

## İNTERNET KULLANIMINDA ORTAYA ÇIKABİLECEK BAZI CEZA HUKUKU SORUNLARI\*

*Yrd.Doç.Dr. Veli Özer ÖZBEK\*\**

### GİRİŞ

İnternetin modern toplumun en önemli kazanımlarından birisi olduğu konusunda bugün herkes görüş birliği içindedir. Gerçekten internet ticaretten eğitime, bilimsel araştırmadan sanata kadar hemen her alanda daha etkin bir çalışma olanağı ve avantajı sunmaktadır. Televizyon ve basın gibi diğer geleneksel iletişim (haberleşme) araçlarının aksine yeni haberleşme aracı olarak kendisini özellikle tüm içeriğinin dijital hale getirilmesi ile gösterir. Yine bu dijital yapı, veri ağında bulunan bilgilerin işlenmesini ve gönderilmesini mümkün kılmaktadır. Söz konusu veri ağı, sunucu<sup>1</sup> üzerindeki pek çok kişi arasında bilginin oldukça hızlı bir şekilde değişimini de sağlamaktadır. Nihayet yazı, resim ve sesin bir arada icrası ve kombine edilebilir olması, ayrı bir niteliği olarak, bu yeni iletişim aracının "Multimedia" (çokluortam) olarak nitelendirilmesine neden olmuştur<sup>2</sup>.

İnternet, aslında pek çok bilgisayarın birbiriyle bağlantısından başka bir şey değildir. Bunun için bilgisayarlar arasında iletişimi sağlamak amacıyla tek bir standartta bir araya gelmiş birbirine bağlı bir ağa ihtiyaç bulunur. Ancak bu

---

\* Bu çalışma 2000-2001 yılları arasında Alman Alexander von Humbold Vakfı tarafından verilmiş olan burs çerçevesinde bulunmuş olduğum Almanya'nın Giessen şehrinde kaleme alınmaya başlanmış ve büyük ölçüde Giessen Justus Liebig Üniversitesi Hukuk Fakültesi kütüphanesinden elde edilmiş eserlerden yararlanılarak tamamlanmıştır. Bu nedenle Humbold Vakfı ve bana son derece rahat ve güzel bir çalışma ortamı hazırlayan, yanında çalışmaktan onur duyduğum Prof.Dr. Walter Gropp'a teşekkür ederim.

\*\* DEÜ Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı Öğretim Üyesi

<sup>1</sup> =Anbieter

<sup>2</sup> Hilgendorf Eric, Die Neuen Medien und das Strafrecht, ZStW 113 (2001), s.650

ağ üzerinde iletişimi sağlamak için ortak bir dile gereksinim vardır; bu iletişim IP veya TCP esaslarına göre gerçekleştirilebilir<sup>3</sup>.

İnternet bir tür “bilgi otobanı” olarak da nitelenir. Bu çerçevede interneti, yani ağ tabanlı iletişimi, diğer iletişim ortamlarından ayıran özelliklerin çokluortam (multimedia), hipermetin (hypertext), paket anahtarlama (packet switching), eşzamanlılık ve etkileşimlilik olduğu söylenmektedir<sup>4</sup>. 1981 yılında sadece 300 olan bilgisayar sayısı bugün on milyonlarla ifade edilmektedir. Dünya nüfusunun yaklaşık onda biri internet ortamını kullanmaktadır<sup>5</sup>.

İnternet üzerindeki içeriklere ulaşmak da son derece kolaydır. Gerçekten bilgisayarın online hizmetinin başlangıç sayfası üzerindeki arama makinasına adresin yazılması ve giriş tuşuna basılması bunun için yeterlidir. Örneğin, Sex.com adresi ile bir kaç saniye içinde binlerce sayfa açılması mümkündür<sup>6</sup>.

Bununla birlikte, internetin toplum ve hukuk bakımından bazı sorunları da beraberinde getirdiği göz ardı edilemez bir gerçektir. İnternet, özellikle hukuksal alanda, pek çok yeni davranış şekilleri ile birlikte yeni sorunlar da ortaya çıkarmıştır. Gerçekten internetin ortaya çıkardığı yeni davranış biçimlerinden bir kısmının mevzuatta yer alan bazı suç tipleri ile örtüştüğü, bazılarının da yasa dışı, ahlak dışı ya da izin verilemeyecek davranışlar olarak nitelenebileceği görülmüştür. Üstelik bu sorunların, hukukun geleneksel yöntem ve araçlarıyla çözümlenmesi de oldukça zor görünmektedir. O halde, bu sorunların çözümlenmesi için söz konusu iletişim yönteminin tüm yönleriyle incelenerek analiz edilmesi gerekir.

İşte bu gelişme, söz konusu davranış şekillerinin ceza hukuku normlarını ihlal edip etmediği, ettiyse ne ölçüde ihlal ettiği sorununu ortaya çıkarmış ve tartışma konusu haline getirmiştir. Bugün internet, gittikçe artan oranda, çocuk pornografisi, özellikle şiddet içeren suç fiilini övme, radikal politik ve dini görüşlerin propagandasını içeren fiillerin işlendiği bir alan haline

<sup>3</sup> **Derksen** Roland, Strafrechtliche Verantwortung für in internationalen Computer-netzen verbreitete Daten mit strafbarem Inhalt, NJW 1997, 1878; **Finke** Thorsten, Die strafrechtliche Verantwortung von Internet-Providern, Tübingen 1998, s.2.

<sup>4</sup> **Atabek** Ümit, İnternet ve Sosyal Bilimlerde Metodoloji, Amme İdaresi Dergisi, C.34, Mart 2001, s.52.

<sup>5</sup> Bu rakam, 2002 yılı için 529 milyon, 2003 yılı için ise 793 milyon olarak tahmin edilmektedir. Türkiye ise, 2002 yılında 2.2 milyon, 2003 yılında ise yaklaşık 3 milyon internet kullanıcısı ile dünya sıralamasında 19.sırada bulunmaktadır ([www.gtreach.com/globstaats.evol.htm](http://www.gtreach.com/globstaats.evol.htm))

<sup>6</sup> **Finke**, 2

gelmiştir. Öte yandan, bu tür suçların daha çok organize suç örgütleri tarafından işleniyor olması, konunun ciddiyetini daha da artırmaktadır. Elbette, sorun sadece bu tür fillerin internet yoluyla işleniyor olduğunu tespit ile sınırlı olamaz. Önemli olan husus, bu filleri kimin işlediğini belirlemek ve özellikle ne şekilde cezalandırılacağını ortaya koyabilmektir. Gerçekten internetin milyonlarca kullanıcısının olduğu, bunların çoğunun kendi sayfasının bulunduğu ve her birinin kendine özgü içeriklerinin var olduğu hatırlandığında sorunun önemi ve hassasiyeti daha da belirginleşmektedir. Yine aşağıda açıklanmaya çalışılacağı üzere, bir iletişim ortamı olarak adlandırılabilir olan internetin bir sahibinin, işletenin ya da idarecesinin bulunmaması hukukçuları daha da güç duruma düşürmektedir. İnternet üzerinde işlenen suçların nerede işlendiği, hangi ülke kanunlarının uygulanacağını tespit bakımından büyük önem taşımaktadır. Nihayet, böylesine özgür bir ortamda soruşturma makamlarının nasıl ve hangi koşullar altında delil elde edebileceği de ayrı bir tartışma konusudur.

Bu çalışmada internet kullanımının ceza hukuku alanında ortaya çıkardığı sorunlardan başlıcaları ele alınacak, bu çerçevede öncelikle internet üzerinde işlenen suçlarda suçun işlendiği yer sorunu, suç faili, internet suçu kavramları üzerinde durulacak; daha sonra, internet kullanımının ceza muhakemesinde ortaya çıkardığı sorunlara değinilerek, özellikle internet üzerindeki haberleşme, en sık kullanılan şekli olarak da elektronik postanın denetlenmesi (e-mail) konuları incelenmeye çalışılacaktır. Ancak bütün bunlardan önce bu tartışmaya temel teşkil edecek internet ve işleyişi hakkında genel bir bilgi vermeyi uygun görmekteyiz.

## **I. İNTERNET VE CEZA HUKUKU**

### **A. TEMEL HAK VE ÖZGÜRLÜKLER, CEZA HUKUKUNUN İKİNCİL OLMA ÖZELLİĞİ VE İNTERNET**

20.yy.ın iletişim çağı olduğunu söylemek yanlış olmayacaktır. Matbaanın icadı ile başlayan iletişim süreci, radyo ve televizyon ile gelişmiş, nihayet internet ile en üst noktasına ulaşmıştır. Bunun bir yansıması olarak basın özgürlüğü kavramı önce sinema, ardından radyo ve televizyon ile zamanla yetersiz hale gelmiş, tüm modern iletişim araçlarını da içine alan iletişim özgürlüğü kavramı işte bu gereksinimin bir sonucu olarak ortaya

çıkıştır<sup>7</sup>. İletişim özgürlüğü aslında düşünce ve ifade özgürlüğünün bir yansımasıdır. Zira düşünceyi en iyi ifade etme araçlarından biri de kitle iletişimidir. Bu yönüyle iletişim özgürlüğü, tüm kitle iletişim araçlarını kapsayan bir anlama sahiptir. Zaman içinde üst bir kavram niteliğindeki iletişim özgürlüğü terimi yerine, spesifik olarak, söz konusu iletişim aracını esas alan mesela, radyo televizyon özgürlüğü gibi terimler tercih edilmiştir<sup>8</sup>. Bu açıdan haber ve düşüncelerin internet aracılığı ile kitlelere ulaştırılması özgürlüğünü “internet özgürlüğü” olarak tanımlamak mümkündür<sup>9</sup>. Bu anlamda sansür bu özgürlüğü kısıtlayacak en tehlikeli araçlardan biridir<sup>10</sup>.

