AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİNDE YER ALAN MADDİ CEZA HUKUKUNA İLİŞKİN DÜZENLEMELER VE ÖZELLİKLE İNTERNETTE ÇOCUK PORNOGRAFİSİ*

Prof. Dr. Füsun Sokullu-Akıncı**

I. Giriş

Bilgi teknolojisinde yaşanan devrim hem son derece hızlı gelişmiş, hem de çok köklü olmuştur. Hayal dahi edemeyeceğimiz pek çok işlem son derece kolaylaşmış, bilgi son derece hızlı bir şekilde erişilebilir duruma gelmiştir. Bilgi teknolojisi adını verdiğimiz bu kavram insanların tüm etkinliklerine kadar sızmıştır. Bilgi teknolojisinde bu denli hızlı devrim telekomünikasyon teknolojisini de zorlamaktadır, öte yandan alışılmış telefon teknolojisi iletişiminin ötesinde ses, metin, müzik, hareketli ve hareketsiz görüntü verilerinin değişimini olanaklı hale getiren sistemlerin geliştirilmesi gerekmiştir.

Hepimizin yakından izlediği tüm bu gelişmeler bize bilgilere ulaşmada pek çok kolaylık sağladığı gibi dünyanın da iyice küçülmesine, coğrafi mesafelerin adeta ortadan kalkmasına neden olmuştur. Sınır tanımayan bu iletişim, bilgilerin de geometrik hızla artmasını sağlamıştır.

Bütün bunların olumlu etki ve sonuçlarına karşın her toplumsal ve ekonomik gelişme ve değişmede olduğu gibi, geleneksel suçların artmasına ve ayrıca yeni bazı suçların da ortaya çıkmasına neden olmuştur. Hem bilinen suçlar artık yeni tek-

---

* İnternet Ortamında Ceza Sorumluluğu konulu panele sunulan bildiri.

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

nolojiyle işlenir duruma gelmiştir hem de yeni bazı suç türlerinin yasalarca belirlenmesi gereği ortaya çıkmıştır.

Klasik Ceza Hukukundan tanıdığımız "mesafe suçları" kavramı artık geniş olarak uygulanması mümkün bir kavramdır. Ancak mesafe suçunu incelerken hangi Devlet yasasının uygulanacağını tartışmaktaydık. Bugün artık ulusal yasalarla bu sorunu çözümlemek mümkün olamamaktadır. Zira geleneksel ceza hukuku kuralları siber uzay olanaklarının kötüye kullanılmasını engellemeye yetmemektedir. Bilgi ağlarının sınır ötesi yapılarından dolayı sorunların çözümü uluslararası alanda aranmalıdır. Nitekim Siber Suç Sözleşmesi tüm taraf devletlerde birbirine benzer suç tipleri saptayarak uluslararası bir yeknesaklık sağlamaya çalışmaktadır. Göz açıp kapayıncaya kadar tüm dünyayı kat edebilecek suçların birbirine eş düzenlemelerle kovuşturulup cezalandırılması gerekmektedir. İşte Siber Suç Sözleşmesi bunu yapmaktadır: Sınır tanımayan bilgi erişimine, sınır tanımayan bir Ceza Hukuku Sistemi gerekmektedir.

Sözleşme ve açıklayıcı rapor Avrupa Konseyi Bakanlar Komitesinin 109. oturumunda kabul edilmiş ve 23 Kasım 2001'de Budapeşte'de imzaya açılmıştır.

Sözleşmede ulusal düzeyde alınacak önlemler bağlamında yapılan Ceza Hukukuna İlişkin Düzenlemelerin ilk grubu şunlardır:

A- Bilişim Suçları Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar

Bu bölümün amacı, bilgisayarla işlenen ya da bilgisayarlarla ilişkili suçlar için ortak bir minimum standart oluşturarak bu suçları önleyecek ve denetim altına alacak önlemleri geliştirmektir. Bu tür bir uyumlaştırma bu suçlarla hem ulusal hem de uluslararası düzeyde yapılan mücadeleyi güçlendirir. Ulusal mevzuatların uyumlu olması, kötüye kullanımların hukuksal standartları düşük olan ülkelere kaymasını önleyebilir.

Sonuçta belirli vakaların ele alınmasında edinilen yararlı ortak deneyimlerin paylaşımı da geliştirilebilir. Çifte suçluluk gibi konulardaki uluslararası işbirliği, özellikle geri verme ve uluslararası adli yardımlaşma gibi konularda kolaylık sağlar.

Maddi hukuk hükümleri bilgi teknolojileri kullanılarak işlenen suçlara ilişkin olmakla birlikte, maddi ceza hukuku suçlarının hem bugünkü hem de gelecekteki teknolojiler için uygulanabilmesini sağlamak amacıyla Konvansiyonda teknoloji açısından nötr bir dil kullanılmıştır.

Bu bölümde yer alan suçlarda eylem *"hukuka aykırı biçimde"* yapılmış olmalıdır. Mağdurun rızası, haklı savunma ya da zorunluluk gibi hukuka uygunluk nedenlerinin bulunduğu eylem hukuka uygun olacaktır.

Ceza sorumluluğunun söz konusu olabilmesi için Konvansiyonda yer alan bütün suçların kasten işlenmesi gerekir. Bazı durumlarda özel kast aranır. Örneğin, bilgisayarla dolandırıcılık suçunda (Madde 8) *ekonomik bir kazanç* elde etmeye yönelik bir maksat aranmaktadır.

Kısımdaki bazı maddeler, Konvansiyonunun ulusal mevzuatta uygulanmasında bazı kısıtlayıcı şartların ilave edilmesine izin vermektedir. Bazı durumlarda hakların saklı tutulması olanağı bile tanınmıştır (bkz. Madde 40 ve 42). Suç olarak tanımlamaya yönelik bu tür çeşitli daha kısıtlayıcı yaklaşımlar, söz konusu davranışın tehlikelilik düzeyiyle ve ceza hukukunu bir karşı tedbir olarak kullanma ihtiyacıyla ilgili farklı değerlendirmeleri yansıtmaktadır. Bu yaklaşım hükümetlere ve kanun koyuculara bu alandaki ceza politikalarını belirleme esnekliğini tanımaktadır.

Bu suçları belirleyen yasalar, ceza yaptırımlarına yol açacak eylem türlerinin yeterince tahmin edilebilir olmasını sağlamak amacıyla mümkün olduğunca açık ve spesifik bir dille kaleme alınmalıdır. Diğer bir deyişle, burada 'belirlilik' aranmaktadır.

Açıklayıcı Rapordan, Taslağı hazırlayanların, kaleme alma sürecinde, bu bölümde yer alan suçlar dışındaki bazı eylemle-

rin suç olarak tanımlanmasının yerindeliğini değerlendirdikleri anlaşılmaktadır. Örneğin Siber işgalcilik (gecekonduculuk) adı verilen, mevcut olan ve genellikle çok tanınan bir kişi ya da kuruluşun adını ya da bir ürün ya da firmanın ticari ismini ya da ticari markasını alan adı olarak kaydettirme eylemi de buna dahildir. Siber işgalciler söz konusu alan adlarını aktif olarak kullanmayı düşünmemekte ve ilgili kişi ya da kuruluşu dolaylı olarak da olsa bu alan adının mülkiyetinin transferi için para ödemeye zorlayarak mali avantaj elde etmeye çalışmaktadırlar. Şu an için bu fiil ticari markalarla ilgili bir sorun olarak ele alınmaktadır. Ticari marka ihlalleri bu Konvansiyonda ele alınmadığı için, taslağı hazırlayanlar bu tür fiilleri suç olarak tanımlama konusunu değerlendirmenin uygun olmadığı sonucuna ulaşmışlardır.

