esnekliğe sahip olan Tarafların, ya bu hükümleri kendi kendine uygulamaya konabilir

olarak değerlendirmesi ya da bunun için gerekli olabilecek yasaları hızla çıkarması beklenmektedir.

256. Bilgisayar verileri son derece geçici niteliktedir. Birkaç tuşa basılarak ya da otomatik programların çalışması sonucunda veriler silinerek bir suçun failine kadar izlenmesi imkansız hale getirilebilir ya da kritik önemdeki suç delilleri yok edilebilir. Bazı bilgisayar verisi biçimleri kısa süreliğine saklanmakta ve sonra silinmektedir. Bazı durumlarda, deliller hızla toplanmazsa kişiler ve mülkler önemli ölçüde zarar görebilir. Bu tür acil durumlarda, sadece talep değil buna verilen cevap da hızlı bir biçimde gerçekleştirilmelidir. Bu nedenle Paragraf 3'te hedeflenen, yardımlaşma temin etme sürecini hızlandırmayı kolaylaştırarak, yardımlaşma talebi hazırlanıp, iletilip cevaplanmadan önce silindiği için kritik bilgi ya da delillerin kaybolmasını önlemektir. Paragraf 3'te bu, (1) Taraflara, acil işbirliği taleplerini, yazılı, mühürlü belgelerin diplomatların çantalarında ya da posta hizmetlerinde taşındığı, çok daha yavaş olan geleneksel iletimler yerine hızlı iletişim yollarıyla yapma yetkisi verilerek, ve (2) talebin yapıldığı Tarafın bu gibi durumlarda

taleplere cevap vermek için hızlı yolları kullanması şart koşularak gerçekleştirilmektedir. Taraflardan her birinin, yardımlaşma anlaşmaları, yasaları ya da düzenlemeleri halihazırda bunu sağlamıyorsa, bu önlemi uygulama yeterliliğine sahip olması şart koşulmaktadır. Faks ve e-posta adreslerinin listelenmesi bu yeterliliğin göstergesidir. İçinde bulunulan şartlar açısından uygun olabilecek herhangi başka bir hızlı iletişim yolu da kullanılabilir. Teknoloji ilerledikçe, yardımlaşma talebi için kullanılacak başka hızlı iletişim yolları da geliştirilecektir. Paragraftaki güvenlik ve doğruluk şartıyla ilgili olarak, Taraflar kendi aralarında iletişimlerin doğruluğunun nasıl güvence altına alınacağına ve özellikle hassas olan bir durumda özel güvenlik korumalarına (şifreleme dahil olmak üzere) gerek duyulup duyulmadığına karar verebilirler. Son olarak, paragrafta, talebin yapıldığı Tarafın, isterse, hızlı iletimin ardından geleneksel kanallarla resmi bir onayın gönderilmesini şart koşmasına da izin verilmektedir.

257. Paragraf: 4'te yardımlaşmanın geçerli yardımlaşma anlaşmalarının (YA) ve ulusal yasaların hükümlerine tabi olduğu ilkesi ortaya

konmaktadır. Bu rejimler, yardımlaşma talebine konu olabilecek, talebin yapıldığı Taraf Ülkede bulunan kişilerin hakları için önlemler getirmektedir. Örneğin, böyle bir önlem için, talebin yapıldığı Taraf Ülkedeki ulusal bir vakada geçerli olan temel şartlar yerine getirilmedikçe, talebi yapan Taraf adına arama ve el koyma gibi müdahaleci önlemler gerçekleştirilmeyecektir. Taraflar hukuki yardımlaşma yoluyla el konan ve ilgili Tarafa sağlanan eşyalarla ilgili olarak kişilerin haklarının korunmasını da güvence altına alabilirler.

258. Ancak, "bu Bölümde aksi açıkça belirtilen" durumlarda paragraf 4 geçerli olmayacaktır. Bu ifadeyle, Konvansiyonda genel ilkeye istisna oluşturan birçok önemli durum bulunduğunu vurgulamak amaçlanmıştır. Bu tür istisnaların ilki, yardımlaşma anlaşmaları, eşdeğerdeki düzenlemeleri ya da yardımlaşma yasalarının halihazırda bu önlemleri içerip içermediğinden bağımsız olarak bütün Tarafların bu Bölümün diğer Maddelerinde (örneğin koruma, verilerin gerçek zamanlı olarak toplanması, arama ve el koyma ve bir 24/7 ağına sahip olunması) belirtilen işbirliği biçimlerini mümkün kılmalarının şart koşulduğu paragraf 2'de

görülmektedir. Diğer bir istisna, talebi yapan ve talebin yapıldığı Taraflar arasında bir YA ya da eşdeğer bir düzenleme bulunmadığı durumlarda, taleplerin uygulanması için daima talebin yapıldığı Tarafın ulusal mevzuatındaki uluslararası işbirliği ile ilgili hükümlerin yerine geçerli olacak Madde 27'de bulunmaktadır. Madde 27 talebi reddetme için bir şartlar ve gerekçeler sistemi sağlamaktadır. Bu paragrafta özel olarak belirtilen diğer bir istisna, en azından Konvansiyonun 2-11. Maddelerinde tanımlanan suçlarla ilgili olarak, talebin yapıldığı Tarafın talebin "mali" bir suçla ilgili olduğunu düşünmesi gerekçesiyle işbirliğinin reddedilemeyeceğidir. Son olarak, bununla ilgili hakkın saklı tutulmasına izin verilmiş olmakla birlikte, çifte suçluluk gerekçesiyle korumanın reddedilemeyeceğini bildiren Madde 29 da bir istisnadır.

259. Paragraf 5, temel olarak, bu Bölüm çerçevesinde yardımlaşmayla ilgili olarak çifte suçluluk durumunun tanımıdır. Talebin yapıldığı Tarafın çifte suçluluğu yardım sağlamak için bir şart olarak ileri sürmesine izin verildiği durumlarda (örneğin, talebin yapıldığı Tarafın "Saklanan bilgisayar verilerinin hızlı korunması"

başlıklı Madde 29, paragraf 4 uyarınca verilerin korunmasıyla ilgili olarak çifte suçluluğu şart koşma hakkını saklı tuttuğu durumlarda), yardım istenen suça konu olan fiil talebin yapıldığı Tarafın yasaları uyarınca da cezai bir suçsa, bu yasalar suçu başka bir suç kategorisine yerleştiriyor ya da suçu adlandırmak için farklı bir terminoloji kullanıyor olsa bile, çifte suçluluğun geçerli olduğu kabul edilecektir. Talebin yapıldığı Tarafın çifte suçluluğu uygulamak için çok katı bir test benimsememesi için bu hükmün gerekli olduğu düşünülmüştür. Ulusal hukuk sistemlerindeki farklılıklar nedeniyle, terminoloji ve cezai fiillerin kategorilenmesinde farklılıkların yaşanması kaçınılmazdır. Fiil her iki sistem uyarınca da cezai bir ihlal teşkil ediyorsa, bu tür teknik farklılıklar yardımlaşmayı engellememelidir. Çifte suçluluk standardının uygulanabilir olduğu hususlarda bu standart yardımın sağlanmasını kolaylaştıracak esnek bir biçimde uygulanmalıdır.

Madde 26 - Anında İletilen Bilgiler

260. Bu Madde, Suçlardan Elde Edilen Kazançların Aklanma, Aranma, El Konma ve Müsaderesiyle İlgili Konvansiyon'un (ETS No. 141) 10.

Maddesi ve Yolsuzlukla İlgili Ceza Hukuku Konvansiyonu'nun (ETS No. 173) 28 Maddesi gibi geçmiş Avrupa Konseyi araçlarındaki hükümlerden türetilmiştir. Giderek artan bir şekilde, bir Taraf Ülkenin belli bir cezai soruşturma ya da takibatta başka bir Taraf Ülkeye yardımcı olabileceğine inandığı değerli bilgilere sahip olduğu ve soruşturma ya da takibatı yürüten ülkenin bunun varlığını bilmediği durumlar yaşanmaktadır. Bu gibi durumlarda, yardımlaşma talebinin yapılması söz konusu değildir. Paragraf 1'de bilgiye sahip olan ülkeye, bu bilgiyi önceden talep edilmeksizin diğer ülkeye iletme yetkisi verilmektedir. Bu hükmün yararlı olacağı düşünülmüştür; çünkü bazı ülkelerin yasaları uyarınca, talep olmaksızın yardım sağlamak konusunda böyle kesin bir yetkilendirme gerekmektedir. Taraflar, bilgiyi diğer Taraflara anında iletmekle yükümlü değildir; mevcut durumun koşulları ışığında takdir haklarını kullanabilirler. Ayrıca, bilgilerin anında ifşa edilmesi, ifşa eden Tarafın, yargı yetkisine sahipse, ifşa edilen bilgilerle ilgili soruşturma ve takibat yapmasını engellemez.

261. Paragraf 2'de, bazı durumlarda, Tarafların bilgiyi ancak hassas bilgiler gizli tutulacaksa ya da

bilginin kullanımıyla ilgili başka şartlar ileri sürülebilirse anında ileteceği olgusu ele alınmaktadır. Daha özel olarak, gizlilik, bilginin açıklanması durumunda bilgiyi veren ülkenin önemli çıkarlarının tehlikeye gireceği, örneğin bilgi toplama yönteminin niteliğinin ya da bir suç grubu ile ilgili soruşturma yürütüldüğünün gizlenmesine ihtiyaç duyulduğu durumlarda önemli bir husus olarak görülecektir. Daha ayrıntılı bir inceleme, bilgiyi alan Tarafın, bilgiyi veren Tarafça aranan bir şarta uyamayacağını ortaya çıkarırsa (örneğin, bilginin kamuya açık bir duruşmada, delil olarak kullanılması gerekliliğinden ötürü gizlilik şartına uyulamayacaksa), bilgiyi alan Taraf, bilgiyi veren Tarafa bunu bildirecek, bu durumda da bu Taraf bilgiyi vermeme seçeneğine sahip olacaktır. Ancak bilgiyi alan Taraf şartı kabul etmişse sözünde durmalıdır. Bu Madde çerçevesinde getirilen şartların, bilgiyi alan Tarafın yardım talebine karşılık olarak bilgiyi veren Tarafça öne sürülebilecek şartlarla tutarlı olacağı umulmaktadır.

BAŞLIK - 4

***Uluslararası Anlaşmaların Yürürlükte Bulunmadığı
Durumlarda Gelen Yardım Taleplerine
İlişkin Usuller***

**Madde 27 - Uluslararası Anlaşmaların Yürürlükte
Bulunmadığı Durumlarda Gelen Yardım
Taleplerine İlişkin Usuller**

262. Madde 27'de, talebi yapan Tarafla talebin yapıldığı Taraf arasında yürürlükte olan tek taraflı ya da karşılıklı mevzuata dayalı bir yardımlaşma anlaşması ya da düzenlemesi bulunmadığı durumlarda Tarafların belirli yardımlaşma usulleri ve şartlarını uygulamaları şart koşulmaktadır. Dolayısıyla bu Maddeyle yardımlaşmanın, yardımlaşma konusundaki ilgili anlaşmalar ve benzer düzenlemelerin uygulanması yoluyla yürütülmesi gerektiği şeklindeki genel ilke pekiştirilmektedir. Konvansiyonu kaleme alanlar, işbu Konvansiyonda diğer uygulanabilir araçlar ve düzenlemeler yerine uygulanabilecek ayrı bir genel yardımlaşma rejiminin yaratılmasını reddetmişler, bunun yerine genel bir husus olarak mevcut YA rejimlerinin esas alınmasının, bu yolla yardımlaşma icracılarının en iyi

tanıdıkları araç ve düzenlemeleri kullanmalarına izin verilmesinin ve birbirine karşıt rejimlerin tesis edilmesinden doğacak karışıklıktan kaçınılmasının daha pratik olacağına karar vermişlerdir. Daha önce belirtildiği gibi, Tarafların, bu işbirliği türlerini yürütmek için, sadece Madde 29-35'teki (Özel hükümler - Başlık 1, 2, 3) gibi bilgisayarla bağlantılı cezai hususlarda hızlı ve etkili işbirliği için özellikle gerekli mekanizmalarla ilgili olarak, mevcut yardımlaşma anlaşmaları, düzenlemeleri ya da yasalarında halihazırda yoksa- yasal temel tesis etmeleri şart koşulmaktadır.

