

Sanal Ortamda İşlenen Suçlar Sözleşmesi

Budapeşte, 23.11.2001

Giriş

Avrupa Konseyi'ne üye Devletler ve bu Sözleşme'yi imzalayan diğer Devletler;

Avrupa Konseyi'nin amacının üyeleri arasında daha geniş bir birlik sağlamak olduğunu dikkate alarak;

Bu Sözleşme'ye taraf olan diğer Devletlerle işbirliğinin geliştirilmesinin öneminin farkında olarak;

Toplulum sanal ortamda işlenen suçlara karşı korunması için diğer hususların yanı sıra, uygun mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi suretiyle ortak bir ceza siyasetinin öncelikli olarak takip edilmesi ihtiyacına kani olarak;

Bilgisayar ağlarının dijitalleşmesinin, yakınsamasının ve sürekli olarak küreselleşmesinin beraberinde getirdiği büyük değişikliklerin farkında olarak;

Bilgisayar ağlarının ve elektronik bilgilerin cezaî suç işlenmesi amacıyla da kullanılabilmesi ve bu tür suçlara ilişkin delillerin bu ağlarda depolanabileceği ve bu ağlar aracılığıyla aktarılabilmesi riskinden endişe duyarak;

Sanal ortamda işlenen suçlarla mücadelede Devletlerle özel sektör arasında işbirliğinin gerekliliğinin ve bilgi teknolojilerinin kullanımı ve geliştirilmesine ilişkin meşru çıkarların korunması ihtiyacını tanıyarak;

Sanal ortamda işlenen suçlara karşı etkin mücadelenin cezaî konularda artırılmış, hızlı ve iyi işleyen bir uluslararası işbirliğini gerektirdiğine inanarak;

İşbu Sözleşme'nin bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini hedef alabilecek eylemleri caydırıcı olmanın yanı sıra, bu tür sistemlerin, ağların ve verilerin kötüye kullanımının işbu Sözleşme'de tanımlandığı gibi böylece eylemlerin suç haline getirilerek engellenmesi ve söz konusu cezaî suçlarla etkili biçimde mücadele edilmesine yetecek yetkilerin temin edilmesini sağlamak amacıyla, bu tür cezaî suçların hem ulusal hem de uluslararası düzeyde tanımlanması, soruşturulması ve yargıya götürülmesinin kolaylaştırılması ve hızlı ve güvenilir uluslararası işbirliğinin sağlanmasına yönelik düzenlemelerin temin edilmesi için gerekli olduğuna kani olarak;

Herkesin müdahale olmaksızın düşünceye sahip olma hakkını, sınırlardan bağımsız olarak her türlü bilgi ve düşünceyi arama, alma ve iletme hakkı da dâhil olmak üzere, ifade özgürlüğü ve özel hayata saygı gösterilmesine ilişkin hakları düzenleyen 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi, 1966 Birleşmiş Milletler Medeni ve Siyasi Haklar Uluslararası Sözleşmesi ve diğer ilgili insan hakları anlaşmalarında güvence altına alındığı üzere, kanunların uygulanması ile temel insan haklarına saygı arasında uygun bir dengeyin sağlanmasına ihtiyaç duyulduğunu dikkate alarak;

1981 Kişisel Verilerin Otomatik İşlenmesinde Bireylerin Korunması Hakkında Avrupa Konseyi Sözleşmesi tarafından belirtildiği gibi kişisel verilerin korunması hakkını dikkate alarak;

1989 Birleşmiş Milletler Çocuk Hakları Sözleşmesi ve 1999 Uluslararası Çalışma Örgütü Çocuk İşçiliğinin En Kötü Durumları Sözleşmesini göz önünde bulundurarak;

Cezaî konularda işbirliğine ilişkin mevcut Avrupa Konseyi sözleşmelerinin yanı sıra Avrupa Konseyi üye Devletleri ve diğer Devletler arasında yapılmış olan benzer antlaşmaları da dikkate alarak ve bilgisayar sistemleri ve verileriyle alakalı cezaî suçlara ilişkin cezaî soruşturmaların ve kovuşturmaların daha etkin bir biçimde gerçekleştirilmesi ve bir cezaî suçun elektronik ortamdaki kanıtlarının toplanabilmesinin sağlanması için işbu Sözleşme'nin ilgili sözleşmeleri tamamlamasının amaçladığını vurgulayarak;

Birleşmiş Milletler, OECD, Avrupa Birliği ve G8 tarafından yapılan çalışmalar da dâhil olmak üzere, sanal ortamda işlenen suçlarla mücadelede uluslararası anlayış ve işbirliğini daha da geliştiren son gelişmeleri memnuniyetle karşılayarak;

Telekomünikasyon dinlemelerine dair istinabe müzekkereleri hususunda Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi'nin pratikte uygulanmasına ilişkin R (85) 10 sayılı Bakanlar Komitesi Tavsiye Kararı'nı, telif hakları ve komşu haklar alanında korsanlık hakkındaki R (88) 2 sayılı Bakanlar Komitesi Tavsiye Kararı'nı, polis sektöründe kişisel verilerin kullanımını düzenleyen R (87) 15 sayılı Bakanlar Komitesi Tavsiye Kararı'nı, özellikle telefon hizmetleri sözkonusu olduğunda telekomünikasyon hizmetleri alanında kişisel verilerin korunması hakkındaki R (95) 4 sayılı Bakanlar Komitesi Tavsiye Kararı'nı, bunların yanı sıra, bazı bilgisayar suçlarının tanımlanmasına ilişkin olarak ulusal yasama organlarına yönergeler sağlayan, bilişim suçları hakkındaki R (89) 9 sayılı Bakanlar Komitesi Tavsiye Kararı'nı ve ayrıca, bilgi teknolojisiyle ilişkili ceza muhakemeleri usul hukuku sorunlarına ilişkin R (95) 13 sayılı Bakanlar Komitesi Tavsiye Kararı'nı hatırlatarak;

Sanal ortamda işlenen suçlara ilişkin iç hukuktaki ceza kanunu hükümlerini birbirlerine yakınlaştırmak ve böylesi suçların soruşturulmasında etkin yöntemlerin kullanılmasını sağlamak amacıyla Bakanlar Komitesi'nin, Avrupa Suç Sorunları Komitesi (CDPC) tarafından sanal ortamda işlenen suçlara ilişkin yürütülen çalışmaları desteklemesini öneren ve Avrupa Adalet Bakanları'nın 21. Konferansı'nda (Prag, 10 ve 11 Haziran 1997) kabul edilen 1 sayılı Kararı; ayrıca, müzakere eden tarafların Sözleşme'ye olabildiğince çok sayıda Devletin taraf olmasını sağlamak için uygun çözümleri bulmak yönünde çabalarını sürdürmelerini destekleyen, bunun yanı sıra sanal ortamda işlenen suçlara karşı mücadelenin kendine özgü koşulları olduğunu gereken şekilde dikkate alan hızlı ve etkin bir uluslararası işbirliği sistemine duyulan ihtiyacı teslim eden 23. Avrupa Adalet Bakanları Konferansı'nda (Londra, 8 ve 9 Haziran 2000) kabul edilen 3 sayılı Kararı göz önünde bulundurarak;

Yeni bilgi teknolojilerine ilişkin gelişmelere Avrupa Konseyi'nin standartlarını ve değerlerini temel alan ortak yanıtlar aramak amacıyla, Avrupa Konseyi Devlet ve Hükümet Başkanları'nın İkinci Zirveleri vesilesiyle (Strazburg, 10 ve 11 Ekim 1997) kabul ettikleri Eylem Planı'nı da göz önünde bulundurarak;

Aşağıda belirtilen hususlarda mutabık kalmışlardır:

Bölüm I – Terimlerin Kullanımı

Madde 1 - Tanımlar

İşbu Sözleşme'nin amaçları bakımından:

- a “bilgisayar sistemi” terimi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder.
- b “bilgisayar verisi” terimi, bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder.
- c “hizmet sağlayıcı” terimi:
 - i hizmetlerini kullananlara bir bilgisayar sistemi aracılığıyla iletişim kurma olanağı sağlayan her türlü kamu veya özel sektör tüzel kişisini, ve

- ii böylece iletişim hizmeti veya bu hizmetlerin kullanıcıları adına bilgisayar verilerini işleyen veya depolayan diğer her türlü tüzel kişiyi ifade eder.
- d “trafik verisi” bir bilgisayar sistemi aracılığıyla gerçekleşen iletişimle ilgili olan, iletişim zincirinin bir halkasını teşkil eden bilgisayar sistemi tarafından üretilmiş, iletişimin başlangıç noktasını, hedefe varış noktasını, izlediği yolu, saatini, tarihini, boyutunu, süresini veya iletişimde kullanılan temel hizmetin türünü gösteren herhangi bir bilgisayar verisini ifade eder.

Bölüm II - Ulusal Düzeyde Alınacak Tedbirler

Kısım 1 - Maddî Ceza Hukuku

Başlık 1 – Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar

Madde 2- Yasadışı Erişim

Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir.

Madde 3 – Yasadışı Araya Girme

Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun sahtekârlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir.

Madde 4 – Verilere müdahale

- 1 Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 2 Taraflardan biri, 1. paragrafta tanımlanan fiillerin ciddi zararlar sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir.

Madde 5 – Sisteme müdahale

Taraflardan her biri, bilgisayar sistemlerine veri girişı yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, deęiřtirerek veya engelleyerek bir bilgisayar sisteminin iřleyiřinin haksız yere engellenmesinin, kasten gerekleřtirildięi zaman, kendi i hukuku kapsamında cezaî suç olarak tanımlanması iin gerekli olabilecek yasama tedbirlerini ve dięer tedbirleri kabul edecektir.