1- Hukuka Aykırı Erişim (m.2)

" Taraf devletlerin her biri, bir bilgisayar sisteminin tamamına veya bir bölümüne hakkı olmadığı halde kasten yapılan erişim eylemlerinin suç olarak belirlenmesi için gerekli yasama faaliyetlerini ve diğer işlemleri yapacaktır. Taraf devletlerden biri söz konusu suçun, bilgisayar verilerinin elde edilmesi amacıyla veya diğer dürüstlüğe aykırı bir amaçla güvenlik sistemini ihlal edilmesi şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemine ilişkin olarak da düzenleyebilirler".

Burada bir bilişim sistemine hukuka aykırı bir şekilde erişim sağlanması düzenlenmiştir.

"Hukuka aykırı erişim" terimi bilgisayar sistem ve verilerinin güvenliğine (yani gizlilik, bütünlük, kullanıma açıklık) yönelik tehlikeli tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Koruma ihtiyacı, kuruluş ve kişilerin sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme ihtiyaçlarını yansıtmaktadır. Sadece "hacking", "cracking" ya da "computer trespass" ilke olarak başlı başına yasadışı olmalıdır. Bu durum, sistemlerin ve verilerin yasal kullanıcılarının engellenmesine ve düzeltilmesi yüksek maliyet

getiren değişiklik ve yıkıma yol açabilir. Bu tür izinsiz girmeler gizli verilere (şifreler, hedeflenen sistemle ilgili bilgiler dahil olmak üzere) ve sırlara erişilmesine, sistemin ücretsiz kullanılmasına yol açabilir, hatta hacker'ları bilgisayarla ilişkili sahtecilik ve dolandırıcılık gibi daha tehlikeli suç türlerine teşvik edebilir.

İzinsiz erişimi önlemenin en etkin yolu şüphesiz ki etkin güvenlik önlemlerinin geliştirilmesi ve uygulanmaya başlanmasıdır. Ancak kapsamlı bir önlem ceza hukukuna ilişkin yaptırımlarını kullanma tehdidini ve bu yaptırımların uygulamalarını da içermelidir. İzinsiz erişimin ceza yoluyla engellenmesi sistem ve veriler için ek bir koruma getirebilir ve yukarıda sayılan tehlikelerin erken bir aşamada önlenmesini sağlayabilir.

"Erişim", bilgisayar siteminin tamamına ya da bir parçasına (donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler) girilmesi anlamındadır. Ancak, sisteme sadece bir e-posta mesajı ya da dosya gönderilmesini kapsamaz. "Erişim", kamusal telekomünikasyon ağları yoluyla ya da bir kuruluşun yerel ağı (LAN) ya da Intranet'i gibi bir ağ üzerindeki başka bir bilgisayar sistemine girmeyi de içine alır. İletişim yöntemi (örneğin kablosuz bağlantılar da dahil olmak üzere uzaktan ya da yakın mesafeden) önemli değildir.

Eylemin hukuka aykırı olması gerekmektedir. Bu ifade, sistemin ya da bir parçasının sahibi ya da başka hak sahiplerinin izniyle yapılan erişimin (örneğin ilgili bilgisayar sisteminin izinli olarak test edilmesi ya da korunması amacıyla) suç olarak tanımlanamayacağı anlamına gelmektedir. Ayrıca, kamunun ücretsiz ve açık erişimine izin veren bilgisayar sistemlerine erişim suç olarak tanımlanamaz. Bu tür erişimler hukuka uygundur.

Birçok ulusal mevzuatta "hacking" suçlarıyla ilgili hükümler zaten bulunmaktadır, ama suçun kapsamı ve unsurları önemli ölçüde farklılık göstermektedir. Madde 2'nin ilk cümlesindeki geniş tanımlama eğilimi tartışma konusudur. Yalnızca izinsiz girme eyleminin hiçbir tehlike yaratmadığı ve hatta hack-

ing olaylarının sistemlerin güvenliğindeki boşluk ve zayıflıkların saptanmasını sağladığı iddia edilmektedir. Bu nedenle bazı ülkelerde "hacking" suçlarına daha bir hoşgörü ile bakılmaktadır.

2- Yasadışı Müdahale (m.3)

"Taraf Devletlerin her biri, aşağıda sözü edilen bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar istemi üzerinden veri iletimine haksız surette dahil olma eylemi, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında bir suç olarak saptanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır. Taraf Devletler söz konusu suçun, ahlaka aykırı maksatla veya, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini kullanarak yapılmasını ayrıca düzenleyebilirler".

Bu hükümle veri iletişiminin gizliliği güvence altına alınmaya çalışılmaktadır. Aynen telefon görüşmelerinin gizli olarak dinlenmesi ve kaydedilmesinde olduğu gibi, bilgisayar sistemine girerek buradaki veri iletimine müdahale edilmesinin suç olarak düzenlenmesi gerekmektedir. İletişimin gizliliği hakkı Avrupa İnsan Hakları Sözleşmesinin 8. Maddesinde son derece önemli bir hak olarak gösterilmiştir. Madde 3'te tanımlanan suç bu ilkenin telefon, faks, e-posta ya da dosya transferi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmasıdır.

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

"Teknik yöntemler" kullanarak müdahale, iletişimin içeriğinin dinlenmesi, kontrolü ya da izlenmesi ve verilerin içeriği-

nin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizli dinleme cihazlarının yardımıyla dolaylı olarak elde edilmesi anlamına gelmektedir. Müdahaleye "kaydetmek" de dahildir. Teknik yöntemler, iletim hatlarına takılan teknik cihazları ve kablosuz iletişimi elde etmekte ve kaydetmekte kullanılan cihazları da kapsar. Bu yöntemler yazılım, şifre ve kodların kullanımını da kapsayabilir. Teknik yöntemler kullanma şartı, gereğinden fazla eylemi suç haline getirmemek için kullanılmış sınırlayıcı bir kavramdır.

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

Bilgisayar verilerinin iletimi biçimindeki iletişim tek bir bilgisayar sisteminin içinde (örneğin işlemciden ekran ya da yazıcıya akış), aynı kişiye ait iki bilgisayar sistemi arasında, birbiriyle iletişim halindeki iki bilgisayar ya da bir bilgisayar ile bir kişi (örneğin klavye yoluyla) arasında olabilir.

"Bilgisayar sistemi" kavramının radyo bağlantılarını da içine almasının, "kamuya açık olmayan" bir iletim de olsa, görece açık ve kolaylıkla erişilebilir bir şekilde yapılan ve bu nedenle, örneğin amatör radyocular tarafından, müdahale edilebilen bir radyo iletimini suç olarak tanımlamak konusunda Taraflara bir zorunluluk getirmediğine dikkat edilmelidir.