263. Dolayısıyla, bu Bölüm çerçevesindeki yardımlaşma biçimlerinin çoğunun; bu araçların Tarafları arasında, Avrupa Cezai Konularda Yardımlaşma Konvansiyonu (ETS No. 30) ve Protokolü (ETS No. 99) uyarınca yürütülmesine devam edilecektir. Diğer taraftan, aralarında yürürlükte olan iki taraflı YA'lar ya da cezai durumlarda yardımlaşmayı düzenleyen diğer çok taraflı sözleşmeler (örneğin Avrupa Birliği'ne üye Ülkeler arasındaki anlaşmalar) bulunan işbu Konvansiyona Taraf Ülkeler, bunların yerine bu Maddenin bazı ya da bütün hükümlerini uygulamayı kabul etmedikleri takdirde, bu

sözleşmelerin hükümlerini ve bunlara ek olarak Bölüm III'ün geri kalanında tanımlanan bilgisayar suçları ya da bilgisayarla bağlantılı suçlara özel mekanizmaları uygulamaya devam edeceklerdir. Yardımlaşma, Avrupa Cezai Konularda Yardımlaşma Konvansiyonu tarafından da kabul edilen (Madde 25, paragraf 4) İskandinav ülkeleri arasında ve İngiliz Uluslar Topluluğu üyeleri arasında geliştirilen işbirliği sistemi gibi tek taraflı ya da karşılıklı mevzuata dayalı düzenlemelere de dayandırılabilir. Son olarak, tek taraflı ya da karşılıklı yardımlaşma anlaşmaları ya da düzenlemelerine yapılan atıf işbu Konvansiyonun yürürlüğe giriş tarihinde yürürlükte olan araçlarla sınırlı değildir ve gelecekte benimsenebilecek araçları da içine almaktadır.

264. Madde 27 (Uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen yardım taleplerine ilişkin usuller), paragraf 2-10'da, tek taraflı ya da karşılıklı mevzuata dayalı YA ya da düzenlemelerin yokluğunda yardımlaşmanın gerçekleştirilebilmesini sağlayacak, merkezi yetkili mercilerin tescimi, erteleme ya da reddetme durumlarında şartların, gerekçelerin ve usullerin getirilmesi, taleplerin gizliliği ve doğrudan

doğruya, iletişimler gibi bir dizi kural getirilmiştir. Böyle açık bir biçimde ortaya konan meselelerle ilgili olarak, tek taraflı ya da karşılıklı mevzuata dayalı yardımlaşma sözleşmesi ya da düzenlemelerinin, yokluğunda, yardımlaşmayı düzenleyen, normalde uygulanacak olan ulusal yasalar yerine bu Maddenin hükümleri uygulanacaktır. Madde 27, diğer taraftan, normalde uluslararası yardımlaşmayı düzenleyen ulusal mevzuatta ele alınan diğer konularla ilgili kurallar getirmemektedir. Örneğin, taleplerin biçimi ve içeriği, tanıkların ifadelerinin talebi yapan ya da talebin yapıldığı Taraflarda alınması, resmi ya da ticari kayıtların sağlanması, tanıkların gözetim altında nakledilmesi ya da müsadereyle ilgili konularda yardımlaşma gibi konuların ele alındığı hiçbir hüküm yoktur. Bu konularla ilgili olarak, Madde 25, paragraf 4'te, bu Bölümde açıkça belirtilen durumlar dışındaki durumlarda, bu tür yardım sağlanması ile ilgili spesifik konuların talebi yapan Tarafın yasalarınca düzenleneceği belirtilmiştir.

265. Paragraf 2'de, yardım taleplerini göndermek ve cevaplamaktan sorumlu merkezi bir yetkili merci ya da mercilerin tesisi şart koşulmuştur. Merkezi yetkili mercilerin kurulması cezai konularda

258. *Avrupa Konseyi*
Siber Suçlar Sözleşmesi Taslağı

yardımlaşmayla ilgili modern araçların ortak bir özelliğidir, ve bilgisayar suçları ve bilgisayarla bağlantılı suçlarla mücadelede çok yararlı olan hızlı tepki çeşidini sağlama konusunda özellikle çok yardımcı olmaktadır. İlk olarak, bu tür yetkili merciler arasında doğrudan iletim, diplomatik kanallardan gerçekleştirilen iletimlere göre daha hızlı ve daha etkilidir. Ayrıca, aktif bir merkezi yetkili merci, hem gelen hem de giden taleplerin titizlikle takip edilmesini, ortak çalışılan yabancı icra mercilerine talebin yapıldığı Taraf Ülkede yasal şartların nasıl en iyi şekilde yerine getirileceği konusunda tavsiye verilmesi ve özellikle acil ya da hassas taleplerin uygun şekilde ele alınmasını sağlamakta önemli bir işlevi yerine getirir.

266. Taraflara etkinlik açısından yardımlaşma amacına yönelik tek bir merkezi yetkili merci belirlemeleri tavsiye edilmektedir. Bir Taraf Ülkenin YA'ları ve ulusal yasaları çerçevesinde bu amaç için belirlenen yetkili merciin, bu Madde uygulanabilir olduğunda da merkezi yetkili merci olarak görev yapması genellikle en etkin yol olarak görülmektedir. Ancak, Taraflar, yardımlaşma sistemleri çerçevesinde uygun olduğu durumlarda birden fazla merkezi yetkili

merci belirleme esnekliğine de sahiptir. Birden fazla merkezi yetkili merci belirlendiğinde, bunu yapan Taraf Ülkenin bütün yetkili mercilerin Konvansiyonun hükümlerini aynı şekilde yorumluyor olmasını ve hem gelen hem de giden taleplerin hızlı ve etkin bir biçimde ele alınmasını sağlaması gerekmektedir. Bütün Taraf Ülkeler bu Madde çerçevesinde yardımlaşma taleplerini almak ve cevaplamakla görevlendirilmiş yetkili merci ya da mercilerinin isim ve adreslerini (e-posta ve faks numaraları dahil olmak üzere) Avrupa Konseyi Genel Sekreterine bildirecektir ve Taraflar bu belirlemelerin güncel tutulmasını sağlamak zorundadır.

267. Yardımlaşma talebinde bulunan bir ülke için çoğu zaman temel hedeflerden biri delilin kabul olunabilirliğini düzenleyen ulusal yasalarının gereğinin yerine getirilmiş olmasını ve sonuç olarak delilin mahkemede kullanılabilmesini sağlamaktır. Bu delil şartlarının yerine getirilebilmesi için, paragraf 3'te, talebin yapıldığı Tarafın, yasalarına aykırı olmadıkça, talepleri, talebi yapan Tarafın belirlediği usullere uygun olarak uygulaması şart koşulmuştur. Bu paragrafın sadece teknik usul şartlarıyla ilgili

olduğu, temel usul korumalarıyla ilgili olmadığı özellikle vurgulanmaktadır. Dolayısıyla, örneğin, talebi yapan Taraf, talebin yapıldığı Tarafın bu konuyla ilgili kendi temel yasal şartlarına uymayan bir arama ve el koyma gerçekleştirmesini şart koşamaz. Yükümlülüğün sınırlılığı nedeniyle, talebin yapıldığı Tarafın hukuk sisteminde böyle bir usule yer olmamasının talebi yapan Tarafın talep ettiği usulün uygulanmasının reddedilmesi için yeterli bir gerekçe olamayacağına karar verilmiştir; bunun yerine usul talebin yapıldığı Tarafın hukuk ilkelerine aykırı olması gerekmektedir. Örneğin, talebi yapan Tarafın yasaları çerçevesinde bir tanığın ifadesinin yeminli olarak alınması bir usul şartı olabilir. Talebin yapıldığı Taraf, kendi ulusal yasalarında ifadelerin yeminli olarak alınması şartı olmasa da talebi yapan Tarafın talebine uymalıdır.

268. Paragraf 4'te bu Madde çerçevesinde gerçekleştirilen yardımlaşma taleplerinin reddedilmesinin hangi şartlarda mümkün olacağı açıklanmaktadır. Yardım, devletin egemenliğine, güvenliğe, kamu düzenine ya da diğer temel çıkarlara zarar gelmesini de içeren Madde 25, paragraf 4'te belirlenen (yani talebin yapıldığı

Tarafın yasalarında belirlenen) gerekçelerle, ve suçun talebin yapıldığı Tarafça siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olarak görüldüğü durumlarda reddedilebilir. En geniş işbirliği önlemini sağlama şeklindeki en önemli ilkeye (bkz. Madde 23, 25) uymak amacıyla, talebin yapıldığı Tarafın tesis ettiği reddetme gerekçeleri dar tutulmalı ve ölçülü bir şekilde kullanılmalıdır. Geniş delil ve bilgi kategorilerine karşılık bu gerekçeler, yardımın kategorik olarak reddedilmesi ya da zahmetli şartlara bağlanması potansiyeli yaratacak kadar geniş olmamalıdır.

269. Bu yaklaşıma uygun olarak, Madde 28'de belirlenen gerekçeler dışında, veri koruma gerekçeleriyle yardımın reddedilmesi sadece istisnai durumlarda gerçekleştirilmelidir. Belli bir durumdaki önemli çıkarlar dengelendiğinde (bir tarafta adaletin sağlıklı bir biçimde sağlanmasının da dahil olduğu kamusal çıkarlar, diğer tarafta gizlilikle ilgili çıkarlar) talep edilen spesifik verileri sağlamak talebin yapıldığı Tarafın reddetmeye gerekçe oluşturabilecek temel çıkarları arasına girecek kadar temel güçlükler yaratırsa böyle bir durum ortaya çıkabilir. İşbirliğini reddetmek yönünde veri koruma ilkelerinin geniş, kategorik ya da sistematik bir

uygulamasını benimsemek engellenmektedir. Dolayısıyla, ilgili Tarafların verilerin gizliliğini korumak için farklı sistemleri (örneğin talebi yapan Tarafın uzmanlaşmış bir veri koruma mercisine sahip olmaması) ya da kişisel verileri korumak için farklı yöntemleri (örneğin talebi yapan Tarafın icra mercilerine ulaşan kişisel verilerin gizliliğinin ya da doğruluğunun korunması için silme süreci dışında yöntemler kullanması) benimsemiş olmaları başlı başına reddetme gerekçesi oluşturmaz. Talebin yapıldığı Taraf, işbirliğini* reddetme gerekçesi olarak "temel çıkarlar"a atıfta bulunmadan önce, verilerin transferine izin verecek koşulları sağlamaya çaba göstermelidir (bkz. bu raporda Madde 27, paragraf 6 ve paragraf 271).

270. Paragraf 5'te, taleple ilgili olarak hemen hukuki işlem yapılmasının talebin yapıldığı Taraftaki soruşturma ve takibatlar için zarar verici olduğu durumlarda, talebin yapıldığı Tarafın yardımı ertelemesine -reddetmesine değil- izin verilmektedir. Örneğin, talebi yapan Tarafın soruşturma ya da duruşmada kullanılmak amacıyla delil ya da tanık ifadesi aradığı ve aynı delil ya da tanığın talebin yapıldığı Tarafta başlamak üzere olan bir duruşma için gerekli

olduğu durumlarda, talebin yapıldığı Taraf yardım sağlamayı erteleme hakkına sahiptir.

271. Paragraf 6'da, talep edilen yardımın başka nedenlerle reddedildiği ya da ertelendiği durumlarda, talebin yapıldığı Tarafın şartlara bağlı olarak yardım sağlayabileceği belirtilmektedir. Şartlar talebi yapan Taraf için uygun değilse, talebin yapıldığı Taraf bunlarda değişiklik yapabilir ya da yardımı reddetme ya da erteleme hakkını kullanabilir. Talebin yapıldığı Taraf mümkün olan en geniş yardımı sağlamakla yükümlü olduğu için, hem ret hem de şart ileri sürme haklarının ölçülü bir biçimde kullanılması gerektiğine karar verilmiştir.

272. Paragraf 7'de talebin yapıldığı Tarafa talebin sonucunu talebi yapan Tarafa bildirme ve yardımı reddetme ya da erteleme durumunda bunun nedenlerini açıklama yükümlülüğü getirilmektedir. Nedenlerin açıklanması, başka şeylerin yanı sıra, talebi yapan Tarafın bu Maddedeki şartları talebin yapıldığı Tarafın nasıl yorumladığını anlamsına yardımcı olabilir, gelecekte yardımlaşmanın etkinliğini artırmak için bir istişare temeli oluşturabilir ve talebi yapan Tarafa tanıkların ya da delillerin

ulaşılabilirliği ya da durumu hakkında önceden bilinmeyen olgusal bilgiler sağlayabilir.