İletişim, düşünce ve ifade özgürlüğünün en rahat kullanıldığı ortam olduğu şüphesiz olan internetin sınırlarüstü yapısı, üstünde etkin bir yönetim ve denetim mekanizması kurulmasını en azından teknik olarak olanaksız kılmaktadır. İnternet ortamında her an ulaşılabilir olma ve internet hizmetlerinden yararlanmak için hiç bir bürokratik engelin bulunmaması bireylere olağanüstü bir özgürlük ortamı sunmaktadır. Ancak, diğer iletişim araçlarında mümkün olmayan yasak bazı faaliyetlerin mümkün olabilmesi, madalyonun diğer yüzünü oluşturmaktadır. Gerçekten pornografiyi, ırkçı ve dinsel faaliyetleri konu alan her türlü web sitesine internet üzerinden ulaşabilmek mümkündür. Öte yandan, internet üzerinde özel hayata müdahale olanakları da oldukça fazladır.

<sup>7</sup> İÇEL Kayıhan, Haberleşme Özgürlüğü, İHFM, C.XLI, S.1-2 den ayrı bası, İstanbul 1975, s.1 vd.

<sup>8</sup> Karşl. Özbek V.Özer, Radyo-Televizyon Özgürlüğü ve Özel Radyo Televizyonlar, İzBD 1994, S.1, s.36 vd.

<sup>9</sup> Karşl. İÇEL Kayıhan, Kitle Haberleşme Hukuku, 4.Baskı, İstanbul 1998, s.23; Sınar Hasan, İnternet ve Ceza Hukuku, İstanbul 2001, s.48.

<sup>10</sup> Nitekim, ülkemizde de zaman zaman sansür tehlikesi interneti de tehdit eder bir noktaya gelmiştir. İnternetteki çocuk pornosu ve satanist içerikli siteleri tek tek engelleyemeyen Türkiye, ABD merkezli freeservers.com’dan hizmet alan bütün siteleri kapatmıştır. Ne var ki, bu uygulamadan suç unsuru barındırmayan birçok internet sitesi de etkilenmiştir. Liselerdeki intihar olayları ve çocuk pornosu vakalarının artması üzerine başkanlığını Ulaştırma Bakanı’nın yaptığı İnternet Üst Kurulu yapılan toplantıda, sakıncalı sitelerin servis sağlayıcı firmalar aracılığıyla engellenmesi kararlaştırılmıştır. Bunun üzerine, Türkiye’deki bütün servis sağlayıcı şirketlere hizmet veren Türk Telekom’a bağlı TTNNet, “filtre” uygulaması başlatmış, dünya üzerinde yüz binlerce internet kullanıcısının sayfalarını barındıran (hosting) ABD merkezli freeservers.com ve buna bağlı 8m.com’dan hizmet alan bütün sitelere Türkiye’den erişim engellenmiştir (www.Haberx .com - 22 Mart 2002).

Bilindiği üzere, sınırsız özgürlük kargaşaya ve bir süre sonra özgürlüklerin bir başka özgürlüğün kullanılması ile sınırlandırılmasına, hatta yok edilmesine yol açar. Hukukun bu anlamda özgürlüklerin hakkaniyet ve adalete uygun bir şekilde kullanılması amacıyla devreye girmesi kaçınılmaz olmaktadır. Bu anlamda, internet de “*hukukun tanınmadığı*” ya da “*hukuk tanımayan*” bir alan olarak kabul edilemez. Özellikle, özel hayatın gizliliğine internet vasıtasıyla yapılacak müdahaleler konunun önemini daha da artırmaktadır<sup>11</sup>. O halde, internetin de belli kuralları ve düzeni olmalıdır.

Ancak, Ceza hukuku bunu sağlamak için son çare olarak başvurulabilen bir hukuk dalı olmalıdır. Çünkü, ceza hukuku suç yaratır; suç, bir yaptırımı da beraberinde getirir. Yaptırım ise, bazı temel hak ve özgürlüklerin kısıtlanması demektir. Bu nedenle, başka hukuk dallarına ait kurum ve kurullarla bir sonuca ulaşabilmek mümkün ise ceza hukukuna başvurmalıdır. Bu çerçevede özgürlükçü demokratik yaşamın vazgeçilmez bir parçası haline gelmiş olan internet, ceza hukuku ile düzenlenmek isteniyorsa, son derece dikkatli bir şekilde hareket edilmeli, ceza hukukunun *son çare* olduğu gözden uzak tutulmamalıdır<sup>12</sup>.

Bugün ülkemizde internet ile işlenen suçlara Basın Kanunu'nun uygulanması, bu konuda özel bir norm olmadığı ve internetten alınan basılmış eser'in “sürelili” ya da “süresiz” sayılabilmesi, Basın Kanununun 5-12.maddelerinin öngördüğü kurallara sahip olmayacağı için mümkün değildir<sup>13</sup>. Aksi halde, aleyhe kıyas ya da yorum yoluna gidilmiş olacaktır.

Bu çerçevede karşılaşılabilecek diğer bir sorun, ortaya çıkması olası problemlerin bazen ulusal hukuk kuralları ile çözülmesinin mümkün olmamasıdır. Çünkü bir ülkede serbest olan faaliyet bir başka ülkede suç olarak kabul ediliyor olabilir. Yine bir ülkede delil sayılan, bir başka ülkede

<sup>11</sup> Ayrıntı için bkz. ve karşı. **Sınar**, 54 vd.; ayrıca **Dinç** Güney, Bilgisayar Çağında Özel Yaşamın Korunması, Ank.BD., S.1987/2, s.195 vd.

<sup>12</sup> Karşı. **Güran Sait/Akünel Teoman/Bayraktar Köksal/Yurtcan Erdener/Kendigelen Abuzer/Beller Önder/Sözer Bülent**, İnternet ve Hukuk Temel Metni, İstanbul 2000, s.42; **Sınar** Hasan, İnternet'in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı, Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni (MHB), Yıl.17-18, S.1-2, 1997-1998, Yılmaz Altuğ'a Armağan, İstanbul 2000, s.355.

<sup>13</sup> **Erman Sahir/Özek Çetin**, Açıklamalı Basın Kanunu ve İlgili Mevzuat, İstanbul 2000, s.29.

delil yasakları içine girebilir. Bu çerçevede ulusal kurallar yanında uluslar arası bazı kurallara da ihtiyaç bulunmaktadır<sup>14</sup>.

## **B. İNTERNET SUÇLARI KAVRAMI**

### **1. Genel Olarak**

İnternet ve ceza hukuku terimleri yan yana geldiğinde, belki de internet ortamından bir bilgisayar vasıtasıyla yararlanılmasının sonucu olarak, akla bilgisayar suçları ya da TCK. daki ifadesi ile «*bilişim suçları*» gelmektedir<sup>15</sup>. Halbuki, internet suçları olarak nitelenebilecek suçlar ile bilgisayar suçları birbirinden tamamen farklıdır. Gerçekten, internetin yaygınlaşmasından önce de bilgisayar kullanımındaki artışa paralel olarak bilgisayar suçları olarak nitelenen bazı davranış şekilleri ortaya çıkmış ve yasakoyucu tarafından düzenlenerek yaptırıma bağlanmıştır. Nitekim TCK'na 1991 yılında 3756 sayılı yasa ile eklenen m.525a, m.525b, m.525c ve m.525d bilgisayar programlarını hukuka aykırı olarak ele geçirme, bilgisayar sisteminde yer alan verileri tahrip etme, silme, değiştirme, bilgisayar sistemini kullanarak haksız çıkar sağlama ve sahtekarlık gibi fiilleri suç haline getirmiştir. Ancak, çalışma konumuzu oluşturan internetin kötüye kullanılması<sup>16</sup> şeklinde ortaya çıkan ve internet suçları olarak nitelenebilecek olan suçlar ise, yine bilgisayar aracılığı ile ve fakat internet ortamında işlenen suçlardır. O halde, *suçun internet*

<sup>14</sup> Nitekim «*Avrupa Konseyi Siber Suç Sözleşmesi*» 23 Kasım'da Budapeşte'de, 26'sı üye ve 4'ü üye olmayan (ABD, Japonya, Kanada ve Güney Afrika) 30 ülke tarafından imzalanmıştır. Bundan sonraki aşamayı, Sözleşme'nin ilke konumuna gelen yaklaşımını imzacı ülkelerin kendi iç hukuklarına uyarlamaları oluşturmaktadır. Bu aşamanın 30 Haziran 2003 tarihine dek tamamlanması öngörülmektedir. Sözleşme, genel ilkeleri ortaya koyan Siber Suçlar hakkındaki ilk uluslararası belgedir. Sözleşmenin kapsamının ayrı bir çalışma konusu yapılmasını gerektirdiği düşüncesiyle bu çalışmada üzerinde durulmayacaktır. (bkz. <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>).