Bir bilgisayar sisteminin elektromanyetik dalgalarındaki

verilere müdahale bu hüküm çerçevesinde suç olarak kabul edilebilir.

Ceza sorumluluğunun söz konusu olabilmesi için yasadışı müdahalenin "kasten" ve "hukuka aykırı olarak" gerçekleştirilmiş olması gerekmektedir. Örneğin müdahale eden kişi bunu yapma hakkına sahipse, iletimin taraflarının talimatları doğrultusunda ya da izinleriyle bunu yapıyorsa (tarafların izin verdiği test etme ve koruma faaliyetleri dahil olmak üzere), ya da izleme ulusal güvenlik ya da soruşturma mercilerinin suçları araştırma çalışmaları çerçevesinde yasal yetkiyle gerçekleştiriliyorsa, eylem hukuka uygundur.

3- Verilere Müdahale (m.4)

1."Taraf devletlerden her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin, kasten olarak yapıldıklarında kendi ulusal mevzuatı kapsamında suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır.

2.Taraf devletler, yukarıda Paragraf 1'de tanımlanan eylemi, ciddi zarara yol açması koşuluna bağlama haklarını saklı tutabilirler."

Bu hükmün amacı, bilgisayar verilerini ve bilgisayar programlarını da, maddi varlığa sahip nesneler gibi, kasten hasar verme eylemlerine karşı koruma altına almaktır. Burada korunan hukuki yarar, depolanmış bilgisayar verileri ya da bilgisayar programlarının bütünlüğü ve uygun biçimde çalışmaları ve kullanımıdır.

Burada "tahrip etmek" ve "bozmak", özellikle veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz biçimde değiştirilmesi demektir. Verilerin "silinmesi", maddi bir cismin imhası gibidir. Veriler imha edilir ve tanınmaz hale getirilir. Bilgisayar verilerinin erişilmez kılınması, verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişi için verile-

rin ulaşılabilirliğini önleyen ya da sona erdiren herhangi bir eylem anlamındadır. "Değiştirme" terimi ise, mevcut verilerin farklı bir hale getirilmesi anlamındadır. Virüs ve Truva atı gibi kötü amaçlı kodların sisteme sokulması ile erişilmez duruma getirme de, bu nedenle, verilerin sonuçta farklı bir hale gelmesi gibi, bu paragrafın kapsamındadır.

Yukarıdaki fiiller ancak "hukuka aykırı olarak" gerçekleştirildiği takdirde cezalandırılabilir.

Ağların tasarımının ayrılmaz bir parçası olan yaygın faaliyetler veya işletmeyle ilgili ya da ticari yaygın uygulamalar -örneğin bir bilgisayar sisteminin güvenliğinin sahibi ya da işletmecisinin izniyle test edilmesi ya da korunması, ya da sistemin işletmecisi yeni bir yazılım edindiğinde (örneğin İnternet'e erişim sağlayan, daha önce yüklenmiş benzer programları çalışmaz hale getiren bir yazılım) bilgisayarın işletim sisteminin konfigürasyonunun değişmesi- hukuka uygundur ve dolayısıyla bu Madde çerçevesinde suç olarak tanımlanmamaktadır. Anonim iletişimleri kolaylaştırmak amacıyla trafik verilerinin farklı bir hale getirilmesi (örneğin anonim yeniden postalama sistemleri), ya da güvenli iletişim amacıyla verilerin farklı bir hale getirilmesi (örneğin şifreleme), ilke olarak gizliliğin meşru bir koruması olarak görülmeli ve hukuka uygun biçimde yapılmış oldukları kabul edilmelidir. Ancak, Taraflar, anonim iletişimle ilgili belli suiistimalleri, örneğin suçlunun kimliğini gizlemek için paket başlık bilgilerinin değiştirildiği durumları suç olarak tanımlamak isteyebilirler.

Ayrıca, failin "kasten" hareket etmiş olması gerekmektedir.

Paragraf 2, Tarafların ciddi zararla sonuçlanan fiillerle ilgili olarak haklarını saklı tutmalarına izin vermektedir. Neyin ciddi zararları oluşturduğunun yorumu ulusal mevzuatça yapılacaktır, ancak Taraf Devletler bu haklarını saklı tutma imkanından yararlanırlarsa çekincelerini Avrupa Konseyi Genel Sekreteri'ne bildirmelidirler.

4- Sistemlere Müdahale (m.5)

Taraf Devletlerden her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve hukuka aykırı bir şekilde engelleme fiilinin, kasten yapıldığında kendi ulusal mevzuatı kapsamında bir suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır.

(89) 9 sayılı Tavsiye Kararında bundan bilgisayar sabotajı olarak söz edilmektedir. Hükmün amacı telekomünikasyon olanakları da dahil olmak üzere bilgisayar sistemlerinin hukuka uygun olarak kullanımının, (bilgisayar verileri kullanılarak ya da bu veriler etkilenerek) uluslararası düzeyde engellenmesi eyleminin suç olarak belirlenmesidir. Korunan hukuksal değer, bilgisayar ya da telekomünikasyon sistemlerinin işletmecilerinin ve kullanıcılarının bu sistemleri uygun biçimde işletme haklarıdır. Metin her tür işleyiş biçiminin koruma altına alınmasını sağlayabilecek şekilde formüle edilmiştir.

"Engelleme" terimi, bilgisayar sisteminin uygun işleyişine müdahale eden eylemler için kullanılmıştır. Bu engelleme, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak yoluyla yapılmış olmalıdır.

Ceza yaptırımına yol açması için engellemenin ayrıca "önemli boyutta" olması gerekir. Taraf Devlet engellemenin "önemli boyutta" sayılması için hangi ölçütlerin gerçekleşmesi gerektiğine kendisi karar verecektir. Sistemin işleyişini önleyen ya da önemli ölçüde yavaşlatan virüs gibi kötü amaçlı kodlar, ya da bir alıcıya sistemin iletişim işlevlerini engellemek üzere çok büyük miktarlarda elektronik posta gönderen programlar bu kapsamda düşünülebilir.

Engelleme "hukuka aykırı olarak" yapılmış olmalıdır. Örneğin, bir bilgisayar sisteminin güvenliğinin sahibi ya da işletmecisinin izniyle test edilmesi ya da korunması, ya da sistemin

işletmecisi daha önce yüklenmiş benzer programları çalışmaz hale getiren yeni bir yazılım edindiğinde bilgisayarın işletim sisteminin konfigürasyonunun değişmesi gibi eylemler, "önemli boyutta" engellemeye yol açsalar da bu Madde çerçevesinde suç olarak tanımlanmamaktadır.