Madde 6 – Cihazların kötüye kullanımı

- 1 Taraflardan her biri, kasten ve haksız yere gerekleřtirildięi zaman, ařaęıdakilerin kendi i hukuku kapsamında cezaî suç olarak tanımlanması iin gerekli olabilecek yasama tedbirlerini ve dięer tedbirleri kabul edecektir:
 - a ařaęıda belirtilenlerin 2 ila 5. maddelerde belirtilmiř herhangi bir suçun iřlenmesi iin kullanılmaları amacıyla üretimi, satıřı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, daęıtımı veya bařka řekilde eriřilebilir hale getirilmesi:
 - i bir bilgisayar programı da dâhil olmak üzere, öncelikli olarak yukarıda belirtilen 2 ila 5. maddelerde belirtilmiř herhangi bir suu iřlemek amacıyla tasarlanmıř veya uyarlanmıř bir cihaz;
 - ii bir bilgisayar sisteminin tamamına veya herhangi bir kısmına eriřimi mümkün kılan bir bilgisayar řifresi, eriřim kodu veya benzer bir veri.
 - ve
 - b yukarıda paragraf a.i veya ii’ de atıfta bulunulmuř bir öęeye, 2 ila 5. maddelerde belirtilmiř herhangi bir suçun iřlenmesi iin kullanılması amacıyla bulundurma. Taraflardan biri, yasa gereęi cezaî sorumluluęun doęması iin bahsi geen öęelerden belli bir sayıda bulundurulmasını řart kořabilir.
- 2 İřbu madde, bu maddenin 1. paragrafında atıfta bulunulan üretme, satma, kullanım amaçlı tedarik, ithalat, daęıtma veya bařka řekilde eriřilebilir hale getirme veya bulundurmanın, 2 ila 5. maddeler uyarınca suç iřlemek maksadıyla gerekleřtirilmemesi durumunda, örneęin bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlölük doęuracağı řeklinde yorumlanmayacaktır.
- 3 Taraflardan her biri, ekincenin iřbu maddenin 1.a.ii paragrafında sözü edilen öęelerin satıřı, daęıtımı veya bařka řekilde eriřilebilir hale getirilmesiyle alakalı olmaması kaydıyla, iřbu maddenin 1.paragrafını uygulamama hakkını saklı tutabilir.

Başlık 2- Bilgisayarla bağlantılı suçlar

Madde – 7 Bilgisayarla bağlantılı sahtecilik

Taraflardan her biri, özgün olmayan verilerle sonuçlanan yeni veri girme, verileri değiştirme, silme veya engelleme eylemlerinin, sözkonusu verilerin yasal açıdan özgün verilerymiş gibi kabul edilmesi veya işlem görmesi niyetiyle, kasten ve haksız yere gerçekleştirildiği zaman, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına bakılmaksızın, bu eylemlerin kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, cezaî yükümlülüğünün doğması için, eylemin hile veya benzer bir sahtekârlık niyetiyle gerçekleştirilmiş olmasını şart koşabilir.

Madde – 8 Bilgisayarla bağlantılı dolandırıcılık

Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

- a bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;
- b bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma.

Başlık 3 – İçerikle bağlantılı suçlar

Madde 9 – Çocuk pornografisiyle bağlantılı suçlar

- 1 Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

- a bir bilgisayar sistemi üzerinden dağıtımını yapmak amacıyla çocuk pornografisi üretmek;
- b bir bilgisayar sistemi üzerinden çocuk pornografisini sunmak veya erişilebilir hale getirmek;
- c bir bilgisayar sistemi üzerinden çocuk pornografisinin dağıtım veya iletimini yapmak;
- d kendisi veya başkası için bir bilgisayar sistemi üzerinden çocuk pornografisi temin etmek;
- e bir bilgisayar sisteminde veya bilgisayar verileri depolama aygıtında çocuk pornografisi bulundurmak.

- 2 Yukarıda 1. paragrafta belirtilen “çocuk pornografisi” terimi aşağıda belirtilenleri görsel anlamda tasvir eden pornografik malzemeleri içerecektir:
 - a reşit olmayan şahsın cinsel içerikli eylemlerde bulunması;
 - b reşit olmayan şahıs görüntüsüne haiz şahsın cinsel içerikli eylemlerde bulunması;
 - c reşit olmayan şahsın cinsel içerikli eylemlerde bulunmasını betimleyen gerçekçi görüntüler.
- 3 Yukarıda 2. paragrafta belirtilen “reşit olmayan” terimi, 18 yaşın altındaki tüm şahısları kapsar. Bununla birlikte, Taraflardan biri, 16’dan küçük olmamak kaydıyla, daha düşük bir yaş sınırı talep edebilir.
- 4 Taraflardan her biri, 1. paragrafın d ve e bentleri ile 2. paragrafın b ve c bentlerinin tamamını veya bir kısmını uygulamaya koymama hakkını saklı tutabilirler.

Başlık 4 – Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar

Madde 10 - Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar

- 1 Taraflardan her biri, Edebiyat ve Sanat Eserlerinin korunmasına ilişkin Bern Sözleşmesi’ni tadil eden 24 Temmuz 1971 tarihli Paris Anlaşması, Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması ve WIPO (Dünya Fikri Mülkiyet Örgütü) Telif Hakları Antlaşması kapsamında üstlendiği yükümlülükler çerçevesinde, bu gibi sözleşmelerce tanınan her tür ahlaki haklar hariç olmak üzere, ilgili Tarafın ulusal mevzuatında tanımlandığı şekliyle, telif haklarının ihlalinin kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla gerçekleştirilmesinin kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 2 Taraflardan her biri, İcracı Sanatçılar, Fonogram Yapımcıları ve Yayın Kuruluşlarının Korunması Hakkındaki Uluslararası Sözleşme (Roma Sözleşmesi), Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması ve WIPO (Dünya Fikri Mülkiyet Örgütü) İcracı Sanatçılar ve Fonogramlar Anlaşması kapsamında üstlendiği yükümlülükler çerçevesinde, bu gibi sözleşmelerce tanınan her tür ahlaki haklar hariç olmak üzere, ilgili Tarafın ulusal mevzuatında tanımlandığı şekliyle, bağlantılı hakların ihlalinin kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla gerçekleştirilmesinin kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 3 Taraflardan biri, başka etkili hukuk yollarının mevcut olması ve bu tür bir çekincenin ilgili Taraf’ın işbu maddenin 1. ve 2. paragraflarında atıfta bulunulan uluslararası belgelerde belirtilen uluslararası yükümlülüklerine halel getirmemesi şartıyla, sınırlı şartlar dâhilinde işbu maddenin 1. ve 2. paragraflarında öngörülen cezaî sorumluluğu tahmil etmeme hakkını saklı tutabilir.

Madde 11 – Teşebbüs ve yardım veya yataklık

- 1 Taraflardan her biri, işbu Sözleşme'nin 2 ila 10. maddelerinde tanımlanan her türlü suçun işlenmesine, suçun gerçekleşmesi amacıyla kasten yardım veya yataklık edilmesinin kendi iç hukukunda cezaî suç olarak düzenlenmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 2 Taraflardan her biri, işbu Sözleşme'nin Madde 3 ila 5, 7, 8 ile 9.1.a ve c bentlerinde tanımlı suçlardan herhangi birine kasten teşebbüs eyleminin kendi iç hukukunda cezaî suç olarak düzenlenmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 3 Taraflardan her biri, işbu maddenin 2. paragrafının tamamını veya bir kısmını uygulamama hakkını saklı tutabilir.

Madde 12 – Kurumsal yükümlülük

- 1 Taraflardan her biri, bir tüzel kişilik bünyesinde aşağıda belirtilen unsurlara dayalı olarak önder konumuna sahip olan herhangi bir gerçek kişinin, bireysel ya da tüzel kişinin bir organının parçası olarak hareket ederek, tüzel kişinin çıkarları için işbu Sözleşme uyarınca cezaî suç olarak kabul edilmiş bir eylemi gerçekleştirmesi durumunda, tüzel kişilerin cezaî suçtan sorumlu tutulabilmesini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:
 - a tüzel kişiyi temsil yetkisi;
 - b tüzel kişi adına karar verme yetkisi;
 - c tüzel kişi bünyesinde murakabe yetkisi.
- 2 İşbu maddenin 1. Paragrafında belirtilen durumların yanı sıra, taraflardan her biri 1. Paragrafta atıfta bulunulan gerçek kişinin denetim veya kontrol eksikliği sonucunda tüzel kişinin yetkisi altında hareket eden gerçek kişinin bu tüzel kişinin menfaati için işbu Sözleşme'de belirlenmiş cezaî suçlardan birini işlemesi mümkün olursa, tüzel kişinin bundan sorumlu tutulmasını sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:
- 3 İlgili Taraf'ın yasal ilkelerine tâbi olarak, tüzel kişinin yükümlülüğü cezaî, hukuki veya idari nitelikte olabilir.
- 4 Böylesi bir yükümlülük, suçu işleyen gerçek kişilerin cezaî yükümlülüğüne halel getirmeyecektir.

Madde 13 – Yaptırımlar ve Tedbirler

- 1 Taraflardan her biri, 2 ila 11. maddelerde tanımlanan cezaî suçların, hürriyetten yoksun bırakmayı da kapsayan etkili, orantılı ve caydırıcı yaptırımlarla cezalandırılabilmesini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

- 2 Taraflardan her biri, Madde 12 uyarınca sorumlu tutulan tüzel kişilerin maddi yaptırımlar da dâhil olmak üzere, etkili, orantılı ve caydırıcı cezaî veya cezaî olmayan yaptırımlara veya tedbirlere tâbi olacağını teminat altına alacaktır.

Kısım 2 – Usul Hukuku

Başlık 1 – Ortak Hükümler

Madde 14: Usul Hükümlerinin Kapsamı

1. Taraflardan her biri, belirli cezaî soruşturma veya kovuşturmalar amacıyla, işbu Kısımda ele alınan yetki ve usulleri belirlemek için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2. Madde 21’de açık bir şekilde belirtilen aksine durumlar hariç olmak üzere, Taraflardan her biri bu maddenin 1. paragrafında sözü geçen yetki ve usulleri aşağıdaki durumlara ilişkin olarak uygulamaya koyacaktır:
 - a. işbu Sözleşme’nin 2 ila 11. maddelerinde tanımlı cezaî suçlar;
 - b. bir bilgisayar sistemi aracılığıyla işlenen diğer cezaî suçlar; ve
 - c. cezaî bir suçun delillerinin elektronik ortamda toplanması.
3. a. Taraflardan her biri, Madde 20’de belirtilen tedbirleri, sözkonusu tedbirlerin uygulandığı suçlar veya suç kategorilerinin Madde 21’de belirtilen tedbirlerin uygulandığı suçlardan daha sınırlı bir çerçevede olmaması kaydıyla, sadece çekince kaydında sözü edilen suçlara veya suç kategorilerine ilişkin olarak uygulama hakkını saklı tutabilir. Taraflardan her biri, Madde 20’de belirtilen tedbirin en geniş şekilde uygulanabilmesi için bu tür bir çekince kaydının sınırlı tutulmasını göz önünde bulunduracaktır.
 - b. İşbu Sözleşme’nin kabul edildiği tarihte yürürlükte olan mevzuat sınırlamalarından dolayı bir Taraf, Madde 20 ve 21’de belirtilen tedbirleri, herhangi bir hizmet sağlayıcının,
 - i. kapalı bir grup kullanıcının yararına işletilen, ve
 - ii. halka açık iletişim ağlarının kullanılmadığı ve halka açık veya özel nitelikli başka bir bilgisayar sistemine bağlı olmayan,

bir bilgisayar sistemi ile aktardığı bağlantılara uygulayamıyor ise, sözkonusu Taraf bu tür iletişimlere bu tedbirleri uygulamama hakkını saklı tutabilecektir. Tarafların her biri, Madde 20 ve 21’de belirtilen tedbirlerin en geniş şekilde uygulanabilmesi için bu tür bir çekince kaydının sınırlı tutulmasını göz önünde bulunduracaktır.