<sup>15</sup> Terimler hakkında ayrıntı için bkz. **Yazıcıoğlu** Yılmaz, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle, İstanbul 1997, s.124 vd.; ayrıca karşı. **Ersöz** Yüksel, Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, AÜSBFD. 1994, C.49, S.3-4, s.160; **Dönmezer** Sulhi, Kişilere ve Mala Karşı Cürümler, 16.Bası, İstanbul 2001, s.615 vd., 632 vd.; **Önder** Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul 1994, s.504; **Tiedeman** Klaus, Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi, çev. Feridun Yenisey, İÜHFİM. 1975, C.XLI, S.1-2, s.321; **İnanıcı** Haluk, Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü, İst.BD., 1996, C.70, S.7-8-9, s.514;

<sup>16</sup> Karşı. **Haft** Fritjof/**Eisele** Jörg, Zur Einführung: Rechtsfragen des Datenverkehrs im Internet, JuS 2001, s.118.

ortamında işlenmiş olması bu suçluluk türünün ana karakterini ve ayırıcı unsurunu ifade etmektedir. Durum böyle olunca, yukarıda sayılan bilgisayar suçlarının internet ortamında işlenmesi halinde bu suçlar da internet suçu<sup>17</sup> kimliğine bürünmüş olacaktır<sup>18</sup>.

İnternetin kötüye kullanılması suretiyle işlenen suçların daha çok şu şekillerde ortaya çıktığı görülür<sup>19</sup>: - Çocuk pornografisi içeren verilerin yayılması, - Aşırı sağ ya da sol grupların görüşlerinin yayınlanması, - Patlayıcı madde yapımına ilişkin bilgiler verilmesi, -Hakaret içeren verilerin yayılması, - Dolandırıcılık ve kara para aklama ya da talih oyunu düzenlenmesi gibi diğer ticari ya da ekonomik suçluluk türleri, - Bilgisayar ve müzik ürünlerinin izinsiz kullanım ve ticareti, -Uyuşturucu madde ve silah ticareti, - Politik muhaliflerin öldürülmesi gibi bazı suçların işlenmesine çağrı niteliği taşıyan verilerin yayımı.

Bununla birlikte, internet suçları ikiye ayrılarak incelenebilir: İnternet aracılığı ile işlenen suçlar ve internete özgü suçlar<sup>20</sup>.

## 2. İnternet Aracılığı İle İşlenen Suçlar

Bu suçlar TCK ve diğer özel ceza kanunlarında tanımlanmış bulunan suçlar olup, bu suçların internet aracılığı ile işlenmesini ifade eder. Bu yönüyle internet suçları, genel suçlardan ayrı niteliklere ve yapısal farklılıklara sahip değildir. Zira internet, bazı suçların işlenişinde bir araç olarak kullanılmakta, bu suçlarla diğer suçlar arasında nitelik ve nicelik yönünden bir fark yaratmamaktadır. Bu bakımdan farklılık sadece suçun işleniş şekli, kullanılan araç ve belki de ceza sorumluluğunun türü bakımındandır. Bu durum ise, suçta etki eden bir sebep olarak kabul edilebilir.

Söz konusu klasik suç tiplerinin internet üzerinden gerçekleştirilmesi halinde suç olarak kabulünün kanunilik ilkesi ile nasıl bağdaştırılacağı sorunu, ilgili suç tiplerinin incelenmesi ile kolayca anlaşılabilir. Gerçekten, bazı suçlar

<sup>17</sup> Bu suçları ifade etmek üzere, siberuzay kavramı sadece interneti değil, benzer network sistemlerini de kapsadığı için, internet suçu terimi yerine “siber suç” teriminin tercih edilmesi gerektiği söylenmektedir (Sınar, 69, Sınar, Altuğ’a Armağan, 356). Bu doğrudur. Ancak, çalışmamız internet ortamı ile sınırlı ve network sistemlerinden şu an için en yaygın olarak kullanılanı internet olduğu için burada “internet suçu” terimi tercih edilmiştir.

<sup>18</sup> Aynı yönde Sınar, Altuğ’a Armağan, 364.

<sup>19</sup> Zöller Mark Alexander, Verdachtlose Recherchen und Ermittlungen im Internet, GA 12/2000, s.565.

<sup>20</sup> Karşl. Sınar, Altuğ’a Armağan, 357.

tanımlanırken hangi araçlarla işlenebileceği de açıkça belirtilmiştir. İnternet bir yayın aracı olduğu kabul edildiğinde, suç tanımında yer alan her türlü *iletişim aracı, her türlü vasıta* gibi terimlerin interneti de kapsayacağı açıktır<sup>21</sup>. Burada örnek olarak, TCK m.127, 145, 153, 155, 158, 159<sup>22</sup>, 175, 197, 311-312, 426, 480, 482; 503-504; Atatürk Aleyhine İşlenen Suçlar Hakkında Yasa m.1, 2; FSEK m.71, 72, 73, 80; TMK m.6, 8 verilebilir<sup>23</sup>.

### 3. İnternete Özgü Suçlar

Bu suçlar internetin yaygınlaşmasıyla ortaya çıkan, internetten önce bilinmeyen veya varolmayan doğrudan internetin işleyişi ile ilgili suçlardır. Bu çerçevede, örneğin, internetteki bir web sitesini kırmak veya tahrif etmek<sup>24</sup>, interneti kullanmak suretiyle başkalarının bilgisayar sitelerine izinsiz olarak girmek<sup>25</sup>, başkalarına ait elektronik posta kutularına sürekli elektronik

<sup>21</sup> Karşl. **Sınar**, Altuğ'a Armağan, 357. Bununla birlikte, örneğin TCK m.504 b.3'de yer alan dolandırıcılığın "Posta, Telgraf ve Telefon İşletmesinin haberleşme araçlarını ... vasıta olarak kullanmak suretiyle" işlenmesinin internet yoluyla işlenmiş sayılıp sayılmayacağı tartışmaya açıktır. Gerçekten Yargıtay bir kararında "... sanığın, komşuları bulunan Aysun ve Uğur'a bankalardan gelen hesap bildirim cetvellerini ele geçirerek bu belgelerdeki bilgilerden yararlanıp evinde bulunan encodem cihazı ile kendisine ait kredi kartının manyetik şeridini yeniden kodlatmak suretiyle ve **internet yoluyla** yurt dışındaki şirketlerden mal siparişinden bulunduğu ileri sürüldüğüne göre ... öncelikle bu işlerde bilgi ve uzmanlığı bulunan üç kişilik bilirkişi kurulu oluşturularak sanığın eyleminde sanığın eyleminde TCY'nın 525/a ve b. bentlerinde gösterilen ... durum(lar)dan herhangi birinin veya birkaçının bulunup bulunmadığı kesinlikle tespit edildikten sonra" karar verilmesi gerektiğini belirtmiştir (6.CD., 29.11.2000, 4851/8874 (YKD. Eylül 2001, s.1433). Kanımca da internet ortamına ulaşmak için sadece PTT işletmesi araçlarını kullanmak zorunlu olmadığı gibi, buna gerek de yoktur. Kaldı ki, internet PTT işletmesinin sunduğu bir haberleşme aracı da değildir.

<sup>22</sup> Nitekim, Türk Net aboneleri olan AEE internetteki Forum sayfasına emniyet görevlilerini eleştiren mesaj göndermiş olan bir kişi bunun üzerine açılan davada mahkeme tarafından TCK m.159/1 uyarınca mahkum olmuştur (**İlkiz** Fikret, İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar, İst.BD. 2001, S.10-11-12, s.987)

<sup>23</sup> Ayrıca TMK, Sıkıyönetim Kanunu, Askeri Ceza kanunu, ÇMKYUHK, FSEK gibi kanunlarda da internet vasıtasıyla işlenen suçların bulunduğu görülmektedir. Alman hukuku bakımından Al CK. § 86, § 86a, § 89, § 90, § 90a, § 90b, § 109d, § 111, § 126, § 129, § 129a, § 130, § 131, § 140, § 166, § 184, § 185-189, § 192, § 202a, § 203 örnek olarak verilebilir (Karşl. **Gercke** Marco, Rechtswidrige Inhalte im Internet, Diss., Köln 2000, s.14 vd.; **Park** Tido, Die Strafbarkeit von Internet-Providern wegen rechtswidriger Internet-Inhalte, GA 2001/1, s.24).

<sup>24</sup> =cracking.

<sup>25</sup> =hacking



posta mesajları göndermek suretiyle kişileri rahatsız etmek, posta kutularını doldurarak işlevsiz hale getirmek<sup>26</sup>, elektronik posta vb. yollarla sisteme bağlı başkalarına ait bilgisayarlara virüs bulaştırmak vb. sayılabilir<sup>27</sup>.

Bugüne kadar bu konuda doğrudan herhangi bir yargı kararına rastlamamakla birlikte, TCK'na 1991 yılında eklenen 525a-525d m.lerinin bu yeni suçlar için uygulanması kısmen de olsa mümkündür kanısındayız. Örneğin, bilgisayar sabotajı olarak da nitelenen, alıcının e-mail adresine virüslü mesaj göndermek suretiyle alıcının sistemini çökertmek, "*bilgisayar sistemini veya sistemdeki verileri tahrip etmek*" suçunu düzenleyen TCK m.525b f.1 kapsamı içinde değerlendirilebilir. Ancak, kanunilik ilkesi karşısında yukarıda sözü edilen her fiil için söz konusu hükümlerin uygulanması sorun oluşturabilir. Bu nedenle vakit kaybedilmeden TCK'na yeni suç tiplerinin alınmasında fayda vardır<sup>28</sup>.

### C. İNTERNET SUÇUNUN FAİLİ

İnternet suçlarının faili, internet hizmetlerinden faydalanan **kullanıcı**-lardır. Teknik anlamda kullanıcı, internette sunulmuş olan hizmetleri bilgi elde etmek ya da bilgiyi ulaşılabılır kılmak amacıyla talep eden gerçek ya da tüzel kişilerdir<sup>29</sup>. Bu anlamda, kullanıcı olarak internet ortamından faydalanan herkes, bu ortamda işlenebilecek suçun/suçların faili olabilir<sup>30</sup>.