Ticari ya da başka amaçlarla istenilmemiş e-postaların gönderilmesi, özellikle büyük miktarlarda ve çok sık bir biçimde gerçekleştirildiğinde (*"spamming"*) alıcıyı rahatsız edebilir. Bu eylem ancak iletişimi kasıtlı olarak ve önemli boyutta engellediğinde suç olarak tanımlanmalıdır. Ancak, Tarafların mevzuatlarında engelleme için farklı yaklaşımlar bulunabilir. Örneğin belli müdahale fiilleri idari suçlar olarak tanımlanabilir ya da başka şekillerde yaptırıma tabi kılınabilir. Metin, mevzuatlarında idari ya da ceza yaptırımı gerektirecek zarar eşiğine ulaşmak için sistemin işleyişinin ne dereceye kadar -kısmen ya da tamamen, geçici ya da kalıcı olarak- engellenmesi gerekeceğini belirlemeyi Taraflara bırakmaktadır.

Suç *kasten* işlenmiş olmalı, yani fail ciddi ölçüde engelleme kastıyla hareket etmiş olmalıdır.

5- Cihazların Kötüye Kullanımı (m.6)

Bu maddede nitelikleri belirtilen bilgisayar sistemlerinin veri veya programlarının önceki maddelerde belirtilen eylemleri gerçekleştirmek amacıyla üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilmesi konusu düzenlenmektedir.

"1.Taraf Devletlerden her biri, aşağıdaki eylemlerin, kasten ve hukuka aykırı olarak yapılması halinde kendi ulusal mevzuatları kapsamında suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır.

a. Aşağıda sayılanların, Madde 2 ila 5'te tanımlanan eylemleri gerçekleştirmek için üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilmesi:

1-Bilgisayar yazılımları da dahil olmak üzere, esas itibariy-

le Madde 2 ila 5'te tanımlanan eylemlerden herhangi birinin gerçekleştirilmesi amacıyla tasarımlanmış veya bu amaca uygun hale getirilmiş cihazlar;

2-Bir bilgisayar sisteminin tamamına veya bir kısmına erişim sağlayan bilgisayar şifreleri, erişim kodları veya benzeri veriler,

b. Yukarıda (a) (1) ve (2) numaralı paragraflarda sözü edilen kalemlerin (parçaların), Madde 2 ila 5'te tanımlanan fiillere yönelik olarak kullanılmak amacıyla elde bulundurulması. Taraf Devletler, ceza sorumluluğunun doğabilmesi için elde bulundurulan kalemlerin belirli bir sayıyı aşması koşulunu arayabilirler.

2. Yukarıda Paragraf 1'de tanımlanan üretim, satış, kullanım amacıyla tedarik, ithal, dağıtım, başka surette elde etme veya elde bulundurma fiillerinin, işbu Konvansiyonun 2 ila 5 numaralı maddelerinde tanımlanan fiillere yönelik olarak kullanılmak amacıyla değil de, örneğin, bir bilgisayar sisteminin yetkili kişilerce test edilmesi veya korunması amacıyla yapıldığı durumlarda, işbu madde hükümleri ceza sorumluluğu doğurur şekilde yorumlanmayacaktır.

3. Taraf Devletler, söz konusu hakkın 1(a) ve 2 numaralı paragraflarda belirtilen kalemlerin satışına, dağıtımına ve başka suretle kullanıma sunulmasına ilişkin durumlarda kullanılmaması şartıyla, işbu maddenin 1 numaralı paragrafını uygulamama haklarını saklı tutmaktadır.

Bu hükümle belli cihazlarla ilgili belirli hukuka aykırı eylemlerin kasten işlenmesi ya da bilgisayar sistemleri ve verilerinin gizliliği, bütünlüğü ve kullanıma açıklığına karşı yukarıda tanımlanan suçları işlemek üzere verilere erişilmesi ayrı ve bağımsız bir suç olarak tanımlanmaktadır. Bu suçları işlemek genellikle erişim araçlarının ("hacker araçları") ya da başka araçların bulundurulmasını gerektirdiği için, bu araçları suç işlemek üzere elde etmeye yönelik, üretim ve dağıtımları alanında bir tür karaborsanın doğmasına yol açabilecek, güçlü bir eğilim vardır. Bu tehlikelerle daha etkin bir biçimde mücadele edebilmek için, ceza hukuku tehlike potansiyeli taşıyan belirli

fiilleri, Madde 2 - 5'te tanımlanan suçların işlenmesinden önce, kaynağında yasaklamalıdır. Bu açıdan hüküm, Avrupa Konseyi'ndeki (şartlı erişime dayalı olan ya da şartlı erişim içeren hizmetlere yasal koruma üzerine Avrupa Konvansiyonu - 178 sayılı ETS) ve Avrupa Birliği'ndeki (Avrupa Parlamentosu'nun ve 20 Kasım 1998 tarihli Konseyin şartlı erişime dayalı olan ya da şartlı erişim içeren hizmetlere yasal koruma üzerine 98/84/EC sayılı Direktifi) bazı yeni gelişmelere ve bazı ülkelerdeki ilgili hükümlere dayanmaktadır. Kalpazanlık üzerine 1929 Cenevre Konvansiyonunda benzer bir yaklaşım benimsenmiştir.

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

Konvansiyon taslağı kaleme alınırken, cihazların münhasıran ya da spesifik olarak suç işlemek üzere tasarımlanmış cihazlarla sınırlı tutulması ve dolayısıyla çift kullanımlı cihazların kapsam dışı bırakılması konusu ayrıntılı olarak tartışılmıştır. Bunun kapsamının çok dar olacağı düşünülmüştür. Böyle bir yaklaşım, hükmü uygulanamaz ya da sadece ender durumlarda uygulanabilir hale getirerek, ceza davalarında üstesinden gelinemeyecek delil bulma güçlüklerine yol açabilir. Alternatif olarak, yasal olarak üretilmiş ve dağıtılmış bile olsa bütün cihazları kapsam dahiline almak görüşü de reddedilmiştir.

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

Ceza sorumluluğunun doğması için gerekli kalemlerin sayısına karar vermek taraflara bırakılmıştır.

Suç kasten ve hukuka aykırı olarak işlenmiş olmalıdır. Cihazların, sistemlerine karşı saldırılar düzenlemek gibi, hukuka uygun amaçlarla üretildiği ve piyasaya sunulduğu durumları da suç olarak tanımlama tehlikesinden kaçınmak için suçu sınırlayacak başka unsurlar eklenmiştir. Genel kastın ötesinde, cihazın işbu Konvansiyonun 2-5. Maddelerinde belirtilen suçları işlemek amacıyla kullanıldığını gösteren özel bir kast da bulunmalıdır.

Bir bilgisayar sisteminin izinli olarak denenmesi veya korunması amacıyla yaratılan araçların hükmün kapsamı dışında olduğu Paragraf 2'de açıkça "hukuka aykırı bir şekilde" ifadesinde belirtilmiştir. Örneğin, sektör tarafından bilgi teknolojisi ürünlerinin güvenilirliğini kontrol etmek ya da sistem güvenliğini test etmek için tasarımlanmış olan test cihazları ("cracking cihazları") ve ağ analiz cihazları meşru amaçlarla üretilmiştir ve "bunların hukuka uygun bir biçimde" kullanıldıkları kabul edilmektedir.