Madde 15 – Şartlar ve Tedbirler

1. Taraflardan her biri, işbu Kısımda ele alınan yetki ve usullerin tanımlanması, yürürlüğe konulması ve uygulanmasının, 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi, 1966 Birleşmiş Milletler Medeni ve Siyasi Haklar Uluslararası Sözleşmesi ve diğer uygulanabilir uluslararası insan hakları belgeleri kapsamında üstlendiği yükümlülüklerden kaynaklanan haklar da dâhil olmak üzere, iç hukukunda düzenlenmiş, insan hak ve özgürlüklerinin gerekli ölçüde korunmasını sağlayacak ve orantılılık ilkesini yerine getirecek şart ve güvencelere tabi olacağını teminat altına alacaktır.
2. Bu tür şart ve güvenceler, ilgili usul veya yetkinin niteliği göz önünde bulundurularak, uygun görüldüğü şekilde, diğer hususlar meyanında, adli veya başka tür bağımsız denetimi, haklı uygulama gerekçelerini ve sözkonusu yetki veya usul kapsam ve süresinin sınırlandırılmasını içerecektir.
3. Kamu yararına, özellikle adaletin sağlam bir şekilde tatbik edilmesine uygun olduğu ölçüde, Taraflardan her biri işbu Kısımda belirtilen yetki ve usullerin üçüncü şahısların hakları, sorumlulukları ve meşru menfaatleri üzerindeki etkisini dikkate alacaklardır.

Başlık 2 – Depolanan bilgisayar verisinin süratli şekilde korunması

Madde 16 – Depolanan bilgisayar verisinin süratli şekilde korunması

1. Taraflardan her biri, yetkili makamlarının, bilhassa bilgisayar veri kayıplarına veya değişikliklerine karşı özellikle korunmasız olma ihtimalinin bulunduğu bilgisayar sistemi aracılığıyla depolanan trafik verisi de dâhil olmak üzere, belirlenmiş bilgisayar verisinin süratli bir şekilde korunması talimatını vermelerini veya benzer biçimde bu korumayı gerçekleştirmelerini sağlamaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2. Taraflardan biri, bir kişinin mülkiyeti veya denetimi altında depolanmış bulunan, belli bilgisayar verilerinin korunması konusunda bir kişiye talimat vermek suretiyle yukarıda belirtilen paragraf 1'i uyguladığında, ilgili Taraf, azami doksan gün olmak üzere, gerek duyulan süre boyunca ilgili kişiyi o bilgisayar verilerini korumaya ve bütünlüğünü sürdürmeye mecbur kılmak ve yetkili makamların bunun açıklanmasını talep etmelerine olanak sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri böyle bir talimatın daha sonra yenilenmesini sağlayabilir.
3. Taraflardan her biri, verilerin korunmasından sorumlu kişiyi veya bilgisayar verilerini koruyacak olan diğer bir kişiyi, kendi iç hukukunun öngördüğü zaman dilimi boyunca, bu tür işlemleri üstlendiğini gizli tutacağına dair bir taahhütte bulunmaya mecbur kılmak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
4. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Madde 17 – Trafik verisinin süratli şekilde korunması ve kısmen açıklanması

1. Taraflardan her biri, Madde 16 uyarınca korunması gereken trafik verisi bağlamında, aşağıda belirtilenler için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:
 - a. sözkonusu haberleşmenin iletimine bir veya daha fazla hizmet sağlayıcının dâhil olmasına bakılmaksızın, trafik verilerinin süratli şekilde korunmasının teminat altına alınması; ve
 - b. ilgili Tarafın yetkili makamına veya bu makamın belirlediği kişiye, haberleşmenin hangi hizmet sağlayıcı ve hangi yol vasıtasıyla gerçekleştirildiğini tespit etmesine imkân verecek yeterli miktardaki trafik verilerinin süratli şekilde açıklamasının sağlanması.
2. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Başlık 3 – Üretim Emri

Madde 18 – Üretim Emri

1. Taraflardan her biri, yetkili makamların:
 - a. Ülkesindeki bir şahsa, o şahsın mülkiyeti veya kontrolünde bulunan, bir bilgisayar sisteminde veya bilgisayar verilerini depolama aygıtında depolanan, belirlenmiş bilgisayar verisini teslim etmesi için; ve
 - b. İlgili Tarafın ülkesinde hizmet sunan bir hizmet sağlayıcıya, sözkonusu hizmet sağlayıcının mülkiyeti veya kontrolünde bulunan hizmetlere ilişkin abone bilgilerini teslim etmesi için;

talimat verme yetkisine sahip olmaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

2. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15'e tabi olacaktır.
3. İşbu maddenin amacı yönünden “abone bilgisi” terimi, bir hizmet sağlayıcı tarafından bilgisayar verileri biçiminde veya başka bir biçimde tutulan, trafik veya içerik verileri hariç olmak üzere, hizmetlerin abonelerine ilişkin:
 - a. kullanılan iletişim hizmeti türünün, ayrıca belirlenen teknik hükümlerin ve hizmet süresinin;

- b. hizmet anlaşması veya düzenlemesi bağlamında erişilebilir abone kimliğinin, posta veya coğrafi adresinin, telefon veya diğer erişim numarasının, fatura ve ödeme bilgilerinin;
- c. hizmet anlaşması veya düzenlemesi bağlamında erişilebilir iletişim teçhizatının kurulduğu yere ilişkin diğer bilgilerin;

belirlenmesini sağlayabilecek herhangi bir bilgiyi ifade eder.

Başlık 4 – Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması

Madde 19 – Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması

1. Taraflardan her biri, kendi ülkesindeki yetkili makamların,
 - a. bir bilgisayar sisteminin tamamını veya bir kısmını ve içerisinde depolanmış bilgisayar verilerini; ve
 - b. bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtını arama ve benzer şekilde bunlara erişme yetkisine sahip olmaları için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
2. Taraflardan her biri, paragraf 1.a uyarınca, makamlarının özel bir bilgisayar sisteminin tamamını veya bir kısmını araması veya benzer şekilde bunlara erişim sağlaması sözkonusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğuna inanmak için gerekçeleri bulunduğu ve sözkonusu veriler yasalara uygun biçimde ilk sistemden erişilebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
3. Taraflardan her biri, yetkili makamlarına, paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine el koymaya veya benzer şekilde güvence altına almaya yetki tanımak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Bu tedbirler:
 - a. bir bilgisayar sisteminin tamamına veya bir kısmına veya bilgisayar verileri depolama aygıtına el koymaya veya bunları benzer şekilde güvence altına almaya;
 - b. sözkonusu bilgisayar verilerinin bir kopyasını oluşturmaya ve bunu muhafaza etmeye;
 - c. ilgili depolanan verilerin bütünlüğünü korumaya;
 - d. erişim sağlanan bilgisayar sistemindeki bilgisayar verilerini erişilemez hale getirmeye veya kaldırmayayönelik yetkileri içerecektir.

4. Taraflardan her biri, paragraf 1 ve 2’de belirtilen tedbirlerin tatbik edilmesine olanak sağlanması amacıyla, kendi yetkili makamlarına bilgisayar sisteminin işleyişi veya içerisindeki bilgisayar verisinin korunması için uygulanan tedbirler hakkında bilgisi olan herhangi bir kişiden, makul ölçüde gerekli bilgileri temin etme konusunda yetki tanınması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
5. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15’e tabi olacaktır.

Başlık 5 – Bilgisayar verilerinin gerçek zamanlı toplanması

Madde 20 – Trafik verilerinin gerçek zamanlı toplanması

1. Taraflardan her biri, yetkili makamlarına aşağıdaki hususlarda yetki tanınması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

Bir bilgisayar sistemi aracılığıyla iletilmiş, ülkesindeki belirli iletişimlerle ilişkili gerçek zamanlı trafik verilerini;

- a. ilgili Tarafın sınırları dahilinde mevcut teknik imkanlar kullanarak toplama veya kaydetme, ve
 - b. bir hizmet sağlayıcının mevcut teknik imkânları çerçevesinde,
 - i. ilgili Tarafın sınırları dahilinde mevcut teknik imkanlar uygulayarak toplamaya veya kaydetmeye; veya
 - ii. toplama veya kaydetmesi için yetkili makamları ile işbirliği yapmaya ve onlara yardım etmeye;
- zorunlu kılmak.

2. Taraflardan birinin, kendi iç hukuk sistemindeki yerleşmiş ilkelerden dolayı paragraf 1 a’da belirtilen tedbirleri kabul edememesi halinde, bunun yerine, ülke sınırları içerisinde iletilmiş belirli iletişimlere ait trafik verilerinin gerçek zamanlı olarak toplanması ve kaydedilmesi işleminin ilgili Tarafın sahip olduğu teknik imkanların uygulanması vasıtasıyla sağlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edebilecektir.
3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu madde ile öngörülen herhangi bir yetkinin ve bununla ilgili herhangi bir bilginin uygulanma şeklini gizli tutmaya zorunlu kılmak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
4. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15’e tabi olacaktır.

Madde 21 – İÇERİK VERİLERİNİN TAKİBİ

1. Taraflardan her biri, iç hukuku kapsamında belirlenecek bir dizi ciddi suçlar ile ilgili olarak yetkili makamlarına aşağıdaki hususlarda yetki tanınması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

Bir bilgisayar sistemi aracılığıyla ülke sınırları içerisinde iletilmiş, gerçek zamanlı, belirlenmiş iletişimlerin içerik verilerini;

- a. ilgili Tarafın ülkesinde teknik yöntemler kullanarak toplama veya kaydetme, ve
- b. bir hizmet sağlayıcıyı, mevcut teknik yeterliliği çerçevesinde,
- i. ilgili Tarafın sınırları dahilinde mevcut teknik yöntemlerin uygulanması vasıtasıyla toplamaya veya kaydetmeye; veya
- ii. toplama veya kaydetme için yetkili makamlar ile işbirliği yapmaya ve onlara yardım etmeye;

zorunlu kılmak.

2. Taraflardan birinin, kendi iç hukuk sistemindeki yerleşmiş ilkelerden dolayı paragraf 1 a'da belirtilen tedbirleri kabul edememesi halinde, bunun yerine ilgili ülke sınırları içerisinde iletilmiş belirli iletişimlere ilişkin içerik verilerinin gerçek zamanlı olarak toplanması ve kaydedilmesi işleminin ilgili Tarafın sahip olduğu teknik imkanların uygulanması vasıtasıyla sağlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
3. Taraflardan her biri, bir hizmet sağlayıcıyı işbu madde ile öngörülen herhangi bir yetkinin ve bununla ilgili bir bilginin uygulanma şeklini gizli tutmaya zorunlu kılmak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
4. İşbu maddede atıfta bulunulan yetki ve usuller Madde 14 ve 15'e tabi olacaktır.