Ancak, internetin kendine özgü suçlar yanında, aynı zamanda, kendine özgü sùjeler yaratmış olduğu da gözden uzak tutulmamalıdır. Dolayısıyla, burada özellik gösteren husus, gerçek kişi kullanıcı ötesinde internet sùjelerinin varlığı ve bunların ceza sorumluluğudur. Web sayfasını hazırlayan ve/veya internet kullanıcıları için erişilebilir kılan sùjelere *internet sùjeleri* denir. İnternet sùjelerinin kim olduğu, internet yoluyla işlenen suçun failini

<sup>26</sup> =spamming

<sup>27</sup> Karşl. Hilgendorf, ZStW 2001, 653, 654; Güran vd., 42; Sınar, Altuğ'a Armağan, 363.

<sup>28</sup> Nitekim 2000 tarihli TCK Öntasarısı, "Bilişim Alanında Suçlar" başlığı altında "Bilişim sistemine girme, verileri tahrip etme ve bozma" (m.345), "Sistemi engelleme, bozma, haksız yarar sağlama" (m.346), "Sahtecilik" (m.347), "Banka ve kredi kartlarının kötüye kullanılması" (m.349), "Suç işlemek için örgütlenme" (m.350) ve "Tüzel kişilerin cezai sorumluluğu" (m.351) konularında hükümler getirmektedir.

<sup>29</sup> Bu tanımlama Alman TDG § 3 no.2 de yer almaktadır. Tüzel kişilerin cezai sorumluluğu bulunmadığından, internet ortamında işlenen suçun faili sadece gerçek kişi olabilir.

<sup>30</sup> İster internet aracılığı ile işlenen klasik suçlar, isterse internete özgü suçları işleyenler bazen kendine özgü terimlerle anılırlar. Bunlar craker, hacker, swapper, vandal gibi adlar taşırlar (Ayrıntı için bkz. Yazıcıoğlu, 120 vd.)

belirlemek bakımından son derece önemlidir. Ülkemizde henüz, internet suçlarının kim ve hukuki, idari ve cezai sorumluluklarının ne ve hangi kapsamda olduğu konusunda yasal bir düzenleme getirilmiş değildir<sup>31</sup>. Bu nedenle, konuyu açılığa kavuşturmak bakımından, Alman hukukundaki durumdan kısaca bahsetmekte yarar görmekteyiz.

1997 tarihli Alman Telekomünikasyon Hizmetleri Yasası önceleri § 5’de düzenlediği internet yayınlarından doğan ceza sorumluluğunun esaslarını, 14 Aralık 2001 tarihli Elektronik Ticaret Yasası<sup>32</sup> Artikel 1 ile değiştirerek, bu defa 3.Bölüm altında yeniden belirlemiştir<sup>33</sup>. Bu çerçevede internet suçleri üçe ayrılabilir<sup>34</sup>:

- içerik sağlayıcı (sunucu),

<sup>31</sup> Nitekim sorun **Çoşkun Ak davasında** ortaya çıkmıştır. Çoşkun Ak Superonline isimli servis sağlayıcı firmada “interaktif bölümler koordinatörü”dür. Firmanın internet sayfasında “Türkiye’de İnsan hakları” konulu bir Forum düzenlenir. Foruma gelen bir mesaj nedeniyle Çoşkun Ak hakkında TCK m.159’u ihlalden dava açılır. İddianamede “... Ülkemizde internetle işlenen suçlar bakımından yasal bir düzenleme olmamakla birlikte sanığın durumu, yazı sahibinin kimliğini açıklamayan mevkute sorumlu müdürü veya yayınlanan durumuna benzemekte olup, suça konu internet sahifesinin düzenlenmesine önyak olan, ...mesajları silmeyen ve İnternet kullanıcılarının hizmetine sunan (sanığın) TCK nun 159.m.sini dört kere ihlal ettiği” belirtilmiştir. Mahkeme sanığı 40 ay ağır hapis cezasına mahkum eder. Buna karşılık Yargıtay 9.CD kararı, “Gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından öncelikle sanığın adı geçen şirkette konumunun ne olduğu, foruma internet ortamında elektronik posta ile gönderilen suçlamaya konu yazılara müdahale etme görev ve yetkisinin bulunup bulunmadığı, müdahale etme yetkisinin bulunmaması halinde bu yetkinin kime ait olduğu hususunun ilgili kurumdan bilgi ve belgeler de sağlanarak saptanması ... mahkemece uzman bilirkişi kurulu ile keşif yapılarak Superonline AŞ nin bir internet servis sağlayıcı mı yoksa her iki fonksiyona birlikte mi sahip olduğu, internet servis sağlayıcı olması durumunda sahibinin kim olduğu, ayrıca dava konusu yazının yayımlandığı forumun ve web sitesi sisteminin bir işletene bağlı olup olmadığı hususlarının saptanmasından sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik soruşturma ile hüküm kurulduğu gerekçesiyle yerinde olarak bozmuştur (**İlkiz**, 987 vd, 1023).

<sup>32</sup> =Elektronischer Geschaeftsverkehr-Gesetz-EGG; BGBl. I, s.3721

<sup>33</sup> Önceki durum için karşı. **Flehsig** Norbert P./**Gabel** Detlev, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, CR 1998/6, s.354; **Hegmanns** Michael, Strafrechtliche Verantwortlichkeit für illegale Inhalte im Internet, JA 2001, s.71 vd.; **Gercke**, 107 vd.. Öte yandan, yasadaki bu hükmün sadece ceza hukukuna özgü bir sorumluluk getirmediği söylenmelidir. Hüküm aynı şekilde hukuki ve idari sorumluluğu da kapsamaktadır (**Park**, 29). Değişikliğin buna bir etkisi olmamıştır.

<sup>34</sup> **Hoeren** Thomas, Rechtsfragen des Internet, Köln 1998, no.355 vd.; **Park**, 30; karşı. **Hegmanns**, 72; **Gercke**, 10 vd.; **Dönmezer**, 637 vd.

- erişim sağlayıcı (sunucu) ve
- servis sağlayıcı (sunucu).

İçerik sağlayıcı<sup>35</sup>, kendisine ya da başkasına ait hizmetleri kullanıma hazır tutan kişilerdir (§ 3 no.1 Al.Teleservisler Yasası). Bu anlamda içerik sağlayıcı internet üzerindeki herhangi bir yayının, örneğin web sayfasının içeriğini hazırlayan kimse olarak karşımıza çıkmaktadır. Söz konusu web sayfası üzerindeki yazı, resim ve diğer materyaller içerik sağlayıcı tarafından hazırlanır, sayfa düzeni oluşturulur. O halde, içerik sağlayıcı kendi hazırladığı verileri **kullanıma hazır tutan kimse olarak**, sadece bu bilgiler bakımından sorumlu tutulmaktadır (§ 8 I Al.Teleservisler Yasası). Bu durumda içeriğin suç teşkil etmesi halinde, onu hazırlayan olarak sahibi durumunda bulunan, içerik sağlayıcı sorumludur. Ancak, içerik sağlayıcının işlevinin sadece sayfanın içeriğini hazırlamaktan ibaret olduğu söylenmelidir. İçerik sağlayıcı onun tarafından nakledilen ya da saklanan bilgilerin izlenmesi ya da duruma göre içeriğin hukuka aykırı olup olmadığını araştırmakla yükümlü değildir (§ 8 II Al.Teleservisler Yasası). Bu nedenle, kanımca içerik sağlayıcının sorumlu tutulabilmesi için söz konusu sayfanın internete aktarılması, yani erişilebilir kılınması yönündeki kusurlu iradesinin ortaya çıkartılması gerekir. Bu kast ya da taksir şeklinde olabilir.

Erişim sağlayıcı<sup>36</sup>, internet bağlantısına sahip olmakla birlikte, başkalarına ait verileri depolayabileceği bir ana bilgisayarı olmayan internet süjesidir. Bu yönüyle erişim sağlayıcı sadece başkalarına ait verilerin internete aktarılmasına aracılık eder. O halde erişim sağlayıcının asıl görevi, kullanıcı ve içerik sağlayıcı arasındaki veri değişimini mümkün kılmaktır. Çoğu içerik sağlayıcı mesela, mail-server ya da arama motorları gibi erişim sağlayıcı olarak faaliyet göstermektedir. Bu nedenle, aktarılan verilerin suç içerikli olup olmadığı konusunda bilgi sahibi olmaması, bilgi sahibi olsa bile bu akışı önlemesinin mümkün bulunmaması nedeniyle kusursuz suç ve ceza olmaz ilkesinin bir sonucu olarak ceza sorumluluğunun bulunmadığı kabul edilir (§ 9 I Al.Teleservisler Yasası). Bununla birlikte, erişim sağlayıcının yabancı içeriği kontrol edebilme ve yine onun yayılmasını bazı tedbirler kullanarak engelleyebilme olanağına sahip olduğu söylenmelidir. Örneğin, arama motoru işleticisi bu arama motoruna girilerek, mesela, çocuk pornografisinin aranması ve pek çok veriye ulaşılması halinde işleten bundan sorumlu olacak mıdır? Kural olarak, içerik sağlayıcının aksine, erişim sağlayıcı aranan içerik bakımından yansız bir konumda bulunur. Gerçekten arama motoru işleten

<sup>35</sup> =Content-Provider.