Ulusal mevzuatlarda suçu sınırlamaya izin verilmiştir. Ancak, Taraflar, paragraf 1 (a) 2'de belirtildiği gibi, en azından bilgisayar şifreleri ve erişim verilerinin satışını, dağıtımını ve elde edilebilir hale getirilmesini suç olarak tanımlamak zorundadır.

B- Bilgisayarlarla İlişkili Suçlar

Günümüzde internet yoluyla yapılan kredi kartı yolsuzluklarının ve benzeri eylemlerin tüm dünyada fazlasıyla çoğalması ve önemli ekonomik kayıplara yol açması açısından klasik sahtecilik ve dolandırıcılık hükümlerinin yetersiz kaldığı ülkeler açısından düzenleme yapılması gerekmektedir.

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

"Bilgisayarlarla ilişkili sahtecilik eylemleri" ve "Bilgisayarlarla ilişkili dolandırıcılık eylemleri", bilgisayarlarla ilişkili belirli suçları, yani bilgisayarlarla ilişkili sahtecilik ve bilgisayarlarla ilişkili dolandırıcılığı, bilgisayar sistemlerinin ve bilgisayar verilerinin manipülasyonunun iki özel türü olarak ele almaktadır. Bu suçların kapsam dahiline alınması, bazı geleneksel hukuki yararların birçok ülkede yeni müdahale ve saldırı biçimlerine karşı yeterince korunmadığı gerçeğinden kaynaklanmaktadır.

1- Bilgisayarla İlişkili Sahtecilik Eylemleri (m.7)

"Taraf Devletlerden her biri, söz konusu verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiilinin, söz konusu farklı verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasten ve hukuka aykırı olarak yapıldığında kendi ulusal mevzuatı kapsamında birer suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır. Taraf Devletler, bu gibi durumlarda ceza sorumluluğunu, hile veya benzeri bir dürüstlüğe aykırı amacın mevcut olması koşuluna bağlayabilirler."

Bu Maddenin amacı, belgelerde sahteciliğe paralel bir suç

oluşturmaktadır. Ceza hukukundaki, bir belgedeki ifadelerin ya da beyanların görsel olarak okunabilirliğini şart koşan ve elektronik olarak saklanan verilere uygulanamayan geleneksel sahtecilikle ilgili boşlukların doldurulması amaçlanmaktadır. Delil teşkil eden bu tür verilerin manipülasyonu, üçüncü bir şahsın yanlış yönlendirilmesine neden oluyorsa geleneksel sahtecilikle aynı ciddi sonuçlara yol açabilir. Bilgisayarlarla yapılan sahtecilik, verilerde içerilen bilgilerin doğruluğuna dayalı hukuki işlemler sırasında verilerin delil olarak değerlerini değiştirmek üzere izinsiz olarak veri yaratılması ya da saklanan verilerin değiştirilmesi yoluyla kandırmaya yöneliktir. Korunan hukuki yarar, hukuki ilişkiler açısından sonuç doğurabilecek elektronik verilerin güvenliği ve güvenilirliğidir.

Günümüzde, ulusal sahtecilik kavramlarının çok çeşitlilik gösterdiği unutulmamalıdır.

Bu hüküm, yasal geçerliliği olan hem resmi hem de özel belgenin eşdeğeri olan verileri kapsar. Doğru ve yanlış verilerin izinsiz olarak "ilave edilmesi", sahte bir belgenin üretilmesi ile aynı anlamdadır. Daha sonraki değiştirmeler (farklı hale getirme, farklı biçimlerini üretme, kısmi değişiklik), silme (verilerin veri ortamından çıkarılması) ve erişilemez kılma (verilerin gizli tutulması, saklanması) genel olarak hakiki bir belgenin tahrifi ile eşanlamlıdır.

Hükmün son cümlesi Tarafların suçu ulusal mevzuatlarına uygularken ceza sorumluluğunu hile veya benzeri bir dürüstlüğe aykırı amacın mevcut olması şartına bağlamalarına izin vermektedir.

2- Bilgisayarla İlişkili Dolandırıcılık Eylemleri (m.8)

Taraf Devletler, aşağıdaki faaliyetlerde bulunmak suretiyle bir başkasının malvarlığının ziyaına sebep olma eyleminin, kasten ve hukuka aykırı olarak yapıldığında, kendi ulusal mevzuatı kapsamında suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır:

2- Dolandırıcılık suretiyle kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma;

3- Dolandırıcılık suretiyle kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme.

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

Bütün olası manipülasyonları kapsam dahiline almak için Madde 8(a)'daki "yeni veriler ekleme", "değiştirme", "silme" veya "erişilmez kılma" şeklindeki unsurlara Madde 8(b)'deki "bir bilgisayar programı ya da sisteminin işleyişine herhangi bir müdahale" şeklinde kapsayıcı bir eylem de eklenmiştir. "Veri ekleme, değiştirme, silme ve veya erişilmez kılma" unsurları, bir önceki Maddedekiyle aynı anlamdadır. Madde 8(b), donanım manipülasyonları gibi fiilleri, yazıcı çıktılarını erişilmez kılmaya yönelik fiilleri ve verilerin kaydedilmesini ya da akışını ya da programların çalışma sırasını etkilemeye yönelik fiilleri kapsamaktadır.

Bilgisayar dolandırıcılığı manipülasyonları, başka bir kişinin malvarlığından doğrudan ekonomik kayba ya da zilyetlik kaybına yol açıyorsa ve fail kendisi ya da bir başkası için kanunsuz ekonomik kazanç sağlamayı amaçladıysa suç olarak tanımlanır. Geniş bir kavram olan "mülkiyetin kaybı" terimi, paranın, ekonomik değeri olan maddi ve gayrimaddi varlıkların kaybını ifade eder.

Suç "hukuka aykırı bir biçimde" işlenmiş ve haksız bir ekonomik çıkar sağlanmış olmalıdır. Şüphesiz, maddi menfaat sağlamayı amaçlayan meşru yaygın ticari uygulamaların bu Maddede tanımlanan suça dahil edilmeleri düşünülmemiştir, çünkü bu uygulamalar hukuka uygun biçimde gerçekleştirilmektedir. Örneğin, etkilenen kişilerle yapılmış geçerli bir sözleşmeye uygun olarak yürütülen faaliyetler hukuka uygun olarak gerçekleştirilmektedir (örneğin sözleşme hükümlerine uygun biçimde bir web sitesini çalışmaz hale getirmek).

Suç *kasten* işlenmiş olmalıdır. Genel kast unsuru bir başkasının mülkiyetinin kaybına yol açan bilgisayar manipülasyonu ya da müdahale anlamındadır. Suç ayrıca işleyenin kendisi ya da bir başkasına maddi ya da başka tür dürüst menfaat sağlamak amacıyla özel bir hile ya da başka tür bir dürüst olmayan niyetin varlığını da şart koşmaktadır. Bu nedenle, örneğin, piyasa rekabeti çerçevesinde yürütülen, bir kişiye maddi zarar ve bir başkasına kazanç sağlayan, ama hile ya da başka tür bir dürüst olmayan niyetle gerçekleştirilmiş olmayan ticari faaliyetlerin bu Maddede tanımlanan suça dahil edilmeleri amaçlanmamıştır. Örneğin, İnternet'te karşılaştırmalı alışveriş için kullanılan bilgi toplama programlarının ("bot") kullanımının, "bot"un ziyaret ettiği siteden izin alınmamış olsa bile suç olarak tanımlanması düşünülmemektedir.

C- Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar (m.10)

Burada fikri haklara ilişkin olarak bugüne kadar yapılmış sözleşmelere yollama yapılmakta ve bu sözleşmelerin bilgisayar sistemleri aracılığıyla ihlal edilmesinin suç haline getirilmesi gerekliliği vurgulanmaktadır.

"Taraf Devletlerden her biri, kendi yasalarında tanımlandığı şekliyle telif haklarının ihlali eyleminin, Edebiyat ve Sanat Eserlerinin Korunmasına Yönelik Bern Konvansiyonu çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WİPO Telif Hakları Anlaşması uyarınca, kasten, ticari ölçekte ve bir bilgisayar

sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlaka ilişkin haklar bu hükme tabi değildir.

Taraf Devletlerden her biri, kendi yasalarında tanımlandığı şekliyle telif haklarına benzer hakların ihlali fiilinin, Roma'da imza edilen Oyuncuların, Plak Yapımcılarının ve Yayım Kuruluşlarının Korunması Hakkında Konvansiyon (Roma Konvansiyonu), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Oyunculuk ve Plakçılık Anlaşması uyarınca , kasten, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla yapıldığında, kendi ulusal mevzuatı kapsamında bir suç olarak tanımlanması için gerekli olabilecek yasama faaliyetlerini ve diğer işlemleri yapacaktır. Sözü geçen Konvansiyonlar çerçevesinde verilen ahlaka ilişkin haklar bu hükme tabi değildir.

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

D- İçerikle İlişkili Suçlar:

1-Çocuk Pornografisiyle İlişkili Suçlar

" Taraf Devletlerden her biri, aşağıdaki eylemlerin kasten yapıldığında kendi ulusal mevzuatı kapsamında bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

a-bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek;

b-bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak ya da çocuk pornografisine erişim sağlamak,

c- bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ya da yaymak,

d-kişinin, bir bilgisayar sistemi üzerinden kendisi ya da başkası için çocuk pornografisi temin etmesi,

e- bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak.

Yukarıdaki paragraf 1'de geçen "çocuk pornografisi" terimi aşağıdakileri görsel anlamda teşhir eden pornografik malzemeler anlamına gelmektedir.

a-cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı,

b-cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı,

c- cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren gerçeğe benzer görüntüler,

Yukarıdaki paragraf 1'de geçen "reşit olmayan kişi" terimi, 18 yaşından küçük kişiler anlamına gelmektedir. Ancak Taraflardan herhangi biri, daha düşük bir yaş sınırı belirleyebilir. Söz konusu yaş sınırı 16'dan az olmayacaktır.

Taraflardan her biri, paragraf 1(d) ve 1(e), ayrıca 2(b) ve 2(c) yi kısmen uygulama ya da hiç uygulamama haklarını saklı tutar.

Çocuk pornografisiyle ilgili olan Madde 9'da ceza hukuku hükümlerini, çocuklara karşı işlenen cinsel suçlarda bilgisayar sistemlerinin kullanımını daha iyi kapsayacak şekilde modernleştirerek, cinsel sömürüye karşı korunmaları da dahil olmak üzere çocuklarla ilgili koruyucu önlemler güçlendirilmeye çalışılmıştır.

Bu hüküm, Avrupa Konseyi Devlet ve Hükümet Başkanlarının 2. zirvesinde (Strasbourg, 10 - 11 Ekim 1997) hazırlanan Eylem Planında (madde III.4) belirtilen kaygılara cevap olarak

hazırlanmıştır ve çocuk hakları, çocukların satışı, çocuk fuhşu ve çocuk pornografisine ilişkin BM Konvansiyonunun Seçmeli Protokolünün kısa bir süre önce benimsenmesinde ve Avrupa Komisyonunun kısa bir süre önce başlattığı çocukların cinsel sömürüsü ve çocuk pornografisiyle mücadele girişiminde (COM2000/854) görülen çocuk pornografisini yasaklamaya yönelik uluslararası trendle de uyumludur.

Bu hükümle çocuk pornografisinin elektronik üretimi, bulundurulması ve dağıtımının çeşitli yönleri suç olarak tanımlanmıştır. Çoğu Devletin çocuk pornografisinin geleneksel üretimini ve fiziksel dağıtımını suç olarak tanımlamış durumda olmasına rağmen, bu tür malzemelerin alışverişinde başlıca araç olarak İnternet'in kullanımının giderek artması karşısında çocukların bu yeni cinsel sömürü ve tehdit biçimine karşı savunulması için uluslararası hukuki bir belgeye özel hükümlerin yerleştirilmesi yaşamsal önem taşımaktadır. Bu materyallerin ve pedofillerin fikir, fantezi ve tavsiye değiş tokuşunda bulunmaları gibi online uygulamaların çocuklara karşı işlenen cinsel suçları beslemekte, teşvik etmekte veya kolaylaştırmakta rol oynadığı, yaygın olarak paylaşılan bir görüştür.

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

Paragraf 1(b)'de bir bilgisayar sistemi üzerinden çocuk pornografisi "sunmak" suç olarak tanımlanmıştır. "Sunmak" kelimesi teklif etmek anlamındadır. Ayrıca çocuk pornografisi elde etmek amacıyla başka kişilere başvurmayı da kapsaması amaçlanmıştır. Bu, malzemeyi sunan kişinin onu gerçekten sağlayabileceği anlamına gelmektedir. "Erişim sağlamak" ifadesinin, örneğin bir çocuk pornografisi sitesi oluşturarak, başkalarının kullanımı için çocuk pornografisini online erişime sunmayı kapsaması amaçlanmıştır. Bu paragrafta, çocuk pornografisine erişimi kolaylaştırmak için çocuk pornografisi sitelerine hyperlink'lerin yaratılması ve derlenmesinin de kapsanması amaçlanmaktadır.

Paragraf 1(c)'de bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ve yaymak suç olarak tanımlanmıştır. "Dağıtım" malzemenin aktif olarak yayınlanmasıdır. Bir bilgisayar sistemi üzerinden başka bir kişiye çocuk pornografisi göndermek, çocuk pornografisi "yayma" suçu olarak ele alınacaktır.

Paragraf 1(d)'deki "kendisi ya da başkası için temin etmek" terimi, örneğin bilgisayarına indirme (download) yoluyla, aktif olarak çocuk pornografisi elde etmek anlamındadır.

Bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda, örneğin bir disket ya da CD-Rom'da, çocuk pornografisi bulundurmak paragraf 1(e)'de suç olarak tanımlanmıştır. Çocuk pornografisi bulundurmak bu tür malzeme için talebi canlandırır. Üretimden bulundurmaya kadar zincirin bütün parçalarının failleri için ceza sorumluluğu getirmek, çocuk pornografisi üretimini azaltmanın etkin bir yoludur.