Kısım 3 – Yargılama Yetkisi

Madde 22 – Yargılama Yetkisi

1. Taraflardan her biri, İşbu Sözleşme'nin 2 ila 11. maddelerinde belirtilen herhangi bir suç üzerinde, bunun aşağıdaki durumlarda işlenmesi halinde, yargılama yetkisinin tesisi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Suç;

- a. kendi ülkesinde; veya

- b. ilgili Tarafın bayrağını taşıyan bir gemide; veya
 - c. ilgili Tarafın kanunları kapsamında kayıtlı bir uçakta; veya
 - d. kendi vatandaşlarından biri tarafından, sözkonusu suçun işlendiği yerde ceza kanununa göre cezalandırılabilir ise veya suç herhangi bir Devletin yerel yargı yetkisi dışında işlenmiş ise.
2. Taraflardan her biri, işbu maddenin 1.b ila 1.d bentleri veya bunların herhangi bir kısmında tanımlanan yargılama yetkisi kurallarını uygulamama veya belirli durum veya şartlarda uygulama hakkını saklı tutabilir.
 3. Taraflardan her biri, zanlının kendi ülkesinde bulunduğu ve bir başka Tarafın iade talebi yapıldıktan sonra sadece uyuşundan dolayı iade edilmediği durumlarda, işbu Sözleşme'nin Madde 24 paragraf 1'de düzenlenen suçlara ilişkin yargılama yetkisini tesis etmek üzere gerekli olabilecek tedbirleri alacaktır.
 4. İşbu Sözleşme, Taraflardan birinin kendi iç hukuku uyarınca icra edilen herhangi bir cezaî yargılama yetkisini hariç tutamaz.
 5. İşbu Sözleşme uyarınca belirlenmiş, itham edilen bir suç üzerinde birden fazla Taraf yargı yetkisi iddia ettiğinde, müdahil Taraflar kovuşturma için en uygun yargılama yetkisini tespit etmek üzere istişare edeceklerdir.

Bölüm III – Uluslararası işbirliği

Kısım 1 – Genel ilkeler

Başlık 1 – Uluslararası işbirliğine ilişkin genel ilkeler

Madde 23 – Uluslararası işbirliğine ilişkin genel ilkeler

Taraflar, bilgisayar sistemleri ve verileri ile ilgili cezaî suçlara ilişkin soruşturma ve kovuşturmalar için, veya cezaî suçlara ilişkin olarak elektronik ortamda delil toplanması amacıyla, işbu bölümün hükümleri uyarınca ve ceza hukukuna dair konulardaki uluslararası işbirliğine ilişkin ilgili uluslararası belgelerin, yeknesak veya karşılıklı mevzuat ile iç hukuku temel alarak üzerinde anlaşmaya vardıkları düzenlemelerin uygulanması suretiyle, birbirleriyle mümkün olan en geniş biçimde işbirliği yapacaklardır.

Madde 24 – Suçluların iadesi

- 1 a Bu madde, Taraflar arasında suçluların iadesi için işbu Sözleşme'nin 2 ila 11. maddelerinde tanımlanmış cezaî suçlara ilişkin olarak sözkonusu suçluların her iki tarafın yasaları çerçevesinde, en az bir yıl süreyle özgürlükten mahrum bırakma cezası veya daha ağır bir ceza ile cezalandırılabilir olması durumunda geçerli olacaktır.
- b Yeknesak veya karşılıklı mevzuatı, veya Suçluların İadesine İlişkin Avrupa Sözleşmesi (ETS No. 24) de dâhil olmak üzere, iki veya daha fazla taraf arasında yürürlükte olan suçluların iadesine ilişkin anlaşmaları temel olarak üzerinde anlaşmaya varılan bir düzenleme çerçevesinde farklı bir asgari cezanın uygulanmasının sözkonusu olduğu durumlarda, sözkonusu düzenleme veya anlaşma çerçevesinde öngörülen asgari ceza geçerli olacaktır.
- 2 Bu maddenin 1. paragrafında tanımlanan cezaî suçlar, iki veya daha fazla Taraf arasındaki suçluların iadesine ilişkin anlaşmalar çerçevesinde suçluların iadesine konu olan suçlar arasında kabul edilecektir. Taraflar arasında suçluların iadesine ilişkin olarak imzalanacak herhangi bir anlaşmada bu tür suçları suçluların iadesine konu suçlar arasına dâhil edecekleri yönünde taahhütte bulunmaktadırlar.
- 3 Suçluların iadesini, buna ilişkin bir anlaşmanın mevcudiyeti şartına bağlayan bir Tarafın, kendisi ile suçluların iadesine yönelik bir anlaşma bulunmayan diğer bir Taraftan suçluların iadesi talebi alması durumunda, talebi alan Taraf, işbu Sözleşme'yi, bu maddenin 1. paragrafında belirtilen herhangi bir cezaî suça ilişkin gerekli yasal zemin olarak kabul edebilir.
- 4 Suçluların iadesini, buna ilişkin bir anlaşmanın mevcudiyeti şartına bağlamayan Taraflar, işbu maddenin 1. paragrafında tanımlanan cezaî suçları suçluların iade işlemi yapılmasına konu olan suçlar olarak aralarında tanıyacaklardır.
- 5 Suçluların iadesi işlemi, iade işlemi gerçekleştirilmesi talep edilen Tarafın sözkonusu işlemi gerçekleştirmesine zemin teşkil eden gerekçeler de dâhil olmak üzere, bu işlemi gerçekleştirmesi talep edilen Tarafın hukukundaki şartlara veya yürürlükte olan suçluların iadesine ilişkin anlaşmalara bağlı olacaktır.
- 6 Bu maddenin 1. paragrafında belirtilen bir cezaî suça ilişkin olarak suçluların iadesinin gerçekleştirilmesi yönündeki bir talebin, sadece iadesi talep edilen kişinin uyuşu dolayısıyla veya suçlunun iadesini gerçekleştirmesi talep edilen Tarafın sözkonusu suça ilişkin olarak yargı yetkisinin haiz olduğunu düşünmesi sebebiyle reddedilmesi durumunda, kendisinden suçlunun iade edilmesi istenen Taraf sözkonusu talebi yapan Tarafın isteği üzerine sorunu dava edilmesi amacıyla kendi yetkili makamlarına iletecek ve nihai sonucu iade talebinde bulunan Tarafa zamanlıca bildirecektir. Bu makamlar, Tarafın kanunlarına göre benzer nitelikte bir suçun sözkonusu olmuş olması durumunda yapacakları şekilde karar alacak ve soruşturma ile kovuşturmalarını da bu şekilde sürdürecektir.
- 7 a Taraflardan her biri, herhangi bir anlaşmanın mevcut olmadığı durumlarda suçluların iadesi veya geçici tutuklama talebini iletecek veya bu yönde bir talebi alacak makamlardan her birinin isim ve adresini Avrupa Konseyi Genel

Sekreteri'ne imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgesini tevdi ederken bildirecektir.

- b Avrupa Konseyi Genel Sekreteri, Tarafların tespit ettikleri makamların kaydını tutacak ve bunu sürekli güncelleyecektir. Her bir Taraf bu kayıta yer alan bilgilerin her zaman doğru olmasını temin edecektir.

Başlık 3 – Karşılıklı yardımlaşmaya ilişkin genel ilkeler

Madde 25 – Karşılıklı yardımlaşmaya ilişkin genel ilkeler

- 1 Taraflar, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlara ilişkin soruşturma ve kovuşturmalara veya bir cezaî suça ilişkin olarak elektronik ortamda delil toplanması hususunda birbirlerine, mümkün olan en geniş ölçüde yardım sağlayacaklardır.
- 2 Taraflardan her biri, 27 ila 35. maddelerde belirtilen yükümlülüklerin yerine getirilmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.
- 3 Taraflardan her biri, acil durumların sözkonusu olması halinde faks veya elektronik posta gibi ilgili hızlı iletişim araçları vasıtasıyla karşılıklı yardım veya iletişim talebinde bulunabilirler. Ancak, sözkonusu araçların gerekli güvenlik ve doğrulama ölçülerini sağlaması (gerekmesi durumunda şifre kullanımı da dâhil olmak üzere) ve kendisinden talepte bulunulan Tarafın istemesi durumunda resmi alındı teyidinde bulunulması gerekecektir. Kendisinden talepte bulunulan Taraf, iletilen talebi kabul edecek ve buna bu tür hızlı iletişim araçları vasıtasıyla cevap verecektir.
- 4 Bu bölümdeki maddelerde açık bir şekilde belirtilen aksine durumlar hariç olmak üzere, kendisinden talepte bulunulan Tarafın işbirliğinde bulunmayı reddedebileceği gerekçeler de dâhil olmak üzere, karşılıklı yardımda bulunma, kendisinden talepte bulunulan Tarafın yasalarındaki veya uygulanabilir karşılıklı yardımlaşma anlaşmalarındaki şartlara bağlı olacaktır. Kendisinden talepte bulunulan Taraf, 2 ila 11. maddelerde belirtilen suçlara ilişkin olarak karşılıklı yardımda bulunmayı, sadece talebin sözkonusu tarafça mali nitelikli olarak telakki edilen bir suç ile ilgili olduğu gerekçesine dayanarak, reddetme hakkını kullanmayacaktır.
- 5 Kendisinden talepte bulunulan Tarafın, bu bölümün hükümlerine uygun olarak, karşılıklı yardım sağlama hususunu, ilgili suçun her iki ülkede de cezaî nitelik taşıması şartına bağlamasına izin verilen durumlarda, talep edilen yardıma konu olan suça zemin teşkil eden fiilin yardım talebinde bulunan Tarafın yasaları çerçevesinde cezaî nitelik taşıması halinde bu şart, kendisinden talepte bulunulan Tarafın bu suçu talepte bulunan Tarafa aynı suç kategorisine koymasına veya aynı terimlerle nitelendirmesine bakılmaksızın, yerine getirilmiş sayılacaktır.

Madde 26 – Kendiliğinden bilgi verme

- 1 Taraflardan biri kendi iç hukukunun sınırları çerçevesinde ve önceden bir talep olmaksızın, kendi yürüttüğü soruşturmalar çerçevesinde edindiği bilgileri, sözkonusu bilgilerin açıklanmasının bilgileri alan Tarafa işbu Sözleşme'de tanımlanan cezaî suçlara ilişkin soruşturma ve davaların başlatılması veya yürütülmesi konusunda

yardımcı olabileceğini veya ilgili Tarafın bu bölüm çerçevesinde işbirliği talebinde bulunmasına neden olabileceğini düşündüğü takdirde, başka bir Tarafa iletebilir.