<sup>36</sup> =Access-Provider

içeriği hiç bir şekilde bilmiyor ya da aramayı sadece onun asli faaliyeti olarak istiyor olabilir. Bu durumda işletenin sorumlu tutulabilmesi için gayri muayyen kastla hareket ettiği ispatlanmalıdır. Bununla birlikte, motor, aranan her kelime için sınırsız bir şekilde düzenlenmişse, pekala en azından taksirin mevcut olduğu da kabul edilebilir<sup>37</sup>.

Servis sağlayıcılar<sup>38</sup>, bir yandan web sayfaları oluşturarak ve kendisine ait hizmetleri vermek suretiyle kendi içeriklerini sunarken, diğer yandan da örneğin, müşterilerinin kendi sayfalarına yer vererek başkalarına ait bilgileri internet ortamına aktarmakta, başkalarına ait bu bilgileri kendi ana bilgisayarında depolamakta ve bu bilgileri internet ortamına aktararak erişilebilir kılmaktadır. İnternet servis sağlayıcıları bu anlamda, bireylerin internete bağlanmalarını, internet üzerinden iletişim kurmalarını ve internetin sağladığı olanakları kullanmalarını temin eder. Örneğin, Superonline.com, e-kolay.net ticari, üniversiteler de ticari olmayan servis sağlayıcılarıdır. İnternetin açılış-kapanış saati bulunmaması ve hizmetlerin sürekli bir şekilde veriliyor olması iyi bir servis sağlayıcıya olan ihtiyacı ortaya koyan özelliklerdir. Bu nedenle, sürekli hazır tutmayı sağlamak amacıyla verilerin büyük bir kısmı servis sağlayıcılar üzerinde depo edilir. Öncelikle, servis sağlayıcının bizzat oluşturduğu içeriklerden sorumluluğunun diğer tüm sunucular gibi sınırsız olduğu söylenmelidir. Alman hukukunda servis sağlayıcıların ancak, ana bilgisayarlarındaki suç içerikli bilgilerin bu niteliğinden haberdar olmaları, bu bilgilerin internet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına ve beklenebilirliğine sahip bulunmaları halinde sorumlu olabileceği kabul edilmektedir (§ 10-11 Al.Teleservisler Yasası)<sup>39</sup>. Bu, icrai ya da ihmali bir hareket sonucu gerçekleşebileceği gibi, kusurlu irade kast ya da taksirle de ortaya çıkabilir. Bununla birlikte, kural olarak, servis sağlayıcıların içeriklere etkide bulunabilme olanakları mevcut değildir. Gerçekten burada bir apartman sahibinin dairelerini kiraya vermesine benzeyen bir durum söz konusudur. Nasıl ki, ev sahibinin kiracısına gelen-gideni kontrol etme hakkı bulunmuyorsa, servis sağlayıcının da her haberi bir sansür organı gibi kontrol etmesi düşünülemez<sup>40</sup>. Ancak, servis sağlayıcı haberi olur olmaz gerekli tertibi almak zorundadır.

<sup>37</sup> Karşl. **Hegmanns**, 74

<sup>38</sup> =Host-Provider/Service-Provider..

<sup>39</sup> Bu husus CompuServe davasında da tartışılmıştır. Bkz. d.pn.69.

<sup>40</sup> Karşl. **Hegmanns**, 75.

Burada tartışılması gereken diğer bir husus da iştirak durumudur. Kanımca, yukarıdaki şekilde fiili işleyen kişilerin fiillerine iştirakin, diğer koşullarının da oluşması halinde asli ya da fer'i iştirak şeklinde ortaya çıkması mümkün olmalıdır (m.64, 65 TCK)<sup>41</sup>.

#### **D. İNTERNET SUÇLARI VE SUÇUN İŞLENDİĞİ YER SORUNU**

##### **1. Genel Olarak**

Ulusal ve uluslararası bilgisayar ağının birlikte gelişmesi bir ülkede işlenmesi mümkün suçların internet vasıtasıyla diğer ülkelerde de işlenmesini olanaklı kılmaktadır. Böylece «sınırötesi suç» ismini verebileceğimiz yeni bir suç işleme şekli ortaya çıkmıştır. Bu daha çok bilgisayar casusluğu, bilgisayar manipilasyonu ve bilgisayar sabotajı suçlarında görülür. Bunun dışında, bu tür suçlar bu gün “beyan suçları”<sup>42</sup> olarak anılan özellikle çocuk pornografisi, şiddet övücü ve ırkçı içeriklere sahip verilerin uluslararası bilgisayar ağlarında ulaşılabilir kılınması biçiminde ortaya çıkar.

İnternette bu «ulusalüstü» suç işleme olanağı, ulusal ceza hukukunun ne dereceye kadar uygulanabilir olduğu sorusunu gündeme getirir. Elbette, bu bir uluslararası ceza hukuku problemidir. “Siber uzay” olarak da adlandırılacak olan global bir ortamda işlenen suçlar bakımından farklı hukuk düzenlerince farklı karar verilebilmesi olasılığı, sorunun önemini artırmaktadır<sup>43</sup>. Gerçekten bazı fiillere hırsyan kültürünün egemen olduğu ülkeler ile islam kültürünün egemen olduğu ülkeler farklı reaksiyonlar verebileceği gibi, dini, politik ve kültürel olarak nispeten birbirine yakın ülkelerin ceza hukuku düzenleri arasında da önemli farklılıklar ortaya çıkabilmektedir. Mesela, nasyonal-sosyalist propaganda Almanya ve Avusturya’da cezalandırılabilir iken, ABD, Avustralya ve Kanada’da düşünce özgürlüğü içinde değerlendirilir ve suç sayılmaz<sup>44</sup>. Yine çocuk

<sup>41</sup> Krşl. **Flehsig** Norbert P./**Gabel** Detlev, Strafrechtliche Verantwortlichkeit im Netz durch Einrichtung und Vorhalten von Hyperlinks, CR 1998, s.356.

<sup>42</sup> =Äußerungsdelikte.

<sup>43</sup> **Sieber** Ulrich, Internationales Strafrecht im Internet, NJW 1999, s.2065

<sup>44</sup> Nitekim sorunun ne şekilde ortaya çıkabileceğini Alman hukukundaki uygulamalardan bazı örnekler vererek somutlaştırabiliriz: -Avustralya tabiiyetine sahip bir kişi Avustralya’daki Internet-sunucusunda Auschwitz toplama kampı hakkındaki tarihi gerçekleri saptırması ve inkar etmiş olduğu için Almanya’yı ziyareti sırasında göz altına alınmıştır.- Diğer bir olayda ise, Alman asıllı Kanadalı olan ve Kanada hukukuna göre muhtemelen cezalandırılmayan sunucunun, nasyonal sosyalist içerikli yazıları hakkında Alman savcılarınca çok sayıda tedbir denenmiştir.

pornografisinin yayınlanması da mesela, korunmuş olan çocuğun yaşı ya da bu yayınlara sahip olanın cezalandırılabilirliği bakımından batılı ülkelerde de farklı değerlendirilmektedir.

Ceza hukuku sistemleri arasındaki bu fark, doğal olarak, uygulamada maddi hukuka ilişkin sorunlar yanında, öncelikle uluslararası ceza hukuku bakımından bazı sorunları da beraberinde getirmiştir. Burada ortaya çıkan problemin iki yönü vardır: İşlenmiş olan suç bakımından hangi ülke soruşturma makamlarının yetkili olacağına ilişkin yetki problemi ve dolayısıyla ceza hukukunda ulusal cezalandırma yetkisinin kabulüyle, kural olarak, ulusal ceza hukuku düzeninin uygulanabilirliği de söz konusu olduğundan, hangi hukukunun uygulanacağına ilişkin maddi hukuk problemi.

Tek bir «tıklama» ile tüm verilere ulaşılabileceği için, internette mevcut pek çok içeriğin farklı devletler tarafından ve farklı ceza hukuku kurallarına tabi olup olmayağı ve Türk ceza hukuku bakımından nasıl bir çözüme başvurulabileceği sorusu bu bölümün ana temasını oluşturacaktır.

## 2. Hukuki Durum

Türk ceza hukukunun uygulanabilirliği bakımından ana prensibin *mülkîlik prensibi* olduğu söylenebilir. Prensibi düzenleyen TCK m.3, suçun işlendiği, dolayısıyla cezalandırılacağı yer sorununa kısmi bir çözüm getirmiş olup, TCK'nın sadece Türkiye'de işlenen suçlarda uygulanacağını, yani Türk devletinin cezalandırma yetkisinin sadece bu tür suçlar bakımından bulunduğunu belirtmekle yetinmiştir. O halde, *Türk Ceza Kanunu* kural olarak, sadece *yurt içinde işlenmiş olan suçlara* uygulanır. Diğer bir deyişle, Türk devletinin cezalandırma yetkisi, kural olarak, bu suçlar için geçerlidir. Mülkîlik prensibinden ortaya çıkacak diğer bir sonuç ise, failin vatandaş ya da yabancı olup olmadığına bakılmaksızın yurt içinde işlenen tüm fillerde TCK'nun geçerli olmasıdır. Nihayet, ülke içinde işlenen suçlara TCK'nun uygulanması bakımından suçun ağırlığı da (nitelik ya da niceliği) önemli değildir.