Paragraf 2'deki "pornografik malzemeler" terimi, malzemelerin müstehcen, kamu ahlakına aykırı ve benzer biçimde ahlak dışı şeklinde sınıflandırılması açısından ulusal standartlar esas alınacaktır. Bu nedenle, sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan materyal pornografik olmayan materyal olarak görülebilir. Görsel teşhir, bilgisayar disketi ya da başka elektronik saklama ortamlarında saklanan, görsel materyale dönüştürülebilen verileri de içine alır.

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

Paragraf 2'de tanımlanan, paragraf 1'de belirtilen suçları

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

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

"Hukuka aykırı biçimde" terimi, yani hukuka özel aykırılık, özel şartlar altında bir kişiyi sorumluluktan kurtaracak hukuka uygunluk nedenlerini sorumluluk dışında tutmaktadır. Dolayısıyla, "hukuka aykırı biçimde" terimi Devletin düşünce, ifade ve özel hayat özgürlüğü gibi temel hakları göz önünde bulundurmasına izin vermektedir. Ayrıca, taraf Devletler sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan "pornografik malzeme"yle ilgili eylemlere ilişkin bir çekince koyabilir. "Hukuka aykırı biçimde" terimi, paragraf 2(b)'yle ilgili olarak da, örneğin Taraf Devletlerin gösterilen kişinin bu hükümde kullanılan anlamda reşit olmayan bir kişi olmadığının saptanması durumunda bu kişinin cezai sorumluluğundan kurtulmasını sağlamalarına da izin verebilir.

Paragraf 3'te "reşit olmayan kişi" terimi, çocuk pornografisiyle ilgili olarak, BM Çocuk Hakları Konvansiyonundaki "çocuk" tanımına (Madde 1) uygun biçimde, genel olarak 18 yaşından küçük herkes şeklinde tanımlanmıştır. Yaş konusunda tek bir uluslararası standart belirlemek önemli bir politika olarak

görülmüştür. Burada söz edilen yaşın (gerçek ya da kurgusal) çocukların cinsel nesne olarak kullanılmasıyla ilgili olduğu ve cinsel ilişki için izin yaşından farklı olduğu göz önünde bulundurulmalıdır. Ancak, belli ülkelerin çocuk pornografisiyle ilgili ulusal mevzuatlarında bir alt yaş sınırı getirdiği göz önüne alınarak, paragraf 3'ün son cümlesinde, Tarafların, 16'dan küçük olmamak şartıyla, farklı bir yaş sınırı getirmelerine izin verilmiştir.

Bu Maddede, Tarafların, çocuk pornografisiyle ilgili olarak, Madde 2-8'de olduğu gibi "kasten hareket etmekte iseler suç olarak tanımlamak zorunda oldukları yasadışı eylemleri sıralanmıştır. Bu hükme göre, çocuk pornografisi sunmak, erişim sağlamak, dağıtmak, yaymak, üretmek ya da bulundurmak konusunda kastı olmayan bir kişi sorumlu tutulamaz. Taraflar daha spesifik bir standart benimseyebilirler (bkz., örneğin, hizmet sağlayıcı yükümlülükleriyle ilgili geçerli Avrupa Topluluğu yasası) ve bu durumda bu standart geçerli olur. Örneğin, yayılan ya da saklanan bilgi üzerinde "bilgi ve kontrol" mevcutsa yükümlülük doğabilir. Örneğin bir hizmet sağlayıcısının, ulusal mevzuatta bu konuyla ilgili gerekli kastı olmaksızın bir taşıyıcı işlevi üstlenmesi ya da bu tür malzemeler içeren bir web sitesi ya da haber odasını barındırması sorumluluğu için yeterli değildir. Ayrıca, bir hizmet sağlayıcı, ceza sorumluluğundan kurtulmak için fiilleri denetlemek zorunda değildir.

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

II- Siber Suç Sözleşmesi Karşısında Türkiye'nin Durumu

Siber Suç Sözleşmesi henüz Türkiye tarafından imzalanmamakla beraber bu sözleşmenin Giriş bölümünde yollama

yapılan temel uluslararası sözleşmeleri Türkiye imzalamıştır. Sözleşmelerden bir kısmı bireyin düşüncelerini ifade etmesi, her türlü bilgiye ulaşmak, bilgiyi iletmek ve özel yaşama saygıyı özellikle vurgulayan A.İ.H.S (1950), B.M. Siyasal ve Sivil Haklar Sözleşmesi (1966), Çocukları Korumayı Amaçlayan B.M. Çocuk Haklarına Dair Sözleşme (1989), Kötü Koşullardaki Çocuk İşçiliğinin Yasaklanması ve Ortadan Kaldırılmasına İlişkin Acil Önlemler Hakkında 182 sayılı ILO Sözleşmesi (2001) gibi...

Burada özellikle B.M. Çocuk Haklarına Dair Sözleşme, Türkiye adına 14.09.1990 tarihinde imzalanmış, 27.01.1995 gün ve 22184 sayılı R.G. de yayınlanarak yürürlüğe girmiştir. Çocukların "Magna Carta"sı olarak tanımlanan bu sözleşme çocuk haklarını her yönü ile düzenlemektedir. Madde 1 "...on sekiz yaşına kadar her insan çocuk sayılır" demektedir. Sözleşme ayrıca taraf Devletlere çocuğun bedensel, zihinsel, ruhsal, ahlaki ya da toplumsal gelişmesine zararlı olabilecek nitelikte çalıştırılmasına karşı koruma sağlar (m. 32). Ayrıca Devletler çocuğa her türlü cinsel sömürüye ve cinsel istismara karşı koruma güvencesi verirler. Özellikle,

a) Çocuğun yasadışı bir cinsel faaliyete girişmek üzere kandırılması veya zorlanmasını,

b) Çocukların fuhuş ya da diğer yasadışı cinsel faaliyette bulundurularak sömürülmesini,

c) Çocukların pornografik nitelikteki gösterilerde ve malzemede kullanılmasını önlemek amacıyla ...ulusal ve uluslararası düzeyde gerekli her türlü önlemi alırlar (m. 34).

25 Mayıs 2000 tarihinde B. Milletler, B.M. Çocuk Hakları Sözleşmesine ek olarak, iki ihtiyari (optional) protokol kabul etmiştir. Bunlardan biri Seks Ticareti Protokolü'dür. Giriş bölümünde, taraf Devletlerin çocukları, çocuk satımına ve çocuk pornografisine karşı korumayı taahhüt ettikleri belirtilmekte ve çocuğun her türlü istismardan ve sosyal gelişimine engel olabilecek çalışmalardan korunmaya hakkı olduğu vurgulanmaktadır. Bu protokol çocuk mağdurları yeterli bir derecede

korumadığı yönünde eleştirilmiştir. Ancak bu konuda uluslararası bir bilinç yaratması açısından yararlı olmuştur.

03.02.2001 tarihinde 24307 numaralı R.G.'de yayınlanmış olan 182 sayılı İLO Sözleşmesi de 2. maddesinde "çocuk" teriminin 18 yaşın altındaki herkesi kapsadığını ifade etmektedir.