- 2 Sözkonusu bilgileri veren Taraf bunları vermeden önce, gizli tutulmasını veya sadece belirli şartlarda kullanılmasını talep edebilir. Bilgileri alan Taraf, bu talebin gereğini yerine getiremeyecek olması halinde, bilgileri veren Tarafı durumdan haberdar edecek, bilgileri veren Taraf da bilgilerin buna rağmen verilir verilemeyeceğini belirleyecektir. Bilgileri alan Tarafın belirli şartlara bağlı olarak bilgileri almayı kabul etmesi durumunda, sözkonusu Taraf bu şartlara bağlı hareket edecektir.

Başlık 4 – Uluslararası anlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardım taleplerine ilişkin usuller

Madde 27 – Uluslararası anlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardımlaşma taleplerine ilişkin usuller

- 1 Talepte bulunan Taraf ve kendisinden talepte bulunulan Taraf arasında yürürlükte olan yeknesak veya karşılıklı mevzuata dayalı herhangi bir karşılıklı yardım anlaşması veya düzenlemesinin mevcut olmadığı durumlarda, işbu maddenin 2 ila 9. paragraflarında belirtilen hükümler geçerli olacaktır. Bu tür bir anlaşma, düzenleme veya mevzuatın mevcut olduğu durumlarda, ilgili Tarafların bu madde hükümlerinin herhangi birini veya tamamını uygulamayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.
- 2
 - a Taraflardan her biri, karşılıklı yardım talebinde bulunmak, bu taleplere cevap vermek, bu taleplerin gereğini yerine getirmek veya bunların gereğini yerine getirecek makamlara bu talepleri iletmekle görevli bir merkezî makam veya makamlar belirleyecektir;
 - b Merkezî makamlar birbirleri ile doğrudan iletişim kuracaklardır;
 - c Taraflardan her biri, herhangi bir anlaşmanın mevcut olmadığı durumlarda işbu paragraf hükümleri uyarınca belirlenen makamlardan her birinin isim ve adresini Avrupa Konseyi Genel Sekreteri'ne imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgesini tevdi ederken bildirecektir;
 - d Avrupa Konseyi Genel Sekreteri, Taraflarca belirlenen merkezî makamların kaydını tutacak ve bunu sürekli güncelleyecektir. Her bir Taraf bu kayıta yer alan bilgilerin her zaman doğru olmasını temin edecektir.
- 3 İşbu Madde çerçevesindeki karşılıklı yardım talepleri, kendisinden talepte bulunulan Tarafın hukukuna aykırı durumlar hariç olmak üzere, talepte bulunan Tarafça tespit edilecek usullere göre işleme konulacaktır.
- 4 Kendisinden talepte bulunulan Taraf, Madde 25 Paragraf 4'te belirtilen red gerekçelerine ek olarak, aşağıdaki hususların sözkonusu olduğu durumlarda yardımda bulunmayı red edebilir:
 - a yardım talebine konu olan suçun kendisinden talepte bulunulan Tarafça siyasi suç olarak veya siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; veya

b sözkonusu talebin gereğinin yerine getirilmesinin kendisinden talepte bulunulan Tarafça bahse konu tarafın egemenliğine, emniyetine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğinin düşünülmesi.

- 5 Kendisinden talepte bulunulan Taraf, herhangi bir talebe ilişkin olarak işlem yapmasının yetkili makamlarınca sürdürülmekte olan cezaî soruşturma veya kovuşturmalara zarar vermesinin sözkonusu olabileceği durumlarda, bu talebe ilişkin işlemleri tehir edebilir.
- 6 Kendisinden talepte bulunulan Taraf, yardımda bulunmayı red veya tehir etmeden önce ve gerekli durumlarda yardım talebinde bulunan Taraf ile görüş alışverişinde bulunarak, yardımın kısmen veya kendisinde talepte bulunulan Tarafın gerekli gördüğü şartlara tabi olarak verilip verilemeyeceği hususunu telakki edecektir.
- 7 Kendisinden yardım talebinde bulunulan Taraf, yardım talebinin işleme konulmasından çıkan sonucu yardım talebinde bulunan Tarafa bildirecektir. Talebin reddi veya tehirine ilişkin gerekçeler bildirilecektir. Kendisinden yardım talebinde bulunulan Taraf, aynı zamanda, talebin yerine getirilmesini imkânsız kılan veya önemli ölçüde geciktirecek olan gerekçeleri de yardım talebinde bulunan Tarafa bildirecektir.
- 8 Yardım talebinde bulunan Taraf, kendisinden yardım talebinde bulunulan Tarafın, işbu bölüm çerçevesinde iletilen taleplere ve bunların içeriklerine ilişkin bilgileri, sözkonusu talebin yerine getirilmesi için gerekli olanlar hariç olmak üzere, gizli tutmasını isteyebilir. Kendisinden talepte bulunulan Tarafın bilgilerin gizli tutulması istemini yerine getiremeyecek olması halinde, sözkonusu Taraf bu durumu yardım talebinde bulunan Tarafa en kısa sürede bildirecek ve talepte bulunan Taraf talebin buna rağmen gerçekleştirilip gerçekleştirilmeyeceğini belirleyecektir.
- 9
 - a Acil durumlarda, karşılıklı yardım talepleri veya bu taleplere ilişkin iletişimler, yardım talebinde bulunan Tarafın adli makamları aracılığıyla kendisinden yardım talebinde bulunulan Tarafın adli makamlarına doğrudan iletilir. Bu tür durumlarda, sözkonusu talebin veya iletişimin bir nüshası yardım talebinde bulunan Tarafın merkezî makamı tarafından kendisinden yardım talep edilen Tarafın merkezî makamına iletilir.
 - b İşbu paragraf çerçevesinde iletilen herhangi bir talep veya iletişim Uluslararası Polis Teşkilatı (Interpol) aracılığıyla gönderilebilir.
 - c İşbu maddenin a paragrafına uygun olarak talepte bulunulması ve ilgili makamın buna ilişkin olarak işlem yapamıyor olması halinde, sözkonusu makam, talebi ulusal düzeyde yetkili olan makama iletecek ve bu durumu yardım talebinde bulunan Tarafa doğrudan bildirecektir.
 - d İşbu paragraf çerçevesinde iletilen ve zorlayıcı eylem içermeyen talepler veya iletişimler, Talepte bulunan Tarafın yetkili makamlarınca kendisinden talepte bulunulan Tarafın yetkili makamlarına doğrudan iletilir.
 - e Taraflardan her biri, etkinlik sağlama gerekçesinden dolayı, işbu paragraf çerçevesinde iletilen taleplerin merkezî makamlarına iletilmesi gerektiğini Avrupa Konseyi Genel Sekreterine imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgesini tevdi ederken bildirebilir.

Madde 28 – Gizlilik ve kullanının sınırlandırılması

- 1 Talepte bulunan Taraf ile kendisinden talepte bulunulan Taraf arasında yürürlükte olan yeknesak veya karşılıklı mevzuatı temel alan herhangi bir karşılıklı yardım anlaşması veya düzenlemesinin mevcut olmadığı durumlarda, işbu madde hükümleri geçerli olacaktır. Bu tür bir anlaşma, düzenleme veya mevzuatın mevcut olduğu durumlarda, ilgili Tarafların bu madde hükümlerinin herhangi birini veya tamamını uygulamayı kabul etmedikleri takdirde, işbu madde hükümleri geçerli olmayacaktır.
- 2 Kendisinden talepte bulunulan Taraf, talebe istinaden bilgi veya malzeme verilmesi için:
 - a karşılıklı hukuki yardım talebinin, bu tür bir şartın mevcut olmaması halinde karşılanamadığı durumlarda, sözkonusu bilgi veya malzemenin gizli tutulmasını, veya
 - b sözkonusu bilgi veya malzemelerin talepte belirtilenler dışında başka bir soruşturma veya kovuşturma için kullanılmamasını şart koşabilir.
- 3 Yardım talebinde bulunan Tarafın, paragraf 2’de belirtilen şartları yerine getiremeyecek olması halinde, sözkonusu Taraf diğer Tarafı ivedilikle durumdan haberdar edecek, diğer Taraf da bilgilerin buna rağmen verilir verilemeyeceğini belirleyecektir. Talepte bulunan Tarafın şartı kabul etmesi halinde, sözkonusu Taraf bu şarta bağlı hareket edecektir.
- 4 Paragraf 2’de belirtilen bir şartı uygulayarak bilgi veya malzeme veren herhangi bir Taraf, diğer Tarafın sözkonusu şarta ilişkin olarak bilgi veya malzemenin nasıl kullanıldığının izah edilmesini isteyebilir.

Kısım 2 – Özel Hükümler

Başlık 1 – Geçici tedbirlere ilişkin karşılıklı yardımlaşma

Madde 29 – Depolanan bilgisayar verilerinin süratli şekilde korunması

- 1 Taraflardan biri, diğer Tarafın ülkesindeki bir bilgisayar sistemi aracılığıyla depolanan ve talepte bulunan Tarafın arama yapma veya veriye benzer şekilde erişim sağlama, el koyma veya benzer şekilde güvence altına alma veya açıklanması amacıyla karşılıklı yardım talebine konu etmeyi düşündüğü verilerin süratli şekilde korunmasına hükmedilmesini veya bunun temin edilmesini sözkonusu Taraftan talep edebilir.
- 2 Paragraf 1 çerçevesinde bilgilerin korunması yönünde gerçekleştirilen bir talep aşağıdakileri içerecektir:
 - a korunmayı isteyen makam;
 - b cezaî soruşturmaya veya kovuşturmaya konu olan suç ve bununla ilgili esasların özeti;
 - c korunacak olan depolanan bilgisayar verisi ve bunun suç ile ilişkisi;