Görüldüğü üzere, Türk hukukunun uygulanması bakımından esas *bağlanma kuralı* olarak «suçun işlendiği yer» kriteri esas alınmıştır. Ancak, TCK bu esas bağlanma kuralı yanında onu tamamlayan yardımcı kriterler de benimsemiştir. Bu kriterleri ifade eden prensipler şahsîlik, koruma ve evrensellik prensipleridir. Buna göre, suç yurt dışında işlenmiş olsa bile «fail veya mağdurun Türk olması», «işlenmiş olan suçun niteliği» kriterleri de

bağlanma kuralı olarak belirlenmiştir (m.4, 5, 6 TCK)<sup>45</sup>. Bu kriterler bakımından ana özellik, suçun işlendiği yerin Türkiye olmasının önemli bulunmamasıdır. Mülklik, şahsılık, koruma ve evrensellik prensiplerinin geçerli olduğu hallerde internet yoluyla işlenen suçlarda Türk hukukunun ne şekilde uygulanacağı konusunda bir sorun bulunmaz. Bu durumda mesela, suç olan içeriği ortama sunan sunucu Türkiye’de bulunuyor ve bu veriler Türkiye’de saklanıyorsa fail mülklik prensibi gereği Türk hukukuna göre cezalandırılır<sup>46</sup>. Yine devletin bölünmez bütünlüğü aleyhine propagandanın internet yoluyla yapılması halinde fiil korunma prensibinin bir gereği olarak Türk hukukuna göre cezalandırılır.

Buna karşılık, mülklik prensibinin Türkiye Cumhuriyeti sınırları içinde işlenmiş olan her fiil bakımından Türkiye Cumhuriyeti devletinin cezalandırma yetkisinin bulunduğunu belirlemiş olması karşısında, suçun işlendiği yer kavramından ne anlaşılması gerektiği sorunu açıklığa kavuşturulmalıdır. Daha açıklıkla ifade etmek gerekirse, hareketin yabancı bir ülkede yapılmış olması durumunda bazı hallerde yine de suçun Türkiye’de işlenmiş sayılması mümkün olabilecek midir? «Türkiye’de işlenmiş olma» ne demektir? Gerçekten, neticesi hareketten ayrılabilen, yani hareket ve neticenin farklı yerlerde gerçekleştiği *mesafe suçları*<sup>47</sup> bakımından suçun Türkiye’de işlenmiş olup olmadığı, diğer bir deyişle, bağlantı noktası olarak «suçun işlendiği yer» kriteri esas alınarak Türkiye’nin cezalandırma yetkisinin bulunup bulunmadığı önemli bir sorun olarak karşımıza çıkmaktadır. Ani suçlar, yani hareketin yapılması ile birlikte neticenin de meydana geldiği suçlar bakımından kural olarak bir problem bulunmaz. Zira bu suçlarda hem hareket, hem de netice aynı yerde işlenmektedir. Yukarıda yer alan düzenleme şekli karşısında TCK’nun mesafe suçları bakımından suskun kaldığı söylenmelidir. Zira TCK m.3 sadece hareketi mi, neticeyi mi, yoksa, her ikisini de mi esas aldığı açıklanamaksızın ülkede işlenmiş olan suçlar bakımından bir düzenleme getirmektedir. Yer bakımından yetkili mahkemeyi «suçun işlendiği yer mahkemesi» olarak belirleyen CMUK’nun 8.m.sinin de mesafe suçu hakkında bir düzenleme getirmediği görülmektedir. Konu, ulusalüstü bir niteliğe sahip internet suçları bakımından büyük önem

<sup>45</sup> Şahsılık, korunma ve evrensellik prensipleri.

<sup>46</sup> Karşl. **Derksen**, NJW 1997, 1880

<sup>47</sup> Karşl. **Kunter** Nurullah, Suçun Maddi Unsurları Nazariyesi, İstanbul 1954, s.91; **Önder** Ayhan, Suçun İşlendiği Yer, AD., S.1-2, s.97.; **Schönke** Adolf/**Schröder** Horst, Strafgesetzbuch - Kommentar, 25. Aufl., München 1997, § 9 no.3, 12 vd.

taşımaktadır. Çünkü, bu tür suçlar niteliği gereği hareket ile neticenin birbirinden ayrılabilirdiği suç tipleridir.

### 3. Suçun İşlendiği Yer Konusunda Kabul Edilen Teoriler

İnternet vasıtasıyla işlenen cezalandırılabilen bir hareketin dünyanın hangi yerinde yapıldığı ve nihai olarak nerede etkili olduğunun tesbit edilmesi oldukça zor bir konudur. İnternetin kendine özgü yapısı ve işleyiş tarzı bu zorluğu daha da artırmaktadır. Gerçekten, diğer iletişim araçlarından farklı olarak internet tüm dünyaya yayılmış, her yerden ulaşılabilir olup, etki gücü de radyo ve TV gibi belli bir alanla sınırlanmış değildir.

Aslında suçun işlendiği yer sadece uygulanacak olan ceza kanununun belirlenmesi açısından değil, aynı zamanda yetkili mahkemenin belirlenmesi bakımından ceza muhakemesini de ilgilendirmektedir. Bu çerçevede konu sadece uluslararası bir boyut da taşımaz; aynı zamanda bir ülkede hangi yer mahkemesinin yetkili olacağı sorunuyla da yakından ilgilidir. Zira internet üzerinden işlenen fiil pekala aynı ülkede farklı yargı alanlarında bulunan yerlerde işlenebilir<sup>48</sup>.

Suçun işlendiği yer konusundaki teorileri başlıca üç grupta toplamak mümkündür<sup>49</sup>: Hareket teorisi, neticeye üstünlük veren teori ve karma teori.

<sup>48</sup> **Önder**, mesafe suçlarında hareket ile netice arasında bir mesafenin bulunması gerekli ise de siyasi bir sınır da bulunmadıkça mesafe suçları özelliği taşımayacağı görüşündedir (**Önder** Ayhan, Ceza Hukuku Genel Hükümler, C.I, İstanbul 1991, s.185; **Önder**, AD., 96).

<sup>49</sup> *Hareket teorisi*, suçun işlendiği yerin tayininde failin yaptığı harekete üstünlük tanır. Buna göre, icra hareketi nerede gerçekleştirilmiş ise, suç da orada işlenmiş kabul edilir. Böyle bir anlayış içinde suçun işlendiği zaman da hareketin işlendiği zaman olarak kabul edilmelidir. Buna karşılık, *neticeye üstünlük veren teori*, yasal tipteki netice nerede meydana gelirse suçun da orada işlenmiş olduğunu kabul eder. Nihayet, *karma teoriye* göre ise, hareket nedensellik bağı ve netice suçun asli unsuru olduklarından bunlar arasında ayırım yapmaz. O halde, suçun hem hareketin, hem hareketin ilk ve doğrudan etkisinin gerçekleştiği ve hem de neticenin meydana geldiği yerde işlenmiş olduğu kabul edilmelidir. Bu ana teoriler dışında bu teorilerin uzantısı niteliğinde olan *arada etki teorisi*, *suçun aralıksız ve yakın neticesinin meydana geldiği yere üstünlük tanıyan teori* ve *genişletilmiş hareket teorisi* gibi başka bazı teoriler daha bulunmaktadır. *Arada etki teorisine* göre, hareketin ilk ve doğrudan etkisinin meydana geldiği yerde suç işlenmiştir. Suç hareket ve netice arasında meydana geldiği için arada etki olarak adlandırılmıştır. *Suçun aralıksız ve yakın neticesinin meydana geldiği yer teorisi* ise suçun yakın ve doğrudan doğruya neticesinin meydana geldiği yere üstünlük tanır. Nihayet failin hareketlerine öncelik tanıyan teori *genişletilmiş hareket teorisi* olarak adlandırılır. Teoriler



Bugün Türk hukukunda hemen her teorinin temsilcisini görmek mümkündür<sup>50</sup>. Yargıtay ise, suçun doğrudan yakın ve aralıksız neticesinin meydana geldiği yeri suçun işlendiği yer olarak kabul etmektedir<sup>51</sup>.

Alman CK, § 9 ile “*her yerde olma prensibi*”<sup>52</sup> olarak da isimlendirilebilecek olan karma teoriyi benimsemiştir<sup>53</sup>. Bu durumda hareket ve netice farklı ülkelerde meydana gelse dahi, bu ülkelerden her ikisi de cezalandırma yetkisine sahiptir<sup>54</sup>. Diğer bir deyişle, Alman hukukunun uygulanabilmesi bakımından hareket veya neticeden herhangi birisinin Almanya’da gerçekleşmiş bulunması yeterlidir. Buna göre, fiilin işlendiği yer bakımından bağlantı noktası olarak 1- Failin icra hareketini yaptığı yer, 2- fiil ihmali ise failin hareket etmesi gereken yer, 3- tipe ait neticenin meydana geldiği yer ve nihayet 4- failin tasavvuruna göre neticenin gerçekleşmesi gereken yer esas alınmalıdır. Bu durumda Alman CK § 9 f.1’e göre “*tipe ait olan netice*” önemlidir. Öte yandan, failin kastının fiilin işlendiği yeri kapsamaması gerekmez<sup>55</sup>. Yani, fiilin işlendiği yerin tesbiti bakımından failin kastının önemi yoktur.

Halen yürürlükte bulunan TCK’da bu konuda bir açıklık olmamakla birlikte, TCK Tasarısı da karma görüşü benimsemiştir. Buna göre, 1- Hareketin kısmen veya tamamen Türkiye’de icrası ya da 2- Neticenin Türkiye’de gerçekleşmesi halinde TCK uygulanır (m.6/1). Tasarının bu şekilde yasalaş-

---

hakkında ayrıntı için **Artuk/Gökçen/Yenidünya**, Ceza Hukuku Genel Hükümler I, Ankara 2002, s.302 vd.