273. Bir Tarafın özellikle hassas ya da talebin yapılmasına yol açan olguların zamanından önce kamuya açıklanmasının felakete yol açabileceği vakalar için talepte bulunduğu durumlar olabilir. Paragraf 8'de talebi yapan Tarafın talebin yapıldığının ve içeriğinin gizli tutulmasını talep etmesine izin verilmektedir. Ancak, talebin yapıldığı Tarafın istenen delil ya da bilgileri elde etmesini imkansız kılacaksa, örneğin yardımı yerine getirmek için gereken bir mahkeme emrinin çıkarılması için bilginin ifşa edilmesinin ya da yardımın başarıyla sağlanabilmesi için delile sahip olan özel kişilerin talepten haberdar edilmesinin gerekli olduğu durumlarda gizlilik talep edilemez. Talebin yapıldığı Taraf gizlilik talebini yerine getiremeyecekse bunu talebi yapan Tarafa bildirmeli, böylece talebi yapan Tarafın talebi geri çekme ya da değiştirme konusunda karar verebilmesi sağlanmalıdır.

274. Paragraf 2 uyarınca belirlenen merkezi yetkili merciler birbirleriyle doğrudan doğruya haberleşecektir. Ancak, acil durumlarda, hukuki

yardımlaşma talepleri talebi yapan Tarafın hakim ve savcılar tarafından doğrudan doğruya talebin yapıldığı Tarafın hakim ve savcılarına yapılabilir. Bu usulü izleyen hakim ya da savcı, talebin yapıldığı Tarafın merkezi yetkili merciine iletilmesi amacıyla talebin bir kopyasını kendi merkezi yetkili merciine göndermelidir. Paragrafın b şıkkı uyarınca talepler Interpol aracılığıyla yapılabilir. Kendi yetki sınırlarının dışına çıkan bir talep alan merciler, c şıkkı uyarınca, ikili bir yükümlülük altındadır. İlk olarak, talebi talebin yapıldığı Tarafın yetkili merciine iletmek zorundadır. İkinci olarak, talebi yapan Tarafın yetkili mercilerini bu iletim konusunda bilgilendirmek zorundadır. Paragrafın d şıkkı uyarınca, talebin yapıldığı Tarafın yetkili mercii cebri önlemlere başvurmadan talebi yerine getirebilecek durumdaysa, acil bir durum olmasa da merkezi yetkili mercilerin müdahalesi olmadan talep iletilebilir. Son olarak, e şıkkı, bir Tarafın, taleplerin daha etkin şekilde ele alınabilmesi için, Avrupa Konseyi Genel Sekreteri aracılığıyla, doğrudan iletişimlerin merkezi yetkili mercie iletilmesi gerektiğini diğer Taraflara bildirmesine izin vermektedir.

Madde 28 - Kullanımda Gizlilik ve Sınırlama

275. Bu hükümde, talebin yapıldığı Tarafın bilgi ya da malzemelerin özellikle hassas olduğu durumlarda bunların kullanımlarının yardımın sağlanma nedeniyle sınırlı tutulmasını ya da talebi yapan Tarafın icra görevlilerinin dışında kimseye açıklanmamasını sağlayabilmesi amacıyla bilgi ve malzemelerin kullanımıyla ilgili sınırlamalar getirilmiştir. Bu sınırlamalar, başka şeylerin yanı sıra, verileri koruma amacına yönelik olarak kullanılabilecek önlemler sağlamaktadır.

276. Madde 27 gibi Madde 28 de sadece talebi yapan ve talebin yapıldığı Taraflar arasında yürürlükte bulunan tek taraflı ya da karşılıklı mevzuata dayalı bir yardımlaşma anlaşması ya da düzenlemesinin olmadığı durumlar için geçerlidir. Yürürlükte böyle bir anlaşma ya da düzenlemenin olduğu durumlarda, ilgili Taraflar aksine karar vermedikçe, gizlilik ve kullanım sınırlamalarıyla ilgili olarak, bu Maddenin hükümleri yerine bu anlaşma ya da düzenlemenin hükümleri geçerli olacaktır. Böylece mevcut iki taraflı ya da çok taraflı hukuki yardımlaşma anlaşmaları (YA) ve benzeri

düzenlemelerle iç içe geçme yaşanması önlenmekte ve icracıların aynı alanda geçerli, çelişkili de olabilecek, araçları uygulamaya çalışmak yerine iyi bilinen normal rejim altında çalışmaya devam edebilmeleri sağlanmaktadır.

277. Paragraf 2'de talebin yapıldığı Tarafın bir yardımlaşma talebine cevap verirken iki tür şart ileri sürebilmesine izin verilmektedir. Birincisi, talebin yapıldığı Taraf, gizli bir bilgi kaynağının kimliğinin söz konusu olduğu durumlar gibi, böyle bir şartın yerine getirilmemesi halinde talebe uyulmasının mümkün olmadığı durumlarda, sağlanan bilgi ve malzemelerin gizli tutulmasını talep edebilir. Örneğin delillerin kamuya açık bir duruşmada kullanılması (zorunlu ifşa da dahil olmak üzere) birçok durumda talebi yapan Tarafın suçu başarıyla soruşturmasını ya da kovuşturmasını engelleyeceği için, talebin yapıldığı Tarafın talep edilen yardımı sağlamakla yükümlü olduğu durumlarda mutlak gizliliği şart koşmak uygun değildir.

278. İkincisi, talebin yapıldığı Taraf, bilgi ve malzemelerin sağlanmasını, talepte belirtilenler dışındaki soruşturma ya da takibatlarda kullanılmaması şartına bağlayabilir. Bu şartın

geçerli olabilmesi için, talebin yapıldığı Tarafça, talebi yapan Tarafın bilgi ve malzemeleri başka şekilde kullanımıyla ilgili hiçbir sınırlama olmadığının açıkça belirtilmesi gerekmektedir. Bunun belirtildiği durumlarda, bu şart bilgi ve malzemelerin sadece talepte öngörülen amaçlarla kullanılabilmesini sağlayacak, böylece malzemelerin talebin yapıldığı Tarafın izni olmadan başka amaçlarla kullanılmasını engelleyecektir. Görüşmeciler kullanımı sınırlama yetkisiyle ilgili iki istisnai durumu kabul etmişlerdir ve bu istisnalar paragrafın hükümlerinde zımni olarak mevcuttur. İlk olarak, birçok ülkenin temel hukuk ilkeleri uyarınca, sağlanan malzemeler suçlanan bir kişiyi aklamaya yönelik delillerse, savunmaya ya da adli bir makama ifşa edilmelidir. Ayrıca, yardımlaşma rejimleri çerçevesinde sağlanan malzemelerin çoğunun duruşmalarda, normalde kamuya açık duruşmalarda (cebri ifşa dahil olmak üzere) kullanılması amaçlanmaktadır. Böyle bir ifşa gerçekleştirildiğinde malzeme kamusal alana geçmiş olmaktadır. Böyle durumlarda, yardımlaşmanın istendiği soruşturma ya da takibat için gizliliğin sağlanması mümkün değildir.

279. Paragraf 3'te bilginin iletildiği Taraf istenen şarta uyamıyorsa, bunu bilgiyi sağlayan Tarafa bildirmesi ve bu Tarafın bilgiyi sağlamama seçeneğine sahip olması gerektiği belirtilmektedir. Ancak bilgiyi alan Taraf şartı kabul etmişse, verdiği söze uygun hareket etmelidir.

280. Paragraf 4'te, talebin yapıldığı Tarafın getirdiği şartlara uyulup uyulmadığını görmesi için, talebi yapan Tarafa paragraf 2'de tanımlanan şartlara tabi olarak aldığı bilgi ya da malzemeleri kullanım biçimini açıklama yükümlülüğü getirilebileceği belirtilmektedir. Talebin yapıldığı Tarafın sağladığı malzeme ya da bilginin her kullanıldığında açıklama istemesi gibi aşırı külfetli bir açıklamayı şart koşamayacağı üzerinde anlaşılmıştır.

KISIM - 2
Özel Hükümler

281. Bu Kısımın amacı bilgisayarla bağlantılı suçlar ve elektronik biçimdeki delillerin söz konusu olduğu durumlarda, uluslararası düzeyde birlikte ve etkin bir şekilde eyleme geçilebilmesi için gerekli spesifik mekanizmaları sağlamaktır.

BAŞLIK - I
***Geçici Önlemlerin Alınması Konusunda
Yardımlaşma***

**Madde 29 - Saklanan Bilgisayar Verilerinin
Hızlı Bir Biçimde Korunması**

282. Bu Maddede, Madde 16'da getirilen ulusal düzeydeki mekanizmanın uluslararası düzeydeki eşdeğeri getirilmektedir. Bu Maddenin 1. paragrafında, verileri elde etmek için bir yardımlaşma talebinin hazırlanması, iletilmesi ve uygulanması için gerekli zaman dilimi içerisinde bu verilerin değiştirilmemesi, taşınmaması ve silinmemesini sağlamak üzere talebin yapıldığı Tarafın ulusal sınırları içinde bulunan saklı verilerin bir bilgisayar sistemi aracılığıyla hızlı bir biçimde korunması için Tarafların talepte bulunmasına izin verilmekte, 3. paragrafta Taraflara bunu elde etmek için hukuki yeterliliğe sahip olmaları şartı getirilmektedir. Koruma, geleneksel bir yardımlaşmanın uygulamasından çok daha hızlı gerçekleştirilmesi düşünülen sınırlı ve geçici bir önlemdir. Daha önce belirtildiği gibi bilgisayar verileri son derece geçici niteliktedir. Birkaç tuşa basılarak ya da otomatik programların çalışması sonucunda

veriler silinebilir, değiştirilebilir ya da taşınabilir ve böylece bir suçun failine kadar izlenmesi imkansız hale getirilebilir ya da kritik önemdeki suç delilleri yok edilebilir. Bazı bilgisayar verisi biçimleri sadece kısa süreler için saklanıp sonra silinirler. Dolayısıyla, haftalar ya da aylar sürebilecek resmi bir yardımlaşma talebinin uygulanması esnasında bu verilere ulaşılabilmesini sağlayacak bir mekanizmaya ihtiyaç duyulduğuna karar verilmiştir.

283. Bu önlem, olağan yardımlaşma uygulamasından çok daha hızlı olmasının yanı sıra, aynı zamanda daha az müdahale edicidir. Talebin yapıldığı Tarafın yardımlaşma görevlilerinin verilerin mülkiyetini koruyucusundan almaları gerekli değildir. Tercih edilen usul talebin yapıldığı Tarafın, ileriki bir aşamada verilerin icra görevlilerine teslim edilmesini gerektiren sürecin gerçekleştirilmesi esnasında koruyucunun (genellikle bir hizmet sağlayıcı ya da başka bir üçüncü şahıs) verileri korumasını (yani silmemesini) sağlamasıdır. Bu usulün avantajı hem hızlı hem de, normal yardımlaşma rejimleri uyarınca tam ifşa ölçütleri yerine getirilmeden önce verilerin herhangi bir devlet görevlisine ifşa edilmemesini ya da bu görevlilerce

incelenmemesini sağlaması açısından verilerle ilişkili kişinin gizliliğini, koruyucu nitelikte olmasıdır. Aynı zamanda, talebin yapıldığı Tarafın, verilerin hızlı korunmasını sağlamak üzere, veriler için bir üretim talimatı ya da arama emrinin hızlı bir biçimde çıkarılması ve uygulanması da dahil olmak üzere, başka usuller kullanmasına izin verilmiştir. Başlıca şart, verilerin geri getirilemez bir biçimde yok olmasını önlemek için son derece hızlı bir sürecin mevcut olmasıdır.

284. Paragraf 2'de bu Madde uyarınca yapılacak koruma taleplerinin içeriği belirtilmiştir. Bunun geçici bir önlem olduğu ve talebin hızlı bir biçimde hazırlanıp iletilmesi gerektiği göz önünde bulundurularak, bilgiler özet şeklinde sunulmalı ve sadece verilerin korunmasını sağlamak için gerekli asgari bilgiyi içermelidir. Talepte, verilerin korunmasını isteyen merci ve önlemin alınmasının istenmesine yol açan suçun belirtilmesinin yanı sıra, olguların bir özeti, korunacak verilerin ve bulundukları yerin belirlenmesi için yeterli bilgi ve verilerin elde edilmesinin ilgili suçun soruşturulması ya da kovuşturulması açısından anlamlı ve verilerin korunmasının gerekli olduğunu gösteren

açıklamalar yer almalıdır. Son olarak, talebi yapan Taraf verilerin üretimini sağlamak için daha sonra bir yardım talebinde bulunacağını taahhüt etmelidir.