- d depolanan bilgisayar verisini korumakla yükümlü olan kişiyi veya bilgisayar sisteminin yerini belirleyen herhangi bir bilgi;
 - e korumanın gerekliliği; ve
 - f tarafın depolanan bilgisayar verisinde arama yapılması veya benzer şekilde buna erişim sağlanması, el konulması veya benzer şekilde güvence altına alınması veya açıklanması amacıyla karşılıklı yardım talebinde bulunma niyetinde olması.
- 3 Başka bir Taraftan talep alması üzerine, kendisinden yardım talebinde bulunulan Taraf belirlenmiş veriyi süratli şekilde korumak için gerekli olan bütün tedbirleri kendi iç hukukuna uygun olarak alacaktır. Bir talebe cevap verilmesi amacıyla ilgili suçun her iki ülkede de cezaî nitelik taşıması şartı aranmayacaktır.
- 4 İşbu Sözleşme'nin 2 ila 11. maddelerinde tanımlanan suçlar dışındaki suçlarla ilgili olarak depolanan verilere ilişkin arama yapma veya benzer şekilde erişim sağlama, el koyma veya benzer şekilde güvence altına alma veya açıklanması amacıyla karşılıklı yardım sağlanması amacına yönelik bir talebe cevap vermek için ilgili suçun her iki ülkede de cezaî nitelik taşıması şartını arayan bir Tarafın, sözkonusu şartın verilerin açıklanacağı tarihte yerine getirilemeyeceğini gösteren gerekçelere sahip olması halinde, sözkonusu Taraf işbu madde çerçevesinde verilerin korunması amacıyla iletilen talepleri reddetme hakkını saklı tutabilir.
- 5 Ayrıca, verilerin korunması amaçlı bir talep sadece aşağıdaki durumlarda reddedilebilir:
- a yardım talebine konu olan suçun kendisinden talepte bulunulan Tarafça siyasi suç veya siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi, veya
 - b sözkonusu talebin gereğinin yerine getirilmesinin kendisinden talepte bulunulan Tarafça bahse konu tarafın egemenliğine, emniyetine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğinin düşünülmesi.
- 6 Kendisinden yardım talep edilen Taraf, verilerin korunması işleminin verilere gelecekte ulaşılmasını güvence altına alamayacağını veya yardım talep eden Tarafın yürüttüğü soruşturmanın gizliliğini zedeleyeceğini veya buna başka şekillerde zarar vereceğini düşünmesi halinde, bunu yardım talebinde bulunan Tarafa en kısa sürede bildirecek, talepte bulunan Taraf talebin buna rağmen gerçekleştirilip gerçekleştirilemeyeceğini belirleyecektir.
- 7 Paragraf 1'de belirtilen talebe cevaben yerine getirilen herhangi bir koruma işlemi, yardım talebinde bulunan Tarafın verilere ilişkin arama yapma veya benzer şekilde erişim sağlama, el koyma veya benzer şekilde güvence altına alma veya açıklanması amacıyla talepte bulunmasına imkân verecek şekilde en az altmış gün süreli olacaktır. Bu yönde bir talebin alınmasının ardından, sözkonusu talep hususunda bir karar verilene kadar verilerin korunmasına devam edilecektir.

Madde 30 – Korunan trafik verilerinin süratli şekilde açıklanması

- 1 Belirlenmiş bir iletişime ilişkin trafik verilerinin korunmasına yönelik olarak Madde 29 çerçevesinde iletilen talebin yerine getirilmesi sırasında, kendisinden talepte

bulunulan Tarafın başka bir Devlet'teki bir hizmet sağlayıcının sözkonusu iletişimin sağlanmasında müdahil olduğunun farkına varması halinde, sözkonusu Taraf, talepte bulunulan Tarafa ilgili hizmet sağlayıcının ve verilerin aktarıldığı yolun belirlenmesine imkân vermek için yeterli miktardaki trafik verisini süratli şekilde açıklayacaktır.

- 2 Paragraf 1 çerçevesinde trafik verilerinin açıklanması işlemi ancak aşağıdaki durumlarda gerçekleşebilir:
 - a yardım talebine konu olan suçun kendisinden talepte bulunulan Tarafça siyasi suç veya siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi; veya
 - b sözkonusu talebin gereğinin yerine getirilmesinin kendisinden talepte bulunulan Tarafça bahse konu tarafın egemenliğine, emniyetine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğinin düşünülmesi.

Başlık 2- Soruşturma yetkileri konusunda karşılıklı yardımlaşma

Madde 31 – Depolanan bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma

- 1 Taraflardan biri, bir diğer Taraftan Madde 29 uyarınca korunan veriler de dâhil olmak üzere, sözkonusu Tarafın ülkesindeki bir bilgisayar sistemi aracılığıyla depolanan veride arama yapmayı veya benzer şekilde buna erişim sağlamayı, el koymayı veya benzer şekilde güvence altına alınmasını veya açıklanmasını talep edebilir.
- 2 Kendisinden talepte bulunulan Taraf, bu talebe, Madde 23'te bahsi geçen uluslararası belgeler, düzenlemeler ve kanunları uygulayarak ve bu Bölümün diğer ilgili hükümleri uyarınca yanıt verecektir.
- 3 Sözkonusu talebe cevap verilmesi işlemi aşağıdaki durumlarda hızla gerçekleştirilecektir:
 - a ilgili verilerin özellikle kaybolmasının veya değiştirilmesinin sözkonusu olabileceğine dair gerekçelerin bulunması; veya
 - b Paragraf 2'de atıfta bulunulan belgeler, düzenlemeler ve kanunlarda süratle işbirliğinde bulunulmasının öngörülmesi.

Madde 32 – Depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesinden erişim sağlanması

Bir Taraf, diğer Tarafın izni olmaksızın:

- a halkın serbest kullanımına sunulan (açık kaynaktan gelen) depolanmış bilgisayar verilerine, bunların coğrafi konumuna bakmaksızın erişebilir; veya
- b kendi ülkesindeki bir bilgisayar sistemi aracılığıyla, diğer Tarafın ülkesindeki depolanmış bilgisayar verilerine, eğer bu Taraf, sözkonusu bilgisayar sistemi aracılığıyla veriyi ifşa etme yetkisini yasal olarak haiz bulunan kişinin yasal ve

gönüllü onayını sağlayabilirse, sözkonusu verilere erişebilir veya bunları temin edebilir.

Madde 33 – Trafik verilerinin gerçek zamanlı olarak toplanması konusunda karşılıklı yardımlaşma

- 1 Taraflar, bilgisayar sistemi üzerinden aktarılan kendi ülkesindeki belirlenmiş haberleşmelerle bağlantılı trafik verilerinin gerçek zamanlı olarak toplanması için karşılıklı yardımda bulunacaklardır. Paragraf 2'nin hükümlerine tabi olmak şartıyla, bu yardımlaşma iç hukukta öngörülen şart ve usullere göre düzenlenecektir.
- 2 Her bir Taraf, en azından, gerçek zamanlı olarak toplanan trafik verilerinin sağlandığı benzer iç davalardaki cezaî suçlar konusunda bu yardımı sağlayacaktır.

Madde 34 – İçerik verilerine el konulması konusunda karşılıklı yardımlaşma

Taraflar yürürlükteki antlaşmalarının ve iç hukuklarının izin verdiği ölçüde, bilgisayar sistemi üzerinden aktarılan belirlenmiş haberleşmelerin içerik verilerinin gerçek zamanlı olarak derlenmesi veya kaydedilmesi konusunda birbirlerine karşılıklı yardımda bulunacaklardır.

Başlık 3 –24 saat 7 gün iletişim ağı

Madde 35 – 24 saat 7 gün İletişim ağı

- 1 Her bir Taraf, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlar konusundaki soruşturma veya kovuşturma veya cezaî suçun elektronik ortamda toplanmış delilleri için anında yardım temin edilmesini sağlamak amacıyla günde 24 saat ve haftanın 7 gününde erişilebilecek bir irtibat noktası belirleyecektir. Sözkonusu yardım, aşağıdakilerin kolaylaştırılmasını veya, iç hukuk ve uygulamalarının izin vermesi halinde, doğrudan yapılmasını içerecektir:
 - a teknik öneri sağlanması;
 - b Madde 29 ve 30 uyarınca verilerin korunması;
 - c delil toplanması, yasal bilgi sağlanması, şüphelilerin yerlerinin tespit edilmesi.
- 2
 - a Taraflardan birinin irtibat noktasının, diğer bir Tarafın irtibat noktasıyla hızlı bir şekilde iletişim sağlayabilecek yeteneğe sahip olması gerekmektedir.
 - b Taraflardan birinin belirlediği irtibat noktasının, o Tarafın uluslararası yardımından veya suçluların iadesinden sorumlu makam veya makamlarının bir parçası olmaması durumunda, sözkonusu irtibat noktasının bu makam veya makamlarla hızlı bir şekilde eşgüdümde bulunabilecek nitelikte olmasını sağlaması gerekmektedir.
- 3 Her bir Tarafın, iletişim ağının işletilmesini kolaylaştırmak için eğitimli ve donanımlı personel bulunmasını sağlaması gerekmektedir.

Bölüm IV – Son hükümler

Madde 36 – İmza ve yürürlüğe giriş

- 1 İşbu Sözleşme, Avrupa Konseyi'ne üye Devletlerin ve Sözleşme'nin hazırlanmasına katılmış üye olmayan Devletlerin imzasına açık olacaktır.
- 2 İşbu Sözleşme onay, kabul veya uygun bulmaya tabidir. Onay, kabul veya uygun bulma belgeleri Avrupa Konseyi Genel Sekreteri'ne tevdi olunacaktır.
- 3 İşbu Sözleşme, en az üçü Avrupa Konseyi üyesi olan beş Devlet, paragraf 1 ve 2 hükümleri uyarınca Sözleşme'ye tâbi olma rızalarını beyan ettikleri tarihten sonraki üç aylık sürenin bitimini izleyen ayın ilk gününde yürürlüğe girecektir.
- 4 İşbu Sözleşme, Sözleşme'ye tâbi olma rızalarını beyan eden, herhangi bir imzacı Devlete ilişkin olarak, paragraf 1 ve 2 hükümleri uyarınca Sözleşme'ye tâbi olma rızasını beyan ettiği tarihten sonraki üç aylık sürenin bitimini izleyen ayın ilk gününde yürürlüğe girecektir.

Madde 37 – Sözleşme'ye Taraf Olma

- 1 İşbu Sözleşme'nin yürürlüğe girmesinin ardından, Avrupa Konseyi Bakanlar Komitesi, Sözleşme'de Âkit Devletlerle görüşüp bu Devletlerin oybirliğiyle onaylamalarının ardından, Konsey üyesi olmayan ve işbu Sözleşme'nin hazırlanmasına katılmış olmayan herhangi bir Devleti Sözleşme'ye taraf olmaya davet edebilir. Bu karar Avrupa Konseyi Yasası'nın Madde 20.d'de belirtilen çoğunluk tarafından ve Bakanlar Komitesi'nde yer almaya hakkı bulunan Âkit Devletlerin temsilcilerinin oybirliğiyle alınacaktır.
- 2 Yukarıda paragraf 1'de belirtilen Sözleşme'ye taraf olan bir Devlete ilişkin olarak, İşbu Sözleşme, Avrupa Konseyi Genel Sekreteri'ne taraf olma belgesini tevdi etme tarihinden sonraki üç aylık sürenin bitimini izleyen ayın ilk gününde yürürlüğe girecektir.