<sup>50</sup> **Dönmezer/Erman, Öztürk/Erdem/Özbek** karma (**Dönmezer Sulhi/Erman** Sahir, Nazari ve Tatbiki Ceza Hukuku, 11. Bası, İstanbul, no.386; **Öztürk Bahri/Erdem** Mustafa R./**Özbek** Veli Özer, Uygulamalı Ceza Hukuku ve Emniyet Tedbirleri Hukuku, 5.Baskı, Ankara 2001, no.43); **Taner**, İçel/**Donay**, Zafer ve **Kunter** hareket (**Taner** Tahir, Ceza Muhakemesi Usulü, İstanbul 1950, s.72; **İçel** Kayıhan/**Donay** Süheyl, Karşılaştırmalı ve Uygulamalı Ceza Hukuku, Genel Kısım, 1.Kitap, 3.Bası, İstanbul 1999, s.166 vd.; **Zafer**, 33; **Kunter**, Suçun Maddi Unsurları, 93); **Önder**, aralıksız netice teorisini (**Önder**, I, 194) kabul ederler.

<sup>51</sup> YCGK, 31.10.1949, 1-108/93 (**Gözübüyük** A.Pulat, Türk Ceza Kanunu Açıklaması, C.I, 4.Bası, İstanbul 1980, s.44 vd.

<sup>52</sup> =Ubiquitätsprinzip

<sup>53</sup> karşl. **Lackner** Karl/**Kühl** Kristian, Strafgesetzbuch, 23.Aufl., München 1999, § 9, no.1; **Tröndle**, Herbert/**Fischer** Thomas, Strafgesetzbuch und Nebengesetze, 49.Aufl., München 1999, § 9 no.1

<sup>54</sup> **Hilgendorf** Eric, Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internet, NJW 1997, s.1873; karşl. **Hilgendorf**, ZStW 113 (2001), 660; **Hoeren**, no.347 vd.

<sup>55</sup> **Lackner/Kühl**, § 9, no.1; **Schönke/Schröder**, § 9 no.15.

ması halinde Alman hukukundaki düzenlemeye çok yakın bir hükme yer verilmiş olacaktır.

Ülke içinde işlenen suçlarda yetkili mahkemenin belirlenmesi açısından harekete üstünlük tanıyan görüş makul ve kabul edilebilirdir. Kamu düzeninin asıl sarsıldığı yerin hareketin yapıldığı yer olduğu, delillerin orada bulunduğu ve failin belki hala orada olabileceği böyle bir kabulün gerekçelerini oluşturur. Buna karşılık, neticeye üstünlük veren teori özellikle teşebbüs aşamasında kalmış suçlar bakımından tatmin edici değildir. Yine suçun bir tehlike suçu, özellikle de soyut tehlike suçu olması halinde yeterli olmaktan uzaktır. Karma teori de sorunu çözümlüyor değildir ; çünkü bu defa da yetki uyuşmazlıkları çıkacaktır. Bununla birlikte, mesafe suçunun diğer bir görünüş şekli olarak hareket ve neticenin farklı ülkelerde gerçekleşmesi durumunda hareket teorisini aynı rahatlıkla savunabilmek ülkenin egemenlik yetkisinin bir yansıması olarak kabul edebileceğimiz cezalandırma yetkisi söz konusu olduğundan kolay olmayacaktır. Konu, internet üzerinde işlenen suçlar bakımından daha da ciddi bir boyut kazanmaktadır.

TCK Tasarısındaki hükmün bir an için yasalaştığı kabul edildiğinde, başka ülkeler tarafından yaşanmış olan bazı sorunların bizim ülkemizde de yaşanması olasılığı büyüktür. Gerçekten, bugün karma teorisinin internet üzerinde gerçekleşen ve siyasal sınır tanımayan veri trafiği karşısında işlevsel olmaktan çıktığı ve pek çok sorunu da beraberinde getirdiği vurgulanmaktadır. Gerçekten Alman hukukunda “beyan suçları” olarak tabir edilen<sup>56</sup> mesela, suç işlemeye tahrik, tehdit, propoganda ya da pornografik yayın gibi suçların internet üzerinde işlenmesi halinde bu düzenleme karşısında internette yapılan ve Alman Ceza Kanununda düzenlenmiş olan tipe uygun her harekete Alman CK uygulanır hale gelmiştir<sup>57</sup>.

#### ***a. Bağlanma Noktası Olarak Neticenin Gerçekleştiği Yerin Esas Alınması***

Bu durum özellikle bağlanma noktası olarak neticenin esas alındığı hallerde karşımıza çıkar. Veri akışının artık sınır tanımadığı günümüz “internet çağı”nda, ABD ya da Kanada’da bulunan bir serverdaki verilere

<sup>56</sup> Karşl. s.12 dpn.62.

<sup>57</sup> Karşl. **Conradi** Ulrich/Schlömer Uwe, Die Strafbarkeit der Internet-Providern, NStZ 1996, s.366 vd., özellikle 368 vd.; **Sieber** Ulrich, Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen, JZ 1996, s.429; **Hilgendorf**, NJW 1997, 1874; **Kuner** Christopher, Internationales Zuständigkeitskonflikte im Internet, CR 1996, s.456.

Almanya'dan rahatlıkla girilebilir. Bu durumda hukuka aykırı içeriğe sahip yazı ya da resme Almanya'dan ulaşılacağı için dünyanın herhangi bir yerinde bu şekilde internet üzerinde işlenmiş her hareket bakımından neticenin Almanya'da gerçekleştiği kabul edileceğinden Alman CK'da düzenlenmiş tipe uygun her harekete Alman CK'nun uygulanması mümkün hale gelecek<sup>58</sup>; netice ülke içinde gerçekleşmiş sayıldığından suç da ülke içinde işlenmiş sayılacaktır. Böylece internet ortamında gerçekleşecek olan tüm suçlar Almanya'da işlenmiş sayılacak ve mülkiyet prensibi gereği cezalandırılabilir. En azından, koğuşurma mecburiyet ilkesi gereği bu tür fiillere ilişkin başlangıç şüphesinin varlığı halinde savcı derhal hazırlık soruşturmasına başlamak zorundadır. Neredeyse dünyada internet vasıtasıyla işlenen her suçta Alman kanununun uygulanması sonucunu doğuran bu yorum şeklinin, bazen Almanyanın dış dünyadaki itibarını zedelediği de olmuştur. Gerçekten 1995 Sonbaharında Münih savcılığı İnternet erişim sağlayıcı firma CompuServe şirketine karşı soruşturma başlatmış, firmanın internet üzerindeki faaliyetini engellemiş, çocuk pornografisinin neşrinin engellenmesi nedeniyle açılan ceza davası sonucunda mahkeme 1998 yılı mayısında şirket genel müdürünü 2 yıl hapse mahkum etmiş ve cezasını ertelemiştir<sup>59</sup>. Ancak, karar Alman firma § 5 III 1 TDG göre yabancı içerikten sorumlu olmayacağı için 1999 yılında bir üst mahkemece<sup>60</sup> kaldırılmıştır<sup>61</sup>. Savcılıkça hazırlık soruşturmasına başlanması ve firmanın faaliyetinin engellenmesi üzerine Almanya dünya çapında protestolara maruz kalarak Alman buraları caddelere dökülmüştür<sup>62</sup>. Böyle bir uygulama ile yabancılar adeta kendi ülkelerinde suç olmayan ve fakat Alman hukukuna göre cezalandırılabilir olan hareketleri nedeniyle cezalandırılacakları kaygı ve şüphesini duymaya zorlanmışlardır.

<sup>58</sup> 96, 369; **Kuner**, CR 1996, 456; **Sieber**, JZ 1996, 430; **Hilgendorf**, NJW 1997, 1874.

<sup>59</sup> Karar için bkz. AG München, NJW 1998, s.2836

<sup>60</sup> Karar, doktrin tarafından da özellikle "cezaların şahsiliği" ilkesine aykırı bulunarak şiddetli bir şekilde eleştirilmiştir (**Hilgendorf**, ZStW 113 (2001), 658). Çünkü, mahkeme kararında Alman CompuServe firmasıyla Amerikan CompuServe firmasının kardeş firmalar olduğunu ve bu nedenle Alman firmanın Amerikan firmasının hareketlerinden sorumlu olacağını, Alman firmanın ağır pornografiyi engellemediği için ihmali bir harekette bulunduğunu ve bu nedenle Alman firma genel müdürünün cezalandırılmasını gerektiği sonucuna ulaşmıştı. Halbuki, Alman firmanın genel müdürünün Amerika kaynaklı verilerin internet üzerinde engelleyebilmesi imkanı son derece sınırlıdır.

<sup>61</sup> Karar için bkz. LG München, NJW 2000, s.2840.

<sup>62</sup> **Hilgendorf**, NJW 1997, s.1874; karşı. **Hilgendorf**, NStZ 2001, 652, özellikle 656 vd.

Benzer bir durum, hem Alman, hem de Kanada vatandaşlığına sahip olan *Ernst Zündel* davasında da yaşanmıştır. Zündel Kaliforniya'da internet üzerinde kendi adına açtığı bir sitede Nasyonel-sosyalist propaganda yapmaya başlar. Almanya Kaliforniya'daki bu sunucuya müdahale edemediği için Mannheim savcılığı Alman Telekom-Online Hizmetleri (T-Online) aleyhine ırkçı propagandaya iştirakten dolayı soruşturma başlatır. T-Online savcılığın talebi üzerine kendi müşterilerine sözkonusu siteye girişi kapatır. Amerikan servis sağlayıcı böyle bir sitenin bulunmasında herhangi bir sakınca görmez. Çünkü, Amerikan kanunlarına göre, nasyonel-sosyalist içeriklerin yayınlanması suç değildir. Sonuçta bu durum Amerika'da son derece adaletsiz bir sansür olarak nitelenmiş ve söz konusu site kopyalanarak bu defa başka adresler altında faaliyetlerine devam etmiştir<sup>63</sup>.