Sözleşmenin amaçları bağlamında kötü koşullardaki çocuk işçiliğinin türleri belirtilirken (m.3) zorla çalıştırma ve kölelik yanında, çocuğun fahişelikte, pornografik yayınların üretiminde veya pornografik gösterilerde kullanılması, bunlar için tedariki ve sunumu açıkça sayılmaktadır.

Öte yandan çocuk pornografisinin internet ortamında giderek yaygınlaşması, bu yasadışı çocuk ticaretini körüklemekte ve özellikle "cinsel turistlerin" ve pedofillerin fazlasıyla ilgisine mazhar olmaktadır. Bu tür ticari cinsel istismarın en başta gelen hedefleri çocuklar olmaktadır, özellikle sosyal açıdan daha alt durumda olan çocuklar: azınlıklar, mülteciler, sokak çocukları, fakir çocuklar, boşanmış anne-babanın çocukları, özürlü çocuklar. Örneğin, ABD'de, yılda 500 bin çocuğun evden kaçtığı ya da atıldığı ve bunların günlük yemek ve barınma gereksinimlerini karşılamak için fuhuş yaptıkları ve organize suç örgütleri tarafından istismar edildikleri saptanmıştır.

Günümüzde çocuk köleliği; çocuk ticareti, çocuk fahişeliği ve çocuk pornografisi şeklini almıştır. Bu köle çocuklar hem maddi hem manevi istismar ile karşılaşmaktadırlar. Irza geçme, işkence, aç bırakılma, hapsedilme, ölümle tehdit ve kötü muamele. Ayrıca bunlar ölümcül hastalıklara da kolayca yakalanabilmektedirler. Örneğin, AİDS. Ayrıca bu çocuklar damgalanmakta, depresyona girmekte ve travma sonrası strese maruz kalmaktadırlar.

III- Çocuk Pornagrafisinin Genel Görünümü ve Etkileri

Avrupa Konseyi Siber Suç Sözleşmesi; bütün bu çalışmaların özellikle çocuk pornografisiyle mücadelede geldiği son noktadır. Bu sözleşmeye taraf olmadan çocuk pornografisi ile baş etmek mümkün olamaz, zira çocuk pornografisi sanal or-

tamda daha yaygın ve daha kolay erişilebilir bir nitelik göstermektedir. Çocuk pornografisi en yıkıcı ve zararlı şeklini internet aracılığı ile alabilmiştir ve çocukların cinsel istismarında çok belirleyici bir faktör haline gelmiştir.

Öte yandan bilgisayar endüstrisi o denli hızlı gelişmektedir ki bu çocuk pornografisi ile uğraşanlara ucuz ve kullanıcı dostu (user friendly) şifreli yazılımlar sağlamakta, kovuşturma örgütlerine ise dosyaların deşifre edilmesinde büyük güçlükler çıkarmaktadır. Kolluk görevlileri görüntüye ulaşsalar da bunun dağıtımına engel olamamaktadırlar. Bir görüntü internete girdiğinde hızlı bir şekilde çok sayıda kullanıcı tarafından kendi cihazlarına yüklenebilmekte ve kalitesinden hiçbir şey yitirmeden geometrik bir hızla çoğaltılabilmektedir.

İnternet ayrıca çocuk istismarlarının ve pedofillerin birbirini kolayca bulmalarına da olanak sağlar; ev yapımı pornografik faaliyetlerin geniş kitlelere ulaşabilmesini hatta dünyanın bir ucundan diğerine kadar çabucak yayılabilmesini sağlar. Örneğin, Türkiye'de (Bursa'da) çocuklara rehberlik ve psikolojik danışmanlık yapan bir kişi tecavüz ve tasaddide bulunduğu çocukların görüntülerini internet yoluyla tüm dünyaya yayabilmektedir.

Erişkinlere ait müstehcen görüntülerin yayınlanması mağdursuz suçtur. Günümüzde bunun yayınlanması ya da seyredilmesi önemsenmemektedir. Ancak çocuk pornografisinde gerçek bir mağdur bulunmaktadır, hatta gerçekten bir çocuk bu cinsel faaliyete katılmamış ve görüntüye çocuk resmi sonradan eklenmiş olsa bile.

Çocuk pornografisinin yaygın hale gelmesi hem çocuklarda bunun "olağan" ve "normal" bir şey olduğu duygusunun yerleşmesine yol açar ve ruh sağlıklarını kalıcı bir biçimde bozar, hem de pedofillerin hızlı bir şekilde çoğalmasına neden olur. Biz ifade özgürlüğüne inanan ve sınırlandırılmasına hiç taraftar olmayan bir kişi olmamıza rağmen, çocuklarımızın korunabilmesi için bu tür sınırlamalara karşı olmadığımızı da belirtmeliyiz.

IV- Amerikan Hukukunda Son Gelişmeler

Yukarıda belirttiğimiz bu özel nedenledir ki, Amerikan Yüksek Mahkemesinin, "sanal" çocuk pornografisini yasaklayan 1996 tarihli Çocuk Pornografisini Önleme Yasasını, Amerikan Anayasasının 1. ekine aykırı bularak kısmen iptal etmesini eleştiriyoruz. Ashcroft v. Free Speech Coalition (İfade Özgürlüğü Koalisyonu) davasında Yüksek Mahkemenin 6 yargıcı bu yasayı 15.04.2002 günü Anayasaya aykırı bulmuş, bir yargıç kısmen aykırı görmüş, iki yargıç ise iptaline karşı oy kullanmıştır. Çoğunluk adına Yargıç Kennedy bu tür yasaların anlatım ve sanat özgürlüğünü sınırlandırdığına ve "Amerikan Güzeli" ve "Trafik" gibi Hollywood filmlerini hatta Shakespeare'in Romeo ve Juliet gibi eserlerinin modern versiyonlarını, çocukların gerçekleştirdiği cinsellik içeren sahneler nedeniyle yasaklanamayacağını belirtmiştir. Ayrıca bu Yasa çok geniştir ve belirsiz olduğu için de ne tür görüntüleri kapsamına aldığı anlaşılmamaktadır" demektedir.

Başkan Rehnquist'in karşı oy yazısı ise sanal görüntülerin bazen gerçeğinden ayırt edilemediğini yoksa Amerikan Kongresi'nin Holywood filmlerinin yasa kapsamına girmesini amaçlamadığını vurgulamaktadır. Nitekim bu yasa yürürlükte olduğu dönemde "Trafik" ve "Amerikan Güzeli" gibi filmlerin ödül aldığını bu durumun ise, yasanın anlatımı ve sanat özgürlüğünü sınırlamayı amaçlamadığının en belirgin göstergesi olduğunu ortaya ifade etmektedir.

Yasa yalnızca sanal (virtual) pornografi açısından iptal edilmiştir. Pornograficinin, hiçbir cinsel faaliyette bulunmayan gerçek bir çocuk resmini manipüle ederek, çocuğun adeta cinsel faaliyette bulunduğu izlemini vermesi hala yasaktır.

Siber Suç Sözleşmesi ise sanal pornografinin de suç haline getirilmesini öngörmektedir. İmzacı Devletler arasında ise ABD de bulunmaktadır. Bu ise Amerikan hukuk çevrelerinin yeni tartışmalara gebe olduğunu göstermektedir.