285. Paragraf 3'te çifte suçluluğun koruma sağlamak için bir şart olarak ileri sürülemeyeceği ilkesi ortaya konmaktadır. Genel olarak, çifte suçluluk ilkesinin uygulanması, koruma bağlamında engelleyicidir. İlk olarak, bir modern yardımlaşma uygulaması meselesi olarak, arama ve el koyma ya da müdahale gibi usulle ilgili en özel hayata müdahale edici önlemler dışında bütün önlemler için çifte suçluluğu kaldırmak yönünde bir trend vardır. Koruma, Konvansiyonu kaleme alanların görüşüne göre, özellikle müdahale edici nitelikte değildir; çünkü koruyucu sadece yasal olarak mülkiyetinde bulundurmaya sürdürmektedir ve verilerin ifşasının istendiği resmi bir yardımlaşma talebinin uygulanmasına kadar veriler talebin yapıldığı Tarafın görevlilerine ifşa edilmemekte ve bu görevlilerce incelenmemektedir. İkinci olarak, uygulama açısından, çoğu zaman çifte suçluluğun varlığını kesin olarak belirlemek için gerekli açıklamaları sağlamak o kadar uzun sürmektedir ki bu arada veriler silinebilmekte,

taşınabilmekte ya da değiştirilebilmektedir. Örneğin, bir soruşturmanın ilk aşamalarında, talebi yapan Taraf ulusal sınırları içinde bir bilgisayara izinsiz girildiğinin farkında olabilir ama hasarın niteliği ve boyutlarını tam olarak anlaması zaman alabilir. Talebin yapıldığı Taraf, çifte suçluluğun kesin olarak belirlenmesi sürecinde izinsiz girişin kaynağının bulunabilmesini sağlayacak trafik verilerini korumayı geciktirirse, kritik önemdeki veriler iletim yapıldıktan sonra bu verileri sadece birkaç saat ya da gün tutan hizmet sağlayıcılar tarafından rutin bir işlem olarak silinecektir. Talebi yapan Taraf daha sonra çifte suçluluğu tesis edebilse bile, önemli trafik verileri kurtarılamayacak ve suçun faili hiçbir zaman teşhis edilemeyecektir.

286. Dolayısıyla, genel kural Tarafların koruma amacıyla herhangi bir çifte suçluluk şartından vazgeçmeleri gerektiğidir. Ancak, paragraf 4 çerçevesinde hakkın sınırlı bir biçimde saklı tutulması mümkündür. Taraflardan biri verilerin üretimine yönelik bir yardım talebine cevap vermek için çifte suçluluğu bir şart olarak ileri sürerse ve ifşa zamanında çifte suçluluk şartının karşılanmadığına inanmak için nedenler

mevcutsa, korumanın önkoşulu olarak çifte suçluluğu şart koşma hakkını saklı tutabilir. Madde 2 ile 11 uyarınca tesis edilen suçlarla ilgili olarak, Konvansiyonda izin verilen suçlar için hakların saklı tutulabilmesi hakkına tabi olmak şartıyla, Taraflar arasında çifte suçluluk şartının otomatik olarak karşılandığı varsayılacaktır. Dolayısıyla, Taraflar bu şartı sadece Konvansiyonda tanımlananlar dışındaki suçlarla ilgili olarak getirebilirler.

287. Bunun dışındaki durumlarda, paragraf 5 uyarınca, talebin yapıldığı Taraf bir koruma talebini ancak bu talebin uygulanmasının egemenliğine, güvenliğine, kamu düzenine ya da diğer temel çıkarlarına zarar verici olduğu, ya da suçun siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olduğunu düşündüğü durumlarda reddedebilir. Bu önlemin bilgisayar suçları ya da bilgisayarla bağlantılı suçların etkin bir biçimde soruşturulması ve kovuşturulması için merkezi bir önemde olmasından dolayı, koruma talebinin başka bir temele bağlı olarak reddedilmesi önlenmiştir.

288. Bazen, talebin yapıldığı Taraf verilerin koruyucusunun talebi yapan Tarafın

soruşturmasının gizliliğini tehdit edecek ya da başka bir biçimde bu soruşturmaya zarar verecek bir eylemde bulunabileceğini fark edebilir (örneğin, korunacak verileri tutan hizmet sağlayıcının bir suç grubu ya da bizzat soruşturmanın hedefi tarafından kontrol edildiği durumlarda). Bu gibi durumlarda, paragraf 6 uyarınca, koruma talebini sürdürmenin yaratacağı riski almak ya da üretim ya da arama ve el koyma gibi daha müdahaleci ama daha güvenli bir yardımlaşma biçimini aramak seçeneklerini değerlendirebilmesi için talebi yapan Taraf derhal bilgilendirilmelidir.

289. Son olarak, paragraf 7'de, Tarafların bu Madde uyarınca korunan verilerin, ifşalarının istendiği resmi bir yardımlaşma talebinin alınması sırasında en az 60 gün tutulmasını ve talebin alınmasından sonra da tutulmaya devam edilmesini sağlamaları şart koşulmaktadır.

Madde 30 - Korunan Trafik Verilerinin Hızlı Bir Biçimde İfşası

290. Bu Maddede, Madde 17'de ulusal düzeyde tesis edilen yetkinin uluslararası düzeydeki eşdeğeri tesis edilmektedir. Suçun işlendiği Taraf Ülkenin

talebi üzerine, talebin yapıldığı Taraf, iletimi kaynağına kadar izleyerek suçun failini bulmak ve kritik delillerin yerini belirlemek üzere kendi bilgisayarları aracılığıyla gerçekleştirilen bir iletimle ilgili trafik verilerini koruyacaktır. Böylece talebin yapıldığı Taraf kendi ulusal sınırları içinde bulunan trafik verilerinin iletimin üçüncü bir ülkedeki ya da talebi yapan Taraftaki bir hizmet sağlayıcıdan kaynaklandığını gösterdiğini keşfedebilir. Bu tür durumlarda, talebin yapıldığı Taraf, talebi yapan Tarafa diğer Ülkedeki hizmet sağlayıcının kimliğini ve bu Ülkeden yapılan iletişimin izlediği yolu belirlemeye yetecek miktarda trafik verisini hızlı bir biçimde sunmak zorundadır. İletim üçüncü bir Ülkeden geliyorsa, bu bilgi, talebi yapan Tarafın bu ülkeye koruma ve iletimi nihai kaynağına kadar izlemek üzere hızlı yardımlaşma talebinde bulunmasını sağlayacaktır. İletim kendisine geri dönmüşse, talebi yapan Taraf ulusal süreçler yoluyla koruma ve başka trafik verilerinin ifşasını temin edebilecektir.

291. Paragraf 2 uyarınca, talebin yapıldığı Taraf trafik verilerini ifşa etmeyi ancak ifşanın egemenliğine, güvenliğine, kamu düzenine ya da diğer temel çıkarlarına zarar verici olduğu, ya da suçun

siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olduğunu düşündüğü durumlarda reddedebilir. Madde 29'da olduğu gibi (Saklanan bilgisayar verilerinin hızlı bir biçimde korunması), bu tür bilgilerin bu Konvansiyon kapsamında suç işleyenleri ya da kritik delillerin yerini saptamak için çok önemli olmasından dolayı, reddetme gerekçeleri sıkı bir biçimde sınırlandırılacaktır ve yardımı reddetmek için başka temellerin ileri sürülmesinin önlenmesine karar verilmiştir.

BAŞLIK - 2
Soruşturma Yetkileri Konusunda
Yardımlaşma

Madde 31 - Saklanan Bilgisayar Verilerine
Erişilmesine İlişkin Yardımlaşma

292. Taraflar, Madde 19 (Saklanan bilgisayar verilerinin aranması ve bunlara el konması) uyarınca ulusal düzeydeki amaçlar için olduğu gibi, başka bir Taraf Ülkenin yararına olarak da, kendi ulusal sınırları içindeki bir bilgisayar sistemi aracılığıyla saklanan verileri arama ya da bunlara benzer şekilde erişme, el koyma ya da bunları benzer şekilde güven altına alma ve ifşa etme yeterliliğine sahip olmalıdır. Paragraf 1'de Tarafların bu tür yardım talebinde bulunmalarına izin verilmiştir ve paragraf 2'de talebin yapıldığı Tarafın bunu sağlayabilecek durumda olması şart koşulmuştur. Paragraf 2'de bu tür işbirliğini sağlamak için geçerli hüküm ve şartların cezai meselelerde hukuki yardımlaşmayı düzenleyen geçerli anlaşma, düzenleme ve ulusal yasalarda belirtilenler olması gerektiği ilkesine de uyulmuştur. Paragraf 3 uyarınca, böyle bir talebe (1) ilgili verilerin kaybolma ya da değiştirilmeye açık olduğuna inanmak için

gerekçelerin mevcut olduğu, ya da (2) anlaşma, düzenleme ya da yasaların gerektirdiği durumlarda hızlı bir biçimde cevap verilmelidir.

**Madde 32 - Saklanan Bilgisayar Verilerine İzinli
Şekilde ya da Bu Verilerin Halka Açık
Olduğu Durumlarda Sınır Ötesinden
Erişim Sağlamak**

293. Tarafların ne zaman yardım talebinde bulunmaksızın başka bir Taraf Ülkede saklanan bilgisayar verilerine tek taraflı olarak erişmelerine izin verilebileceği konusu Konvansiyonu kaleme alanlarca ayrıntılı bir biçimde tartışılmıştır. Ülkelerin tek taraflı hareket etmelerinin kabul edilebilir olduğu ve olmadığı durumlar ayrıntılı bir biçimde ele alınmıştır. Sonuçta Konvansiyonu kaleme alanlar bu alanı düzenleyen kapsamlı, hukuki açıdan bağlayıcı bir rejim hazırlamanın henüz mümkün olmadığına karar vermişlerdir. Bu, kısmen; bugüne kadar bu durumlarla ilgili somut deneyimler yaşanmamasından ve kısmen uygun çözümün çoğu zaman tam olarak tekil durumlardaki koşullara bağlı olmasından, dolayısıyla genel kurallar formüle etmenin güçlüğünden kaynaklanmaktadır. Sonuçta Konvansiyonu kaleme alanlar, Madde 32'de,

herkesin tek taraflı hareket etmenin mümkün olduğunda anlaştığı durumların belirtilmesiyle yetinilmesine karar vermişlerdir. Daha fazla deneyimin sahip olunduğu ve bu deneyimler ışığında daha fazla tartışmanın yapıldığı bir zamana kadar diğer durumların düzenlenmemesi kararlaştırılmıştır. Buna uygun olarak, Madde 39, paragraf 3'te diğer durumlara ne izin verildiği ne de bunların engellendiği belirtilmiştir.

294. Madde 32'de (Saklanan bilgisayar verilerine izinli şekilde ya da bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlamak) iki durum ele alınmıştır: ilk olarak, erişilen verilerin kamuya açık olduğu, ve ikinci olarak, bir Tarafın kendi sınırları içerisindeki bir bilgisayar sistemini kullanarak ulusal sınırları dışında bulunan verilere eriştiği ya da bu verileri aldığı, ve bu sistem aracılığıyla verileri bu Tarafa ifşa etmeye yasalar uyarınca yetkili bir kişinin yasalara uygun ve gönüllü olarak rızasını aldığı durumlar. Verileri ifşa etmek için "yasalar uyarınca yetkili" kişinin kim olduğu, koşullara, kişinin niteliğine ve durum için geçerli yasaya bağlı olarak farklılık gösterebilir. Örneğin, bir kişinin e-postası bir hizmet sağlayıcı tarafından başka bir ülkede

saklanabilir ya da bir kişi kasıtlı olarak başka bir ülkede veri saklayabilir. Maddede belirtildiği gibi, bu kişiler verileri tekrar kazanabilirler ve, yasalara uygun olarak yetki sahibi olmaları koşuluyla, gönüllü olarak verileri icra görevlilerine ifşa edebilir ya da bu görevlilerin verilere erişmelerine izin verebilirler.

**Madde 33 - Trafik Verilerinin Gerçek Zamanlı
Olarak Toplanması Konusunda
Yardımlaşma**

295. Çoğu durumda, temel önemdeki trafik verileri iletim zincirindeki bir hizmet sağlayıcı tarafından korunmadan önce otomatik olarak silindiği için, soruşturmayı yürütenler önceki iletimlerin izini sürerek bir iletişimi kaynağına kadar izleyebileceklerinden emin olamazlar. Bu nedenle, bütün Taraf Ülkelerdeki soruşturma yürüten merciler için diğer Taraf Ülkelerde bilgisayar sistemleri aracılığıyla iletilen iletişimlerle ilgili trafik verilerini gerçek zamanlı olarak elde etme yeterliliği önemlidir. Dolayısıyla, Madde 33 (Trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma) uyarınca, bütün Taraflar, diğer Taraflar için trafik verilerini gerçek zamanlı

olarak toplamakla yükümlüdür. Bu Madde Tarafların bu konularda işbirliğine gitmesini şart koşmakla birlikte, diğer hususlarda olduğu gibi burada da mevcut yardımlaşma biçimlerine saygı gösterilmektedir. Dolayısıyla bu işbirliğinin sağlanmasında geçerli olacak hükümler ve şartlar, genellikle cezai konularda hukuki yardımlaşmayı düzenleyen geçerli anlaşmalar, düzenlemeler ve yasalarda belirtilen hükümler ve şartlardır.