Madde 38 – Belirli Bölgelerde Uygulama

- 1 Devletlerden herhangi biri, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgelerini tevdi ederken, Sözleşme'nin uygulanacağı bölge veya bölgeleri belirtebilir.
- 2 Devletlerden herhangi biri, daha sonraki bir tarihte Avrupa Konseyi Genel Sekreteri'ne yapacağı bir bildirimle, işbu Sözleşme'nin uygulama alanını bildirimde belirlenmiş başka herhangi bir bölgeye teşmil edilmesini belirtebilir. İşbu Sözleşme, böyle bir bildirimin Genel Sekreter tarafından alınmasından sonraki üç aylık sürenin bittiği ayı izleyen ayın ilk gününde yürürlüğe girecektir.
- 3 Önceki iki paragraf kapsamında yapılan herhangi bir bildirim, böyle bir bildirimde belirtilen herhangi bir bölge açısından Avrupa Konseyi Genel Sekreteri'ne yapılacak bir bildirimle geri çekilebilir. Geri çekilme, böyle bir bildirimin Genel Sekreter

tarafından alınmasından sonraki üç aylık sürenin bittiği ayı izleyen ayın ilk gününde yürürlüğe girecektir.

Madde 39 – Sözleşme’nin Etkileri

- 1 İşbu Sözleşme, aşağıda isimleri yer alan sözleşmelerin hükümleri de dâhil olmak üzere, Taraflar arasında yürürlükte olan çok taraflı veya ikili anlaşmaları veya düzenlemeleri tamamlamaya yöneliktir:
 - 13 Aralık 1957 tarihinde Paris’te imzaya açılan Suçluların İadesine Dair Avrupa Sözleşmesi (ETS No. 24);
 - 20 Nisan 1959 tarihinde Strazburg’da imzaya açılan Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (ETS No. 30);
 - 17 Mart 1978 tarihinde Strazburg’da imzaya açılan Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi’ne Ek Protokol (ETS No. 99).
- 2 Eğer iki veya daha fazla Taraf, işbu Sözleşme’de ele alınan konular hakkında daha önce sözleşme veya anlaşma akdetmiş veya bu tür konulara dair ilişkilerini başka şekilde tesis etmişlerse veya ileride tesis etmeleri durumunda, sözkonusu Taraflar bu anlaşma veya sözleşmeyi uygulama veya sözkonusu ilişkilerini bunlara uygun olarak düzenleme hakkına sahip olacaktır. Ancak, Tarafların işbu Sözleşme’de ele alınan konulara dair ilişkilerini işbu Sözleşme’de düzenlendiği şekilde tesis etmemiş olmaları halinde, işbu Sözleşme’nin amaç ve ilkeleriyle tutarsız olmayacak şekilde hareket etmeleri gerekecektir.
- 3 İşbu Sözleşme’nin hiçbir hükmü, bir Tarafın diğer haklarını, sınırlamalarını, yükümlülüklerini ve sorumluluklarını etkilemeyecektir.

Madde 40 – Beyanlar

Devletlerden herhangi biri, Avrupa Konseyi Genel Sekreteri’ne hitaben yazılı bir bildirimde bulunarak, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgesini tevdi ederken, Madde 2,3,6 Paragraf 1.b,7,9 Paragraf 3 ve 27 ve Paragraf 9.e kapsamında belirtildiği üzere, ek unsurlar talep etme olanağından yararlanabileceğini beyan edebilir.

Madde 41 – Federal Devletlere İlişkin Madde

- 1 Federal bir Devlet, işbu Sözleşme’de Bölüm II çerçevesinde belirtilen, merkezi Hükümeti ve ülkeyi oluşturan Eyaletler veya diğer benzer nitelikteki idari bölgeleri arasındaki ilişkilerin dayandığı temel ilkeleriyle tutarlı yükümlülükleri, Bölüm III çerçevesinde işbirliği yapabilmesi kaydıyla kabul etme hakkını saklı tutabilir.
- 2 Federal bir Devlet, paragraf 1’de belirtildiği şekilde çekince beyanında bulunduğu, bunun koşullarını Bölüm II’de yer alan tedbirlerin alınmasına ilişkin zorunlulukları dâhil etmemek veya önemli ölçüde azaltmak için uygulayamaz. Genel olarak, Federal Devlet bu tedbirlere ilişkin geniş ve etkili bir yasa uygulama yeteneğini sağlayacaktır.

- 3 Eyaletlerin yargı yetkisi veya federasyonun anayasal sistemi uyarınca yasama tedbirlerini alma zorunluluğu bulunmayan diğer benzer idari bölgelerin uyguladığı Sözleşme'nin hükümlerine ilişkin olarak, federal Hükümet, sözkonusu Eyaletlerin yetkili makamlarına bahsi geçen hükümleri olumlu görüşüyle birlikte bildirecek, bu makamları bunları yürürlüğe koymak amacıyla gereğini yapmaları konusunda teşvik edecektir.

Madde 42 – Çekinceler

Devletlerden herhangi biri, Avrupa Konseyi Genel Sekreteri'ne hitaben yazılı bir bildirimde bulunarak, imza sırasında veya onay, kabul, uygun bulma veya taraf olma belgesini tevdi ederken, 4. maddenin 2. paragrafı, 6. maddenin 3. paragrafı, 9. maddenin 4. paragrafı, 10. maddenin 3. paragrafı, 11. maddenin 3. paragrafı, 14. maddenin 3. paragrafı, 22. maddenin 2. paragrafı, 29. maddenin 4. paragrafı ve 41. maddenin 1. paragrafında belirtilen çekinceyi(leri) kullandığını beyan edebilir. Başka hiçbir çekince getirilemez.

Madde 43 – Çekincelerin Durumu ve Bunlardan Vazgeçilmesi

- 1 Madde 42 uyarınca çekince getiren bir Taraf, Avrupa Konseyi Genel Sekreteri'ne hitaben yazılı bir bildirimde bulunarak, çekincesinden tamamen veya kısmen vazgeçebilir. Vazgeçme işlemi, bu yazılı bildirim Genel Sekreter tarafından alındığı tarihte yürürlüğe girecektir. Eğer bildirim çekince hakkının belirtilen bir tarihte geri çekilmesini bildiriyorsa ve bu, bildirimin Genel Sekreter tarafından alındığı tarihten sonraki bir tarih ise, geri çekme işlemi sözkonusu sonraki tarihte yürürlüğe girecektir.
- 2 Madde 42 uyarınca çekince getiren bir Taraf, bu haktan, şartlar elverdiği andan itibaren tamamen veya kısmen vazgeçecektir.
- 3 Avrupa Konseyi Genel Sekreteri, Madde 42'de belirtildiği üzere bir veya daha fazla çekince getiren Taraflarla, bu çekince(ler)den vazgeçmesine ilişkin olanakları düzenli aralıklarla araştırabilir.

Madde 44 – Değişiklikler

- 1 Herhangi bir Taraf, işbu Sözleşme'de değişiklikler yapılması önerisinde bulunabilir ve bu değişiklikler Avrupa Konseyi Genel Sekreteri tarafından Avrupa Konseyi üye Devletleri'ne, işbu Sözleşme'nin hazırlanmasına katılmış üye olmayan Devletlere, ayrıca Madde 37 hükümleri uyarınca işbu Sözleşme'ye taraf olan veya taraf olmaya davet edilen herhangi bir Devlete bildirilebilir.
- 2 Bir Tarafın önerdiği herhangi bir değişiklik, Avrupa Suç Sorunları Komitesi'ne (CDPC) bildirilecek, bu Komite sözkonusu değişiklik önerisine ilişkin görüşlerini Bakanlar Komitesi'ne sunacaktır.
- 3 Bakanlar Komitesi önerilen değişikliği ve CDPC'nin sunduğu görüşü inceleyecek ve Sözleşme'ye taraf olan üye olmayan Devletlerle istişarede bulunduktan sonra sözkonusu değişikliği kabul edebilecektir.

- 4 İşbu Maddenin 3. paragrafı uyarınca Bakanlar Komitesi tarafından kabul edilen herhangi bir değişikliğin metni, kabul için Taraflara gönderilecektir.
- 5 İşbu Maddenin 3. paragrafı uyarınca kabul edilen herhangi bir değişiklik, tüm Tarafların bununla ilgili kabulü Genel Sekreter'e bildirmelerinden sonraki otuzuncu günde yürürlüğe girecektir.

Madde 45 – Uyuşmazlıkların Çözümü

- 1 Avrupa Suç Sorunları Komitesi (CDPC), işbu Sözleşme'nin yorumu veya uygulamasına ilişkin olarak sürekli şekilde bilgilendirilecektir.
- 2 Taraflar arasında işbu Sözleşme'nin yorumlanması ve uygulamasına ilişkin bir uyuşmazlık doğması durumunda, ilgili Tarafların üzerinde anlaşacağı şekilde, uyuşmazlığın CDPC'ye, kararları Tarafları bağlayıcı bir hakem heyetine veya Uluslararası Adalet Divanı'na götürülmesi de dâhil olmak üzere, Taraflar müzakere yoluyla veya kendilerinin tercih edeceği diğer barışçıl yollarla çözüm arayacaklardır.

Madde 46 – Taraflar Arasındaki İstişareler

- 1 Taraflar, uygun görüldüğü şekilde, aşağıdaki hususları kolaylaştırmak amacıyla düzenli aralıklarla istişarede bulunacaklardır:
 - a işbu Sözleşme'nin etkin şekilde kullanılması ve uygulanması, bu hususlara ilişkin sorunların ve işbu Sözleşme çerçevesinde yapılan herhangi bir beyan veya çekincenin etkilerinin belirlenmesi;
 - b sanal ortamda işlenen suçlara ilişkin önemli yasal, siyasal veya teknolojik gelişmeler ve elektronik ortamda delil toplanması konularında bilgi teatisinde bulunulması;
 - c Sözleşme'ye olası ilave veya değişikliklerin göz önünde bulundurulması.
- 2 Avrupa Suç Sorunları Komitesi (CDPC), paragraf 1'de belirtilen istişarelerin sonucu hakkında düzenli aralıklarla sürekli şekilde bilgilendirilecektir.
- 3 CDPC, uygun görüldüğü şekilde, paragraf 1'de belirtilen istişareleri kolaylaştırmak ve Sözleşme'ye ilavede bulunmaya veya değişiklik yapmaya yönelik çalışmalarında Taraflara yardımcı olmak için gerekli tedbirleri alacaktır. İşbu Sözleşme yürürlüğe girdikten en geç üç yıl sonra, Avrupa Suç Sorunları Komitesi (CDPC), Sözleşme'nin tüm hükümlerini Taraflarla işbirliği içinde gözden geçirecek ve gerektiği takdirde, uygun değişiklik tekliflerini yapacaktır.
- 4 Avrupa Konseyi tarafından üstlenilen masraflar hariç olmak üzere, paragraf 1 hükümlerini yerine getirmek için yapılan masraflar, Taraflarca, kendilerinin belirleyeceği şekilde karşılanacaktır.
- 5 Avrupa Konseyi Sekreteryası, Taraflara, işbu Madde çerçevesindeki görevlerini yerine getirmelerinde yardımcı olacaktır.