296. Çoğu ülkede, trafik verilerinin gerçek zamanlı olarak toplanmasıyla ilgili olarak geniş kapsamlı bir yardım sağlanmaktadır; çünkü bu tür bir toplama hem içerik verilerine müdahaleden hem de arama ve el koymadan daha az müdahaleci bir önlem olarak görülmektedir. Ancak, bazı ülkeler daha dar bir yaklaşım benimsemiştir. Buna uygun olarak, eşdeğer ulusal önlemlerin kapsamıyla ilgili olarak Madde 14 (Usul hükümlerinin kapsamı), paragraf 3 uyarınca haklarını saklı tutmayı seçebildikleri gibi, paragraf 2'de de Tarafların bu önlemin uygulama kapsamını Madde 23'te (Uluslararası işbirliğine ilişkin genel ilkeler) belirtilenlerden daha dar bir suç grubuyla sınırlamalarına izin verilmiştir. Bir ikaz söz konusudur: suç grubu

eşdeğer ulusal bir davada böyle bir önlemin geçerli olduğu bir suç grubundan daha dar olamaz. Trafik verilerinin gerçek zamanlı olarak toplanması bazen bir suçun failinin kesin olarak teşhis edilmesinin tek yolu olduğu ve bu önlem daha az müdahale edici nitelikte olduğu için, paragraf 2'deki "en azından" ifadesinin Tarafları mümkün olan en geniş yardıma, yani çifte suçluluğun bile olmadığı bir durumda yardımlaşmaya izin vermeye teşvik etmesi amaçlanmıştır.

Madde 34 - İçerikle İlgili Verilere Müdahale Edilmesi Konusunda Yardımlaşma

297. Müdahalenin özel hayata müdahale edici niteliği yüzünden, içerik verilerine müdahale için yardımlaşma sağlama yükümlülüğü sınırlandırılmıştır. Yardım Tarafların geçerli anlaşma ve yasalarının izin verdiği ölçüde sağlanacaktır. İçerik verilerine müdahale konusunda işbirliğinin sağlanması yardımlaşma uygulamasının yeni şekillenmekte olan bir alanı olduğu için yardım sağlama yükümlülüğünün kapsamı ve sınırları konusunda mevcut yardımlaşma rejimlerine ve ulusal yasalara uyulmasına karar verilmiştir. Bu nedenle,

telekomünikasyonlara müdahale için sorgulama müzekkereleriyle ilgili olarak Avrupa Cezai Konularda Yardımlaşma Konvansiyonu'nun pratikte uygulanması konusunda Madde 14, 15 ve 21'deki değerlendirmelere ve No R (85) 10'a atıfta bulunulmuştur.

BAŞLIK - 3

24/7 Ağı

Madde 35 - 24/7 Ağı

298. Daha önce açıkladığı gibi, bilgisayar sistemi kullanılarak işlenen suçlarla etkin biçimde mücadele etmek ve elektronik biçimdeki delillerin etkin biçimde toplanması çok çabuk karşılık vermeyi gerektirir. Ayrıca, dünyanın bir noktasında birkaç tuşa basılarak gerçekleştirilen eylemin sonuçları aynı anda binlerce kilometre ve birkaç saat dilimi uzakta yaşanabilir. Bu nedenle, bilgisayar çağının tehditlerine etkin bir biçimde cevap verebilmek için mevcut polis işbirliği ve yardımlaşma biçimlerine yeni kanalların eklenmesi gerekmektedir. Bu Maddede tesis edilen kanal, G8 grubu ülkelerin himayesinde yaratılmış, halen faaliyette olan bir ağ sayesinde kazanılmış deneyime dayanmaktadır. Bu Madde uyarınca, bütün Taraflar, bu Bölüm kapsamındaki, özellikle Madde 35, paragraf 1, şık a ve c'de tanımlanmış soruşturma ve takibatlarda acil yardım sağlayacak, günde 24 saat, haftada 7 gün ulaşılabilen bir irtibat noktası belirlemek zorundadır. Bu ağın kurulmasının, bu

Konvansiyonda belirtilen, Tarafların bilgisayar suçları ve bilgisayarla bağlantılı suçların yarattığı icrayla ilgili tehditlere etkin bir biçimde cevap vermelerini sağlayan en önemli yollardan biri olduğuna karar verilmiştir.

299. Bütün Taraf Ülkelerin 24/7 irtibat noktaları, başka şeylerin yanı sıra, teknik danışmanlık, verilerin korunması, delil toplanması, hukuki bilgilerin verilmesi ve şüphelilerin yerinin tespit edilmesi işlemlerini kolaylaştıracak ya da doğrudan yerine getirecektir. Paragraf 1'deki "yasal bilgi" terimi, gayriresmi ya da resmi işbirliği sağlamak için gereken herhangi bir önkoşul için işbirliği isteyen başka bir Taraf Ülkeye verilecek danışmanlık anlamındadır.

300. Taraflar irtibat noktasını kendi icra yapılarının neresine yerleştireceklerini belirlemek konusunda özgürdür. Bazı Taraf Ülkeler 24/7 irtibat noktasını yardımlaşmayla ilgilenen merkezi yetkili merciine yerleştirmek isteyebilir, bazı Ülkeler en iyi noktanın bilgisayar suçları ve bilgisayarla bağlantılı suçlarla mücadele konusunda uzmanlaşmış bir polis birimi olduğuna inanabilir, bazı Ülkeler içinse devlet yapıları ve hukuk sistemleri açısından başka

seçenekler uygun olabilir. 24/7 irtibat noktası hem bir saldırıyı durdurma ve izlemeye yönelik teknik danışmanlık sağlayacağı hem de şüphelilerin yerinin saptanması gibi uluslararası işbirliği görevlerini yerine getireceği için tek bir doğru cevap yoktur ve ağın yapısının zamanla gelişmesi beklenmektedir. Ulusal irtibat noktası belirlenirken, başka dillerin kullanıldığı irtibat noktalarıyla iletişim sağlanması ihtiyacı da göz önünde bulundurulmalıdır.

301. Paragraf 2'de, 24/7 irtibat noktalarının yerine getireceği kritik görevler arasında doğrudan yerine getirmeyeceği işlevlerin hızlı bir biçimde gerçekleştirilmesini kolaylaştırmanın da bulunduğu belirtilmektedir. Örneğin, Taraflardan birinin 24/7 irtibat noktası polis biriminin parçasıysa, günün ya da gecenin herhangi bir saatinde gerekli işlemin yapılabilmesi için, uluslararası iade ya da yardımlaşmayla ilgilenen merkezi yetkili merci gibi kendi devlet yapısı içindeki ilgili birimlerle hızlı bir biçimde işbirliğine gidebilecek durumda olmalıdır. Ayrıca, paragraf 2'de bütün Taraf Ülkelerin 24/7 irtibat noktalarının ağın diğer üyeleriyle iletişimleri hızlı bir biçimde

yürütebilecek kapasitede olması şart koşulmuştur.

302. Paragraf 3'te ağdaki bütün irtibat noktalarının uygun teçhizata sahip olması şart koşulmaktadır. Ağın düzgün işleyebilmesi için en gelişmiş telefon, faks ve bilgisayar teçhizatı temel önemdedir ve teknoloji geliştikçe diğer iletişim biçimleri ve analitik teçhizatın sistemin bir parçası haline gelmesi gerekecektir. Paragraf 3'te Taraf Ülkenin ağ ekibini oluşturan personelin bilgisayar suçları ve bilgisayarla bağlantılı suçlar ile bunlara nasıl etkin bir biçimde karşılık verileceği konusunda gerekli eğitimi almış olması da şart koşulmaktadır.

BÖLÜM - IV

Diğer Hükümler

303. Bazı istisnalar olmakla birlikte, bu Bölümün hükümleri büyük ölçüde, Şubat 1980'deki Vekillerin 315. toplantısında Bakanlar Kurulu tarafından onaylanan "Avrupa Konseyi'nde akdedilmiş konvansiyon ve sözleşmeler için bitiş cümleleri modelleri"ne dayanmaktadır. Madde 36 ila 48'in büyük bir bölümünde cümle modellerinin standart dili kullanıldığı ya da Avrupa Konseyi'ndeki uzun bir geçmişe sahip anlaşma yapma uygulamaları esas alındığı için, bu maddelerle ilgili spesifik değerlendirmeler yapmak gerekmemektedir. Ancak, standart cümle modellerinde yapılan belirli değişiklikler ya da bazı yeni hükümlerin bir parça açıklanmasına gerek duyulmaktadır. Bu bağlamda cümle modellerinin bağlayıcı olmayan bir hükümler grubu olarak benimsendiği göz önüne alınmıştır. Cümle Modellerinin girişinde belirtildiği gibi "bitiş cümlesi modelleriyle sadece uzman komitelerinin işlerinin kolaylaştırılması ve metinler arasındaki gerçek bir nedenden kaynaklanmayan farklılıklardan kaçınılması amaçlanmıştır. Modeller hiçbir şekilde bağlayıcı

değildir ve farklı cümleler belli durumlara uyacak şekilde uyarlanabilir."

Madde 36 - İmza ve Yürürlük

304. Madde 36, paragraf 1, Avrupa Konseyi çerçevesinde geliştirilmiş, yürürlüğe girmeden önce hem Avrupa Konseyi'ne üye ülkelerin hem de hazırlanmasına katkıda bulunmuş üye olmayan ülkelerin imzasına açık olan, Hükümlülerin Nakli Konvansiyonu (ETS No. 112) ve Suçlardan Elde Edilen Kazançların Aklanma, Aranma, El Konma ve Müsaderesiyle İlgili Konvansiyon (ETS No. 141) gibi başka konvansiyonlarda tesis edilmiş çeşitli emsallere uygun olarak kaleme alınmıştır. Hükümde, sadece Avrupa Konseyi üyelerinin değil ilgi gösteren azami sayıda ülkenin mümkün olduğunca kısa sürede Taraf olmasının sağlanması amaçlanmıştır. Hükmün, Konvansiyonun geliştirilmesine aktif olarak katılmış, üye olmayan dört ülke, Kanada, Japonya, Güney Afrika ve Amerika Birleşik Devletleri için geçerli olması hedeflenmektedir. Konvansiyon paragraf 3 uyarınca yürürlüğe girince, bu hükmün kapsamına girmeyen diğer üye olmayan ülkeler Madde 37, paragraf 1'e

uygun olarak Konvansiyona katılmaya davet edilebilir.

305. Madde 36, paragraf 3'te, Konvansiyonun yürürlüğe girmesi için gerekli tasdik, kabul ve onay sayısı 5 olarak belirtilmektedir. Bu sayı Avrupa Konseyi anlaşmalarındaki olağan eşikten (3) yüksektir ve uluslararası bilgisayar suçları ve bilgisayarla bağlantılı suçlar tehdidinin ele alınmasının başarıyla başlatılması için biraz daha büyük bir ülkeler grubuna ihtiyaç duyulduğu inancını yansıtmaktadır. Ancak Konvansiyonun yürürlüğe girmesini gereksiz şekilde geciktirmemek için sayının çok yüksek tutulmasından da kaçınılmıştır. İlk beş ülkeden en az üçü Avrupa Konseyi üyesi olmalıdır ve diğer iki ülke Konvansiyonun geliştirilmesine katkıda bulunmuş üye olmayan dört ülke arasından seçilebilir. Bu hükümde, şüphesiz, Konvansiyonun beş Avrupa Konseyi üyesi ülkenin kabulüne dayalı olarak yürürlüğe girmesine de izin verilmektedir.

Madde 37 - Konvansiyona Katılım

306. Madde 37 de diğer Avrupa Konseyi konvansiyonlarında tesis edilen emsallere uygun olarak kaleme alınmıştır; ama bazı ilave sarih

unsurlar içermektedir. Bakanlar Kurulu, uzun bir geçmişe sahip uygulamalar uyarınca, kendi inisiyatifiyle ya da talep üzerine, bir konvansiyonun geliştirilmesine katkıda bulunmamış olan üye olmayan bir ülkeyi, üye olsun olmasın konvansiyonu imzalamış olan bütün Taraflara danıştıktan sonra, konvansiyona katılmaya davet edebilir. Dolayısıyla imza sahibi Taraflardan herhangi birisi üye olmayan bir Ülkenin katılımına itiraz ederse Bakanlar Kurulu genellikle bu ülkeyi konvansiyona katılmaya davet etmez. Ancak, normal düzenleme uyarınca, Bakanlar Kurulu -teorik olarak- üye olmayan bir Taraf Ülke katılımına itiraz etse dahi üye olmayan Ülkeyi konvansiyona katılmaya davet eder. Bu, -teorik olarak- Avrupa Konseyi anlaşmalarını diğer üye olmayan Ülkelere genişletme sürecinde üye olmayan Ülkelere genellikle veto hakkı tanınmadığı anlamına gelmektedir. Ancak, Bakanlar Kurulunun üye olmayan bir Ülkeyi Konvansiyona katılmaya davet etmeden önce bütün İmza Sahibi Ülkelere -sadece Avrupa Konseyi üyelerinin değil- danışması ve bütün Ülkelerin onayını alması şeklinde sarıh bir şart eklenmiştir. Yukarıda belirtildiği gibi, böyle bir şart uygulamayla tutarlıdır ve Konvansiyonda İmzası bulunan

bütün Ülkelerin hangi üye olmayan Ülkelerle anlaşma ilişkilerine gireceklerine karar verme hakkına sahip olmaları gerektiği gerçeğini yansıtmaktadır. Ancak, üye olmayan bir Ülkeyi katılıma davet etme yönünde resmi karar, normal uygulama uyarınca, imza sahibi Tarafların Bakanlar Kurulunda yer alma hakkına sahip temsilcileri tarafından alınacaktır. Bu karar Avrupa Konseyi Yasasının 20.d sayılı Maddesinde belirtilen üçte iki çoğunluğu ve imza sahibi Tarafların Kurulda yer alma hakkına sahip temsilcilerinin oybirliğini gerektirmektedir.

307. Konvansiyona katılmak ve Madde 41 uyarınca bir beyanda bulunmak isteyen federal Ülkelerin, önceden Madde 41, paragraf 3'te söz edilen bildirinin bir taslağını sunmaları ve böylece Tarafların federal ülkelerle ilgili hükmün uygulanmasının müstakbel Tarafın Konvansiyonu uygulamasını nasıl etkileyeceğini değerlendirebilmelerini sağlamaları gerekmektedir (bkz. paragraf 320).]

Madde 39 - Konvansiyonun Sonuçları

308. Madde 39, paragraf 1 ve 2'de Konvansiyonun diğer uluslararası sözleşme ve düzenlemelerle ilişkisi ele alınmaktadır. Avrupa Konseyi

konvansiyonlarının birbirleriyle ve Avrupa Konseyi dışında yapılmış iki ya da çok taraflı başka anlaşmalarla nasıl ilişkilendirileceği yukarıda söz edilen Cümle Modellerinde ele alınmamıştır. Avrupa Konseyi'nin ceza hukuku alanındaki konvansiyonlarında genelde kullanılan yaklaşım şöyledir (örneğin, Denizyoluyla Yasadışı Ticaretle İlgili Sözleşme (ETS No 156)): (1) Yeni konvansiyonlar özel meselelerle ilgili uluslararası çok taraflı konvansiyonlardan kaynaklanan hak ve taahhütleri etkilemeyecektir; (2) Yeni bir konvansiyonun Tarafları, konvansiyonun hükümlerine eklemeler yapmak ya da bu hükümleri güçlendirmek ya da konvansiyonda yer alan ilkelerin uygulamasını kolaylaştırmak amacıyla aynı konularla ilgili olarak birbirleriyle iki ya da çok taraflı sözleşmeler yapabilirler; ve (3) yeni bir konvansiyonun iki ya da daha fazla Tarafı konvansiyonda ele alınan bir konuyla ilgili olarak halihazırda bir sözleşme ya da anlaşma imzalamış ya da bu konuyla ilgili olarak ilişkilerini başka bir biçimde tesis etmiş durumdalarsa, uluslararası işbirliğini kolaylaştırıyor olması şartıyla, yeni konvansiyon yerine bu sözleşme ya da anlaşmayı uygulama ya

da bu ilişkilerini buna uygun olarak düzenleme hakkına sahip olacaklardır.

309. Konvansiyonda genel olarak Taraflar arasındaki çok taraflı ve ikili sözleşme ve anlaşmaların yerine geçmek yerine bunları tamamlamak amaçlandığı için, Konvansiyonu kaleme alanlar "özel konular"a yapılan, sınırlayıcı nitelikte olabilecek atfın öğretici olacağına inanmamaktadırlar ve gereksiz bir karışıklığa yol açabileceğinden endişe etmişlerdir. Bunun yerine, Madde 39 paragraf 1'de bu Konvansiyonun Taraflar arasındaki diğer geçerli anlaşma ve sözleşmeleri desteklediği belirtilmekle yetinilmiş ve örnek olarak bütünü kapsamayan üç Avrupa Konseyi anlaşması anılmıştır: 1957 Avrupa İade Konvansiyonu (ETS No. 24), 1959 Avrupa Cezai Konularda Yardımlaşma Konvansiyonu (ETS No. 30) ve 1978 Ek Protokol (ETS No 99). Dolayısıyla, genel konularla ilgili olarak, bu sözleşme ve düzenlemeler ilke olarak siber suç Konvansiyonuna Taraf Ülkelerce uygulanmalıdır. Sadece bu Konvansiyonda ele alınan özel konularla ilgili olarak, lex specialis derogat legi generali yorumlama kuralı Tarafların bu Konvansiyonda içerilen kurallara öncelik

vermesini gerektirir. Örnek olarak belirli bir iletişimin izlediği yolu belirlemek için gerekli olduğunda korunan trafik verilerinin hızlı bir biçimde ifşasını öngören Madde 30 gösterilebilir. Bu spesifik alanda, daha genel olan yardımlaşma sözleşmelerinden önce lex specialis olan Konvansiyona başvurulmalıdır.

310. Benzer şekilde, Konvansiyonu kaleme alanlar, mevcut ya da gelecekte yapılacak sözleşmelerin uygulanmasını işbirliğini "güçlendirme"ye ya da "kolaylaştırma"ya bağlayan ifadelerin sorun yaratabileceğini düşünmüşlerdir; çünkü uluslararası işbirliği Bölümünde tesis edilen yaklaşım uyarınca Tarafların ilgili uluslararası sözleşme ve düzenlemeleri uygulayacakları varsayılmaktadır.

311. İşbirliğine temel oluşturan bir yardımlaşma anlaşması ya da sözleşmesinin olduğu durumlarda bu Konvansiyon sadece gerekli olduğu durumlarda mevcut kuralları destekleyecektir. Örneğin, orijinal anlaşma ya da düzenleme çerçevesinde böyle bir imkan yoksa bu Konvansiyon yardımlaşma taleplerinin hızlı iletişim yöntemleriyle iletilmesini (bkz. Madde 25, paragraf 3) sağlayacaktır.

312: Konvansiyonun destekleyici niteliği ve özellikle de uluslararası işbirliğine yaklaşımına uygun olarak, paragraf 2'de Tarafların halen yürürlükte olan ya da gelecekte yürürlüğe girecek sözleşmeleri uygulamakta özgür oldukları belirtilmiştir. Bu tür bir eklelemeye örnek Hükümlülerin Nakli Konvansiyonu'nda (ETS No. 112) bulunmaktadır. Şüphesiz, uluslararası işbirliği bağlamında, diğer uluslararası sözleşmelerin (bunların çoğu uluslararası yardım konusunda etkinliği kanıtlanmış, uzun bir geçmişe dayanan formüller sunmaktadır) uygulanmasının işbirliğini teşvik edeceği umulmaktadır. Bu Konvansiyonun hükümlerine uygun olarak, Taraflar bu tür başka sözleşmeler yerine Konvansiyondaki uluslararası işbirliği hükümlerini uygulamaya karar verebilirler (bkz. Madde 27(1)). Bu tür durumlarda Madde 27'de belirtilen ilgili işbirliği hükümleri bu sözleşmelerdeki ilgili kuralların yerine geçecektir. Bu Konvansiyon genellikle asgari yükümlülükler getirdiği için, Madde 39, paragraf 2'de, ele alınan konularla ilgili ilişkilerini kurarken Tarafların Konvansiyonda belirtilenlere ek olarak daha spesifik yükümlülükler üstlenmekte özgür oldukları kabul edilmektedir.

Ancak bu mutlak bir hak değildir: Taraflar bunu yaparken Konvansiyonun hedef ve ilkelerine uygun davranmak zorundadırlar ve dolayısıyla Konvansiyonun amacına aykırı yükümlülükler kabul edemezler.

313. Ayrıca, Konvansiyonu kaleme alanlar, Konvansiyonun diğer uluslararası sözleşmelerle ilişkisini belirlerken Tarafların Anlaşma Hukuku Üzerine Viyana Konvansiyonu'ndaki ilgili hükümler için ek tavsiyeler arayabileceği üzerinde de anlaşmışlardır.

314. Konvansiyonda çok ihtiyaç duyulan bir uyumlulaşma düzeyi sunulmakla birlikte, bilgisayar suçları ya da bilgisayarla bağlantılı suçlar konusunda sonuca bağlanmamış bütün konuların ele alındığı da iddia edilmemektedir. Bu nedenle, Konvansiyonun sadece ele aldığı hususlarda etkili olacağını açıklığa kavuşturmak için paragraf 3 eklenmiştir. Mevcut olabilecek ama Konvansiyonda ele alınmamış diğer haklar, sınırlamalar, yükümlülükler ve sorumluluklara da dokunulmamaktadır. Diğer uluslararası sözleşmelerde böyle bir "tasarruf hükmü" için emsaller bulunabilir (örneğin, BM Teröristlerin Finansmanı Konvansiyonu).

Madde 40 - Yazılı Beyanlar

315. Madde 40'ta, çoğu Konvansiyonun, Tarafların hükümlerin kapsamını değiştirecek bazı belirli ek unsurlar eklemelerine izin verilen, usul hukuku Kısımında tesis edilen suçlarla ilgili olarak bazı maddelere atıfta bulunmaktadır. Bu tür ek unsurlarla, global olma iddiasındaki bir anlaşmada sadece Avrupa Konseyi bağlamında geçerli olan bir anlaşmadakinden daha haklı olabilecek belirli kavramsal ya da hukuki farklılıkların ele alınması amaçlanmaktadır. Yazılı beyanlar Konvansiyon hükümlerinin kabul edilebilir yorumlarıdır ve Tarafların Konvansiyonda ortaya koñan belli yükümlölüklerin hukuki etkilerini hariç bırakmalarına ya da değiştirmelerine izin veren hak saklı tutma hükümlerinden ayırt edilmelidir. Konvansiyonun Tarafları için diğerk Tarafların, eğer getirdilerse, hangi ek unsurları getirdiklerini bilmek önemli olduđu için, bir tasdik, kabul, onay ya da katılım belgesi imzalandığında ya da teslim edildiğinde bunun Avrupa Konseyi Genel Sekreteri'ne beyan edilmesi yükümlölüğü vardır. Bu bildirim, usulle ilgili belli yetkilerin uygulanmasında Taraflarca çifte suçluluk şartının yerine getirilmesi gerektiğı için, suçların

*Ankara Barosu
Bilgi İşlem Merkezi Yayınları*

**ANKARA BAROSU
BİLGİ ve BELGE MERKEZİ**

tanımları söz konusu olduğunda özellikle önemlidir. Yazılı beyanlar için sayısal bir sınır getirilmesi gerekli görülmemiştir.

Madde 41 - [Federal Ükelere İlişkin Hüküm (11)]

316. Mümkün olduğunca çok Ülkenin Konvansiyona Taraf olması amacına uygun olarak, Madde 41'de federal Ükelerin merkezi ve bölgesel yönetimler arasındaki karakteristik yetki dağılımlarının sonucu olarak yaşayabilecekleri güçlükler için uygulanmak üzere özel bir tür yazılı beyana izin verilmektedir. Ceza hukuku alanının dışında, diğer uluslararası sözleşmeler için hazırlanmış federal beyan ve hak saklı tutma hükümleri emsalleri mevcuttur (12). Bu Konvansiyonun 41. Maddesinde, federal Ülke olan Tarafların çok yerleşmiş durumdaki ulusal yasa ve uygulamalarının sonucu olarak kapsamlı ilgili küçük farklılıkların olabileceği kabul edilmektedir. Bu farklılıklar federal Ülkenin Anayasasına ya da ceza hukuku konularındaki yetkilerin merkezi yönetimle eyaletlerin ya da mülki birimlerin arasında nasıl bölündüğünü belirleyen diğer temel ilkelere dayandırılmalıdır. Konvansiyonu kaleme alanlar, federal ülkelere ilişkin hükmün uygulanmasının, Konvansiyonun

uygulanmasında sadece küçük farklılıklara yol açacağı konusunda anlaşmaya varmışlardır.