Madde 47 – Sözleşmeden Ayrılma

- 1 Herhangi bir Taraf, dilediği zaman, Avrupa Konseyi Genel Sekreteri'ne hitaben bir bildirimde bulunarak, işbu Sözleşme'den ayrılabilir.
- 2 Ayrılma işlemi, bildirimün Genel Sekreter tarafından alınmasından sonraki üç aylık sürenin sonunu izleyen ayın ilk gününde yürürlüğe girecektir.

Madde 48 – Bildirimler

Avrupa Konseyi Genel Sekreteri, Avrupa Konseyi üye Devletleri'ne, işbu Sözleşme'nin hazırlanmasına katılan üye olmayan Devletlere, ayrıca Sözleşme'ye taraf olan veya taraf olmaya davet edilen herhangi bir Devlete:

- a her imzayı;
- b tevdi edilen her onay, kabul, uygun bulma veya taraf olma belgesini;
- c Madde 36 ve 37 uyarınca her yürürlüğe giriş tarihini;
- d Madde 40 uyarınca yapılan her beyanı veya Madde 42 uyarınca getirilen her çekinceyi;
- e işbu Sözleşme'ye ilişkin diğer her tür eylem, bildirim veya iletişimi bildirecektir.

Yukarıdaki hususlar muvacehesinde, aşağıda imzası bulunanlar usulüne uygun şekilde yetkilendirilmiş olarak işbu Sözleşme'yi imzalamışlardır.

İşbu Sözleşme, 23 Kasım 2001 tarihinde Budapeşte'de, her iki metin de aynı derecede geçerli olmak üzere, İngilizce ve Fransızca dillerinde, Avrupa Konseyi arşivlerinde saklanacak şekilde tek nüsha olarak imzalanmıştır. Onaylı nüshaları Avrupa Konseyi Genel Sekreteri tarafından Avrupa Konseyi üye Devletleri'ne, işbu Sözleşme'nin hazırlanmasına katılan üye olmayan Devletlere, ayrıca Sözleşme'ye taraf olan veya taraf olmaya davet edilen tüm Devletlere gönderilecektir.

SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİ (ETS-NO.185) İLE İLGİLİ ÇEKİNCELER VE BEYANLAR

40. Madde ve 2. Madde'ye istinaden, Türkiye Cumhuriyeti Devleti, suçun bilgisayar verilerini elde etmek veya başka bir sahtekar niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koştuğunu beyan eder.

40. Madde ve 7. Madde'ye istinaden, Türkiye Cumhuriyeti Devleti, bilgisayarla bağlantılı sahteciliğe ilişkin Madde 7'deki suç tanımının Türk kanunlarına göre dolandırma veya benzeri hileli davranış kastını gerektirdiğini beyan eder.

42. Madde ve 14. Maddenin 3 (b) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak, söz konusu sistemin belirli bir kullanıcı grubunun menfaatine işletiliyor olması; 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 20. ve 21. Maddelerde belirtilen önlemleri uygulamama hakkını saklı tutar.

42. Madde ve 22. Madde'ye istinaden, Türkiye Cumhuriyeti Devleti, Türk vatandaşının yurt dışında işlemiş olduğu suçlardan dolayı Türk Ceza Kanunu'nun 11. ve 13. Maddeleri çerçevesinde yargı yetkisini kullanma hakkını saklı tutar.

42. Madde ve 29. Maddenin 4. Paragrafına istinaden, Türkiye Cumhuriyeti Devleti, çifte suçluluk şartının verilerin açıklandığı tarihte yerine getirilemiyor olduğuna ilişkin gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması talebini reddetme hakkını saklı tutar.

24. Maddenin 7 (a) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, suçluların iadesine ilişkin anlaşma mevcut olmadığı durumlarda, suçluların iadesi veya geçici tutuklama taleplerini iletmek veya almak üzere Adalet Bakanlığını yetkili makam olarak belirler.

27. Maddenin 2 (c) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, karşılıklı yardım taleplerinde bulunmak, talepleri yanıtlamak, bu taleplerin gereğini yerine getirmek veya bunların gereğini yerine getirecek makamlara bu talepleri iletmekle Adalet Bakanlığını merkezi makam olarak belirler.

35. Maddenin 1. Paragrafına istinaden, Türkiye Cumhuriyeti Devleti, 7 gün/24 saat esasına göre temas noktasının:

Emniyet Genel Müdürlüğü
Siber Suçlarla Mücadele Daire Başkanlığı
Kızılırmak Mah. Anadolu Bulvarı 2185.Sk. No:14
06520 Söğütözü-Çankaya/ANKARA
siber@egm.gov.tr.
olduğunu beyan eder.



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

- a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c "service provider" means:
 - i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
 - ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;
- d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
 - a the production, sale, procurement for use, import, distribution or otherwise making available of:
 - i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
 - b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a any input, alteration, deletion or suppression of computer data;
- b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a producing child pornography for the purpose of its distribution through a computer system;
 - b offering or making available child pornography through a computer system;
 - c distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - e possessing child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
 - a a minor engaged in sexually explicit conduct;
 - b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

- 3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
- 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

- 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
- a a power of representation of the legal person;
 - b an authority to take decisions on behalf of the legal person;
 - c an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
 - b other criminal offences committed by means of a computer system; and
 - c the collection of evidence in electronic form of a criminal offence.
- 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
- b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
- i is being operated for the benefit of a closed group of users, and
 - ii does not employ public communications networks and is not connected with another computer system, whether public or private,
- that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 - Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
- 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 16 – Expedited preservation of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
 - a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
 - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
 - a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

- b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
- a the type of communication service used, the technical provisions taken thereto and the period of service;
 - b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
 - c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
- a a computer system or part of it and computer data stored therein; and
 - b a computer-data storage medium in which computer data may be stored
- in its territory.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - b make and retain a copy of those computer data;

- c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
- a collect or record through the application of technical means on the territory of that Party, and
 - b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party; or
 - ii to co-operate and assist the competent authorities in the collection or recording of,
- traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

- 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

- a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party, or
 - ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - a in its territory; or
 - b on board a ship flying the flag of that Party; or
 - c on board an aircraft registered under the laws of that Party; or
 - d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
- 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

- 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
- 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III - International co-operation

Section 1 - General principles

Title 1 - General principles relating to international co-operation

Article 23 - General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 - Principles relating to extradition

Article 24 - Extradition

- 1
 - a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
 - b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
- 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
- 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

- 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
- 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
- b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

- 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
- 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
- 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
- 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

- 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
- 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

- 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2
 - a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
 - b The central authorities shall communicate directly with each other;
 - c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
 - d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
- 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
- 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
 - a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
- d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
- e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality and limitation on use

- 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

- a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
 - b not used for investigations or proceedings other than those stated in the request.
- 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
- 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 - Specific provisions

Title 1 - Mutual assistance regarding provisional measures

Article 29 - Expedited preservation of stored computer data

- 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
- 2 A request for preservation made under paragraph 1 shall specify:
- a the authority seeking the preservation;
 - b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
 - c the stored computer data to be preserved and its relationship to the offence;
 - d any available information identifying the custodian of the stored computer data or the location of the computer system;
 - e the necessity of the preservation; and
 - f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
- 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

- 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
- 5 In addition, a request for preservation may only be refused if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
 - b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

- 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
- 2 Disclosure of traffic data under paragraph 1 may only be withheld if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

- 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

- 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
- 3 The request shall be responded to on an expedited basis where:
 - a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

- 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
- 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

- 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
 - a the provision of technical advice;

- b the preservation of data pursuant to Articles 29 and 30;
 - c the collection of evidence, the provision of legal information, and locating of suspects.
- 2
 - a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
 - b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
 - 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

- 1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
- 2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
- 3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
- 4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

- 1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
- 2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

- 1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
- 2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
- 3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

- 1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
 - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
 - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
 - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
- 2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
- 3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

- 1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
- 2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
- 3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

- 1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
- 2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
- 3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

- 1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
- 2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
- 3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
- 4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
- 5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

- 1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
- 2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

- 1 The Parties shall, as appropriate, consult periodically with a view to facilitating:
 - a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
 - b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
 - c consideration of possible supplementation or amendment of the Convention.
- 2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

- 3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
- 4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
- 5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 - Denunciation

- 1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
- 2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 - Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d any declaration made under Article 40 or reservation made in accordance with Article 42;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

RESERVATIONS AND DECLARATIONS WITH RESPECT TO CONVENTION ON CYBERCRIME (No. 185)

In accordance with Article 40 and Article 2 of the Convention, the Republic of Turkey declares that it requires that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or relation to computer system that is connected to another computer system.

In accordance with Article 40 and Article 7 of the Convention, the Republic of Turkey declares that the offense set forth in Article 7 regarding computer-related forgery requires an intent to defraud or similar dishonest intent under Turkish Law.

In accordance with Article 42 and Article 14 paragraph 3 (b) of the Convention, the Republic of Turkey reserves the right not to apply the measures referred in Article 20 and Article 21 to communications being transmitted within a computer system if the system is being operated for the benefit of a closed group of users and does not employ public communications networks and is not connected with any other public or private computer system.

In accordance with Article 42 and Article 22 of the Convention, the Republic of Turkey reserves the right to establish jurisdiction within the scope of Article 11 and 13 of the Turkish Criminal Law when the offence is committed by a Turkish national outside its sovereign territory.

-In accordance with Article 42 and Article 29 paragraph 4 of the Convention, the Republic of Turkey reserves the right to decline the request for preservation of data under this article in cases where it has reasons to believe that at the time of the disclosure of stored computer data the condition of dual criminality cannot be fulfilled.

-In accordance with Article 24 paragraph 7 (a) of the Convention, the Republic of Turkey designates the Ministry of Justice as the authority responsible for making or receiving requests for extradition or provisional arrest, in the absence of an extradition treaty.

-In accordance with Article 27 paragraph 2 (c) of the Convention, the Republic of Turkey designates the Ministry of Justice as the central authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

-In accordance with Article 35 paragraph 1 of the Convention, the Republic of Turkey designates as point of contact available on a twenty-four hour, seven-day-a-week basis:

Turkish National Police
Department of Cybercrime
Kızılırmak Mah. Anadolu Bulvarı 2185.Sk. No:14
06520 Söğütözü-Çankaya/ANKARA
siber@egm.gov.tr.