317. Örneğin, Amerika Birleşik Devletleri'nde, Anayasa ve federalizmin temel ilkeleri uyarınca, federal ceza mevzuatı genellikle eyaletler arası ya da dış ticareti etkileyen konuları düzenlerken, küçük ve tamamen yerel öneme sahip meseleler geleneksel olarak eyaletler tarafından düzenlenmektedir. Bu federalizm anlayışı bu Konvansiyonun kapsamındaki yasadışı fiillerin büyük bir bölümünün ABD federal ceza hukuku uyarınca ele alınmasını gerektirirken, eyaletlerin etkileri küçük çaplı ya da tamamen yerel öneme sahip konuları düzenlemeye devam etmesine izin vermektedir. Bazı durumlarda, federal hukuk yerine eyalet tarafından düzenlenen bu küçük fiil kategorisi içerisinde, bir eyalet aksi takdirde bu Konvansiyonun kapsamına girecek bir önleme izin vermeyebilir. Örneğin, tek başına çalışan bir kişisel bilgisayara ya da tek bir bina içerisinde birbirlerine bağlı olan bir bilgisayar ağına yapılacak bir saldırı saldırının gerçekleştiği eyaletin yasaları izin veriyorsa cezai nitelik taşıyabilir, ancak İnternet'in kullanımı eyaletler arası ya da dış ticaret üzerinde federal hukukun uygulanmasını gerektirecek etkiyi

yaratacağı için bilgisayara erişim İnternet yoluyla yapılmışsa saldırı federal bir suç sayılacaktır. Amerika Birleşik Devletleri ya da benzer şartlardaki başka bir federal ülkenin yasaları uyarınca bu Konvansiyonun uygulanması Madde 41'deki şartlara uygun olmalıdır.

318. Federal ülkelere ilişkin hükmün uygulanmasının kapsamı Bölüm II'nin hükümleriyle sınırlı olacaktır (maddi ceza hukuku, usul hukuku ve yargı yetkisi). Bu hükmü kullanan federal Ülkeler, bir kanun kaçağının ya da delilin bulunduğu eyalet ya da benzer mülki birim ilgili fiili suç olarak tanımlamasa da ya da bu Konvansiyon çerçevesinde gerekli olan usullere sahip olmasa da Bölüm III uyarınca diğer Taraf Ülkelerle işbirliğine gitme yükümlülüğü altında olacaklardır.

319. Federal yönetim, uygulaması Eyaletlerin ya da benzer mülki birimlerin yasama alanına giren hükümleri "favourable endorsement" ile bu birimlerin yetkili mercilerine devredeceklerdir. (Madde 41, paragraf 2).

320. Madde 41, paragraf 1 çerçevesinde yazılı bir beyanda bulunan federal bir Ülkenin, diğer

Tarafların federal ülkelere ilişkin hükmün uygulanmasının Konvansiyonun hükümlerinin uygulanması üzerindeki olası etkisini değerlendirebilmelerini sağlayacak derecede spesifik bir bildirimde bulunması gerekmektedir.]

Madde 42 - Hakların Saklı Tutulması

321. Madde 42'de bir dizi hususta hakların saklı tutulmasına izin verilmiştir. Bu yaklaşımın benimsenmesinin nedeni, Konvansiyonun birçok ülke için oldukça yeni olan bir ceza hukuku ve ceza usulleri hukuku alanını kapsamasıdır. Ayrıca, Avrupa Konseyi'ne üye olan ya da olmayan ülkelere açık olan Konvansiyon'un global niteliği bu hak saklı tutma imkanlarını gerekli kılmıştır. Bu hak saklı tutma imkanlarıyla, kendi ulusal mevzuatlarıyla tutarlı belli yaklaşım ve kavramları koruyarak mümkün olduğunca çok ülkenin Konvansiyona Taraf olmasının sağlanması amaçlanmıştır. Konvansiyonu kaleme alanlar, bir yandan da, hak saklı tutma imkanlarını sınırlandırarak Konvansiyonun Taraflarca mümkün olduğunca tek tip bir biçimde uygulanmasını sağlamaya çalışmışlardır. Dolayısıyla sayılanlar dışında saklı tutulabilecek bir hak bulunmamaktadır. Ayrıca, hak saklı

tutmalar sadece tasdik, kabul, onay ve katılım belgeleri imzalandığında ya da teslim edildiğinde yapılabilir.

322. Bazı Taraflar için bazı hakların saklı tutulmasının anayasal ilkelerle ya da temel hukuk ilkeleriyle çatışmaktan kaçınmak için temel önemde olduğu göz önünde bulundurularak Madde 43'te hakların saklı tutulmasından vazgeçilmesi için herhangi bir zaman sınırlaması getirilmemiştir. Vazgeçme işlemi şartlar izin verir vermez gerçekleştirilmelidir.

323. Taraflar üzerinde bir parça baskı yaratmak ve onların saklı tuttıkları haklardan vazgeçmeyi en azından değerlendirmelerini sağlamak için, Konvansiyonda Avrupa Konseyi Genel Sekreteri'ne düzenli olarak vazgeçme olasılıklarını soruşturma yetkisi getirilmiştir. Bu soruşturma imkanı halen birçok Avrupa Konseyi aracı için uygulanmaktadır. Taraflara böylece belirli hükümlerle ilgili olarak haklarını saklı tutmaya hala ihtiyaç duyup duymadıklarını gösterme ve sonrasında artık gerekli görülmeyenlerden vazgeçme fırsatı verilmektedir. Konvansiyonun tek tip olarak uygulanmasını teşvik etmek için zamanla

Tarafların saklı tuttıkları hakların mümkün olduğunca büyük bir kısmından vazgeçecekleri umulmaktadır.

Madde 44 - Değişiklikler

324. Madde 44 için, hükmün Avrupa Konseyi çerçevesinde geliştirilen ceza hukuku konvansiyonları için bir yenilik olarak getirildiği Suçlardan Elde Edilen Kazançların Aklanma, Aranma, El Konma ve Müsaderesiyle İlgili Konvansiyon (ETS No. 141) emsal alınmıştır. Değişiklik usulünün çoğunlukla usulle ilgili ya da teknik oldukça küçük değişiklikler için olduğu düşünülmektedir. Konvansiyonu kaleme alanlar Konvansiyon üzerinde büyük değişikliklerin ek protokoller yoluyla yapılabileceğini düşünmektedirler.

325. Taraflar Madde 46'da sağlanan istişare usulü uyarınca değişiklik ya da protokol ihtiyaçlarını kendileri inceleyebilirler. Avrupa Suç Sorunları Komitesi (CDPC) bu açıdan sürekli olarak bilgilendirilecek ve Konvansiyonu değiştirme ya da ona ekleme yapma çabalarında Taraflara yardım etmek için gerekli önlemleri alacaktır.

326. Paragraf 5 uyarınca, benimsenen bütün değişiklikler ancak bütün Taraflar kabul ettiklerini Genel Sekreter'e bildirince yürürlüğe girecektir. Bu şart, Konvansiyonun tek tip bir biçimde gelişmesini sağlamak için getirilmiştir.

Madde 45 - Anlaşmazlıkların Çözümü

327. Madde 45, paragraf 1'de Avrupa Suç Sorunları Komitesi'nin (CDPC) Konvansiyonun hükümlerinin yorumu ve uygulanması hakkında düzenli olarak bilgilendirilmesi gerektiği bildirilmektedir. Paragraf 2'de Taraflara Konvansiyonun yorumu ve uygulanması ile ilgili herhangi bir anlaşmazlığı barışçı yollarla çözmeye çalışmaları yükümlülüğü getirilmektedir. Anlaşmazlıkları çözmeye yönelik herhangi bir usul üzerinde ilgili Taraflar anlaşmaya varmalıdır. Bu hükümde üç olası anlaşmazlık çözme mekanizması önerilmiştir: Avrupa Suç Sorunları Komitesi (CDPC), tahkim kurulu ya da Uluslararası Adalet Divanı.

Madde 46 - Tarafların İstişarede Bulunmaları

328. Madde 46'da, Taraflar için, Konvansiyonun uygulaması, bilgisayar suçları ya da bilgisayarla bağlantılı suçlar ve delillerin elektronik ortamda

toplanmasıyla ilgili önemli hukuk, politika ya da teknoloji gelişmelerinin etkileri, ve Konvansiyon için ekleme ya da değişiklik yapma imkanı konularında istişarede bulunabilecekleri bir çerçeve yaratılmıştır. İstişarelerde, Madde 40, [41] ve 42 uyarınca yapılan beyan ve hak saklı tutmaların etkileri de dahil olmak üzere, özellikle Konvansiyonun kullanılması ve uygulanmasında karşılaşılan konular incelenecektir.

329. Usul esnektir ve toplantı yapmak istiyorlarsa bu toplantıları nasıl ve ne zaman yapacakları Taraflara bırakılmaktadır. Konvansiyonu kaleme alanlar, Avrupa Suç Sorunları Komitesi'nin (CDPC) yetkilerini korurken, Avrupa Konseyi'ne üye olmayan ülkeler de dahil olmak üzere Konvansiyonun bütün Taraflarının -eşit düzeyde- takip mekanizmalarına katılımını sağlamak için böyle bir usulün gerekli olduğuna inanmaktadırlar. Komite Taraflar arasındaki istişareler hakkında düzenli olarak bilgilendirilecek, bu istişarelerin gerçekleştirilmesini kolaylaştıracak ve Tarafların Konvansiyona ekleme ya da değişiklik yapma çabalarına yardım etmek için gerekli önlemleri alacaktır. Siber suçların etkin bir biçimde

önlenmesi ve kovuşturulması ihtiyacı, bağlantılı gizlilik konuları, ticari faaliyetlere olası etkileri ve diğer ilgili etkenler açısından, icra, sivil toplum ve özel sektör kuruluşları da dahil olmak üzere ilgili tarafların görüşleri bu istişareler için yararlı olabilir (paragraf 14'e de bkz.).

330. Paragraf 3'te Konvansiyonun yürürlüğe girdikten üç yıl sonra gözden geçirileceği ve bu tarihte uygun değişikliklerin tavsiye edileceği belirtilmektedir. CDPC bu gözden geçirmeyi Tarafların yardımıyla gerçekleştirecektir.

331. Paragraf 4'te, masrafların Avrupa Konseyi'nce üstlenildiği durumlar hariç Madde 46'nın 1. paragrafı uyarınca yürütülecek istişarelerin finansmanının Taraflarca gerçekleştirileceği belirtilmektedir. Ancak, Avrupa Suç Sorunları Komitesi'nin (CDPC) yanı sıra Avrupa Konseyi Sekreterliği de Tarafların bu Konvansiyon çerçevesinde gerçekleştirecekleri çabalara yardımcı olacaktır.

NOTLAR :

- (1) Implementation of Recommendation N° R (89) 9 on computer-related crime (R (89) 9 sayılı Tavsiyenin bilgisayarla bağlantılı suçlara uygulanması), Profesör Dr. H.W.K. Kaspersen tarafından hazırlanan rapor (doc. CDPC (97) 5 ve PC-CY (97) 5, sayfa 106).
- (2) Bkz. Computer-related crime (Bilgisayarla bağlantılı suçlar), Avrupa Suç Sorunları Komitesi Raporu, sayfa 86.
- (3) Bkz. Problems of criminal procedural law connected with information technology (Bilgi teknolojisiyle bağlantılı ceza usulleri hukuku sorunları), R (95) sayılı Tavsiye 13, ilke n° 17.
- (4) Konvansiyonun metni, 21 Eylül 1970'te yürürlüğe giren Protokol No. 3 (ETS No. 45), 20 Aralık 1971'de yürürlüğe giren Protokol No. 5 (ETS No. 55) ve 1 Ocak 1990'da yürürlüğe giren Protokol No. 8'in (ETS No. 118) hükümleri uyarınca değiştirilmiştir ve Madde 5, paragraf 3 uyarınca, 21 Eylül 1970'teki yürürlüğe girişinden beri Konvansiyonun ayrılmaz bir parçasını teşkil eden Protokol No. 2'nin (ETS No. 44) metnini içermektedir. Bu

Protokollerle değiştirilmiş ya da eklenmiş olan bütün hükümlerin yerini 1 Kasım 1998'deki yürürlüğe girişinden itibaren Protokol No. 11 (ETS No. 155) almıştır. Bu tarihten itibaren 1 Ekim 1994'te yürürlüğe giren Protokol No. 9 (ETS No. 140) yürürlükten kaldırılmıştır ve Protokol No. 10 (ETS No. 146) amacını kaybetmiştir.

- (5) Klass ve diğerleri-Almanya, A28, 06/09/1978 davasında Avrupa İnsan Hakları Mahkemesi Kararı.
- (6) Kruslin-Fransa, 176-A, 24/04/1990 davasında Avrupa İnsan Hakları Mahkemesi Kararı.
- (7) Huvig-Fransa, 176-B, 24/04/1990 davasında Avrupa İnsan Hakları Mahkemesi Kararı.
- (8) Malone-Birleşik Krallık, A82, 02/08/1984 davasında Avrupa İnsan Hakları Mahkemesi Kararı.
- (9) Halford-Birleşik Krallık, Raporlar 1997 - III, 25/06/1997 davasında Avrupa İnsan Hakları Mahkemesi Kararı.

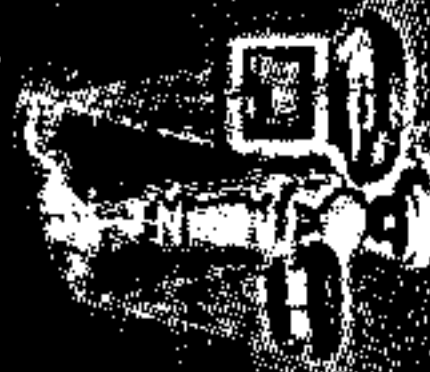
- (10) Lambert-Fransa, Raporlar 1998 - V, 24/08/1998 davasında Avrupa İnsan Hakları Mahkemesi Kararı.
- (11) Bu konuyla ilgili olarak CDPC'nin Bakanlar Kuruluna sunduğu Giriş Raporu'na bkz.
- (12) Örneğin 28 Temmuz 1951 tarihli Mültecilerin Statüsüyle İlgili Konvansiyon, Madde 34; 28 Eylül 1954 tarihli Devletsiz İnsanların Statüsüyle İlgili Konvansiyon, Madde 37; 10 Haziran 1958 tarihli Yabancı Tahkim Kurulu Kararlarının Kabulü ve Yürürlüğe Konmasına Dair Konvansiyon, Madde 11; 16 Kasım 1972 tarihli Dünyanın Kültürel ve Doğal Mirasının Korunmasına Dair Konvansiyon, Madde 34.

ANKARA BAROSU
BİLGİ İŞLEM MERKEZİ YAYINLARI



UYAP
ULUSAL YARGI AĞI
PROJESİ

Hedef: Hızlı ve Güvenli Yargı
Yol: Ulusal Yargı Ağı Projesi



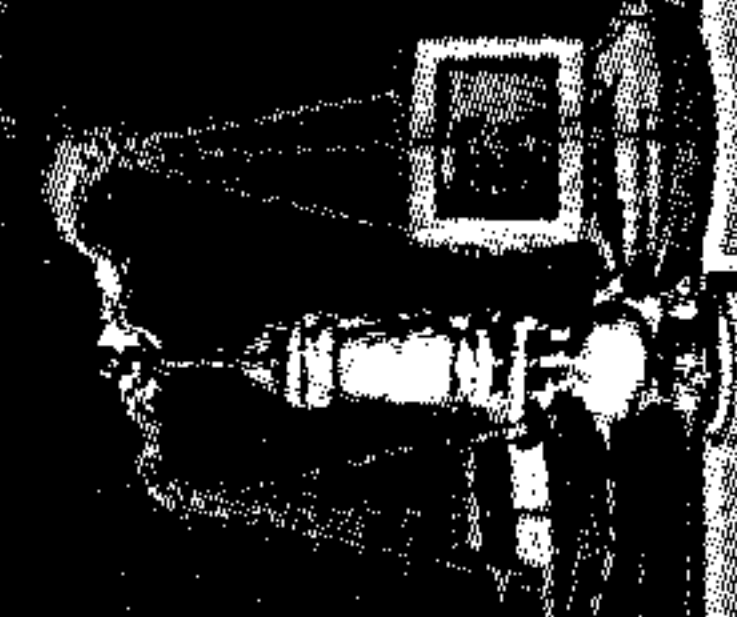
Detaylı Bilgi için:



Bilgi İşlem Dairesi Başkanlığı
Sarıyer, Mahallesi Meriç Sokak No 21/A
06510 Sırpçepe / Yenimahalle / ANKARA
Tel : 0 312 212 65 95 - 155
Faks : 0 312 215 66 43



Ankara Barosu Başkanlığı
ankarabaresu@ankarabaresu.org.tr
Açıkça Sırpçepe / Kat: 5 Sırpçepe / ANKARA
Tel : 0 312 310 65 25 (14 Hattı)
Faks : 0 312 309 22 37



BİRİNCİ
GÜNCELLEŞTİRİLMİŞ

Teknoloji Ulusal Yargı Ağı ile Adaletin Hizmetinde

ANKARA - 2005

BİRİNCİ BASKI : 1.000 Adet, Kasım 2005

İKİNCİ BASKI : 1.000 Adet, Haziran 2006

GÜNCELLEŞTİRİLMİŞ ÜÇÜNCÜ BASKI : 1.000 Adet, Ağustos 2006



ANKARA
BAROSU



TÜRKİYE
BİLİŞİM DERNEĞİ

ELEKTRONİK İMZA EL KİTABI



Türkiye Bilişim Derneği
Çıdın Evi, Bakır 4. Cad. No:8
Çankaya / Ankara
Telefon: 0312 473402
Faks: 0312 473407



Ankara Barosu Başkanlığı
ankbarosusu@ankbarosu.org.tr
Adliye Salıhi Kkt. 5. Sıhıya / ANKARA
Tel: 0312 310 55 25 (14 Hk)
Faks: 0312 310 22 37

Detaylı Bİgi için

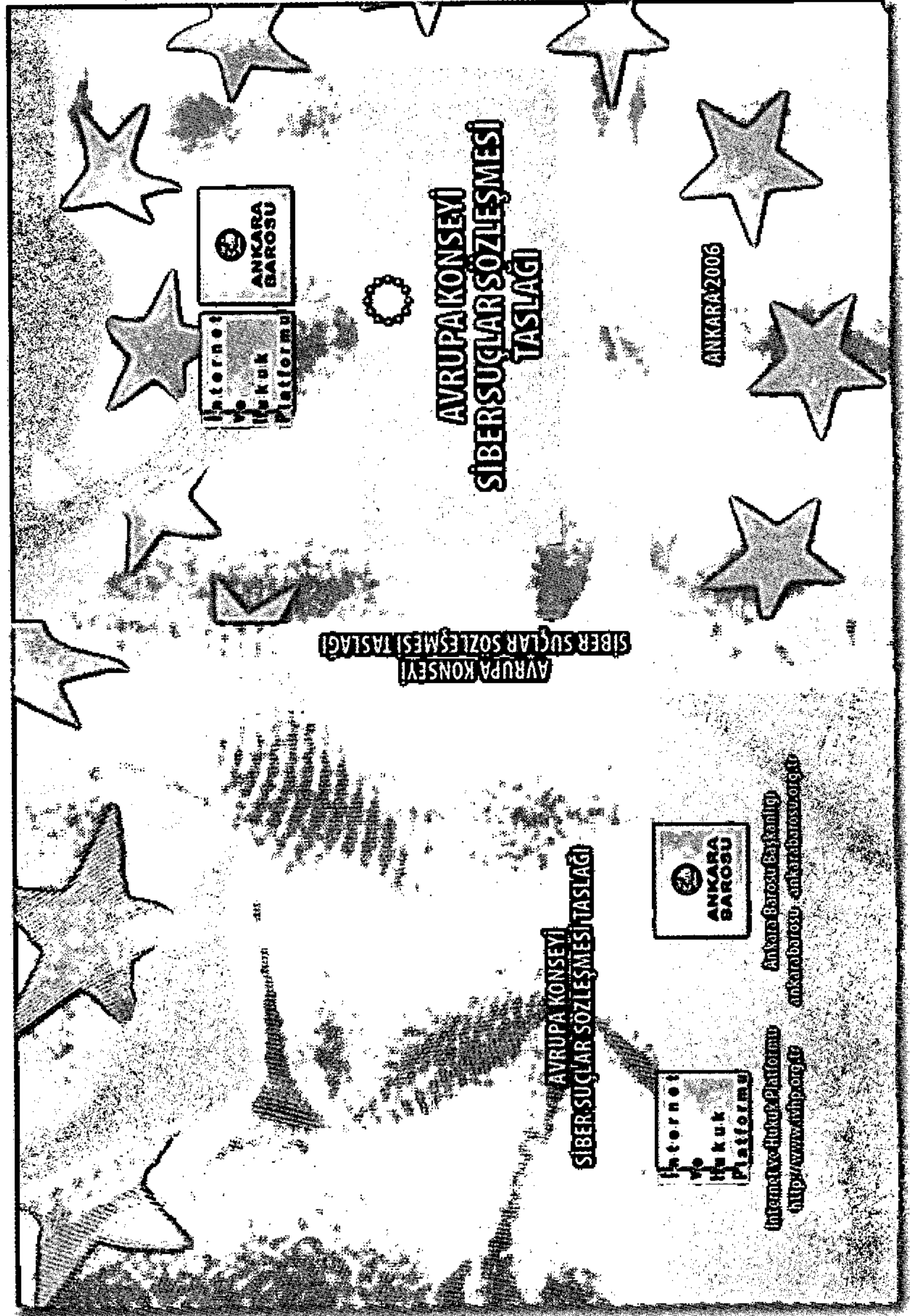


GÜNCELLEŞTİRİLMİŞ 2. BASKI

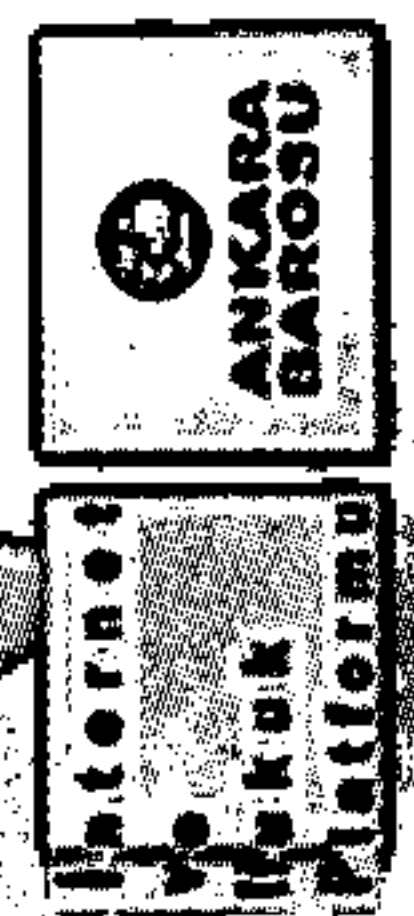
ANKARA - 2006

BİRİNCİ BASKI : 3.000 Adet, Haziran 2006

GÜNCELLEŞTİRİLMİŞ İKİNCİ BASKI : 1.000 Adet, Ağustos 2006



**AVRUPA KONSEYİ
SİBER SUÇLAR SÖZLEŞMESİ
TASLAĞI**



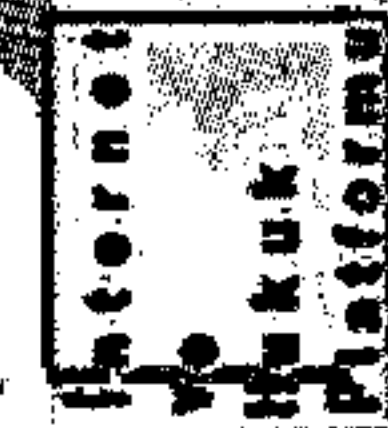
ANKARA 2006

**AVRUPA KONSEYİ
SİBER SUÇLAR SÖZLEŞMESİ TASLAĞI**

**AVRUPA KONSEYİ
SİBER SUÇLAR SÖZLEŞMESİ TASLAĞI**



Ankara Barosu Sayışıklığı
ankarabarosy.ankarabarovu.org.tr



Internet Hukuk Platformu
http://www.ihp.org.tr

BİRİNCİ BASKI : 1.000 Adet, Ağustos 2006