Yukarıda verilen bu örneklerin tersi de mümkündür. Örneğin, bir Alman Almanya'da insan haklarını savunan bir sitesi nedeniyle mesela, Sudan ya da Irak'ı ziyareti sırasında devletin şahsiyeti aleyhine suç işlemekten dolayı cezalandırılabilir. Görülüyor ki, karma teori bakımından neticenin esas alınması halinde ülkenin cezalandırma yetkisi olağanüstü genişlemekte, sanki ülke dünya jandarması haline dönüşmektedir. Bu durum, her ülke kendi yasasını uygulamak isteyeceğinden, ülkeler arası sonu gelmez yetki çatışmalarının ortaya çıkmasına neden olabilecektir.

#### *aa. Teoriyi sınırlandırma çabaları*

Yukarıdaki kabulün ortaya koyduğu diğer bir sonuç karma teorisinin artık çağdışı kaldığıdır<sup>64</sup>. Bu nedenle neticenin meydana geldiği yerin suçun işlendiği yer olarak kabulüne yorum yoluyla bazı sınırlamalar getirilmek istenmiştir. Bunlardan ilki, *subjektif yorumdur*. Buna göre, fail hareketiyle ülke içinde etki doğurmayı amaçlamışsa, sadece bu durumda fiil ülkede işlenmiş sayılmalıdır<sup>65</sup>. *Diğer bir görüşe göre ise*, neticenin ülke içinde gerçekleşmesi sadece hareketin objektif unsuru nedeniyle doğrudan ülke ile bir bağlantı yaratılabilmesi halinde kabul edilir. Örneğin, sunulmuş olan veri Almanca ya

<sup>63</sup> Haft/Eisele, 119.

<sup>64</sup> Karşl. Conradi/Schlömer, NSTZ 1996, 369.

<sup>65</sup> Collardin, CR 1995, 621; Engel Christoph, Inhaltskontrolle im Internet, AfP 3/1996, s.226; Ringel Kurt, Rechtsextremistische Propaganda aus dem Ausland im Internet, CR 1997, s.307. Dersken, NJW 1997, 1880

da Türkçe kaleme alınmış ise<sup>66</sup>. Ancak Alman hukukunda bu öneriler pek inandırıcı bulunmamıştır<sup>67</sup>.

**bb. Zarar suçu-tehlike suçu (Netice suçu-eylem suçu)**

Karma teorinin benimsenmesi ve bağlanma noktası olarak neticenin kabul edilmesi halinde ortaya çıkabilecek diğer bir sorun, suçun işlendiğinin kabulü için neticenin gerçekleşmesinin aranmadığı suçlardır. Bilindiği üzere, bu tür suçlara tehlike suçları denmektedir.

Suç tipinde belirtilen hareketin yönelik olduğu konunun hareketten etkileniş derecesine ve şekline göre suçlar geleneksel olarak zarar (netice) suçları<sup>68</sup> ve tehlike suçları<sup>69</sup> olarak ikiye ayrılır<sup>70</sup>.

<sup>66</sup> **Breuer** Barbara, Anwendbarkeit des deutschen Strafrechts auf extraterritorial handelnde Internet-Benutzer, MMR 1998, s.144; **Hilgendorf**, NJW 1997, 1876

<sup>67</sup> **Ringel**, CR 1997, 302; **Hoeren** Thomas/**Sieber** Ulrich, Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, München 1999, no.404.

<sup>68</sup> =Erfolgsdelikte

<sup>69</sup> =Gefährdungsdelikte

<sup>70</sup> Netice veya zarar suçlarında hareketin yönelmiş olduğu konuda bir zararın meydana gelmiş olması aranırken, tehlike ya da eylem suçlarında suçun konusu üzerinde zarar tehlikesinin meydana gelmesi neticenin kabulü için yeterli olup, hareketin yönelik olduğu konunun gerçekten zarara uğramış olması şart değildir. Bu anlamda bir zarar tehlikesini yaratabilme imkanının varlığı, yani eylem suç tipinin ihlali için yeterlidir. Öte yandan, tehlike suçları da somut ve soyut tehlike suçları olarak iki gruba ayrılır. *Somut tehlike suçlarında* hareketin konusu bakımından gerçekte *bir zarar tehlikesi* yaratılmış olması şarttır. Diğer bir deyişle, yasakoyucu somut tehlike suçlarında *somut durumda, korunmuş olan hukuki yararı ihlal sonucunu doğurmaya elverişli ve uygun olan ve fakat ihlali de sonuçlanmamış olmayan bir hareketi* cezalandırmaktadır (**Tröndle/Fischer**, no.13a vor § 13). Bu şekilde bir zarar tehlikesinin bulunmaması halinde somut tehlike suçu da gerçekleşmiş olmaz. O halde, somut tehlike suçlarında netice tehlikesinin meydana gelmesidir. Bu nedenledir ki, bazı yazarlar somut tehlike suçlarını da neticeli suçlar yani zarar suçları içinde sayarlar (**Ringel**, CR 1997, 303; **Tröndle/Fischer**, vor § 13 no.13). Görüldüğü üzere, belirli bir hukuki menfaat bakımından somut bir tehlikeye sebep olunması halinde tipe uygun neticenin mevcut olduğu kabul edilir (**Ringel**, CR 1997, 303; **Tröndle/Fischer**, § 9 no.3). Somut tehlike suçlarında tehlikede bulunan hukuki menfaatin zarar görüp görmeyeceği tamamen tesadüfe bağlıdır. Bu bağlamda münferit olayda genel yaşam tecrübesine dayanan “objektif-sonradan yapılan” bir tahmine göre zarar meydana gelmiyor olmalıdır (BGH, NStZ 1985, 263 vd; JZ 1985, 399). Görüldüğü üzere, somut tehlike suçları bakımından suçun oluşup oluşmadığının kabulü için zarar tehlikesinin araştırılması gerekir. *Soyut tehlike suçlarında* ise, hareketin suçun konusu üzerinde tehlike yaratmış olup olmaması araştırılmaz. Tipte yeralan icrai ya da ihmali bir hareketin yapılması ile suçun konusunun tehlikeye maruz kaldığı kabul edilir. Diğer bir deyişle, haksızlık tipi

Verilerin değiştirilmesi ya da ortadan kaldırılması gibi zarar suçlarının internet üzerinde işlenmesi halinde neticenin gerçekleştiği yerin tespiti herhangi bir sorun doğurmaz. Hatta, somut tehlike suçları bakımından da tipin kesin bir şekilde içine aldığı somut tehlikenin meydana geldiği yer, neticenin meydana geldiği yer olarak kabul edilebilir. Bu durumda tipin gerçekleşmesi için gerekli etkinin meydana geldiği yer, yani internet suçları bakımından ilgili verinin saklandığı yer neticenin meydana geldiği yerdir. Buna karşılık, internet üzerinde işlenen suç, soyut tehlike suçu ise, suçun işlendiği yerin nasıl belirleneceği, diğer bir deyişle Türkiye'nin cezalandırma yetkisinin doğup doğmayacağı bir sorun olarak karşımıza çıkabilir.

Bu sorunu çözümlenmek amacıyla Alman hukukunda iki görüşün ortaya çıktığı görülür:

- *Sınırlayıcı görüş*: Bu görüşe göre soyut tehlike suçlarında netice bulunmadığından sadece hareketin yapıldığı yer söz konusudur<sup>71</sup>. Bu durum karşısında ülke dışında pornografik bir içeriğe sahip verinin yurt dışındaki bir sunucu üzerinden sunulması, Alman sunucuya postalanması ya da mail olarak gönderilmesi halinde hareket yurt dışında yapılmış olduğundan Alman hukukuna göre cezalandırılması mümkün değildir. Görüldüğü üzere bu görüş Alman ceza hukukunun uygulama alanını olağanüstü bir şekilde sınırlandırmaktadır. Hatta, klasik neticeli suçlar ve somut tehlike suçlarında

failin hareketi içinde tükenmiştir. O halde, soyut tehlike suçlarında ihmali veya icrai hareketin yapılması ile suç konusunun tehlikeye girdiği kabul edilip, konu üzerinde gerçekten bir tehlikenin meydana gelmiş olup olmadığı araştırılmaz. Görüldüğü üzere, bu suçlar, Türk ceza hukukunun yurt içinde geçerli olması için bağlantı noktası olarak tipik hareketin sonucu anlamında tipe uygun bir neticeye sahip değildir (Karsl. **Schönke/Schröder**, § 9 no.6; **Hilgendorf**, NJW 1997, 1875 vd.). Elbette, soyut tehlike adı altında bir netice Türk hukukunda öngörülmemiştir. Bu anlayışa göre, bu suç tipleri cezalandırılabilen bir hareketin yapılmasıyla gerçekleşmiş olur. *Soyut tehlike suçlarının amacı*, hukuki menfaat için somut bir tehlike oluşmadan önceki alanda bir hareketi ceza yaptırımını altında bulundurmaktır. Mesela, ülke içinde yaşayan bir azınlığa dönük düşmanlık içeren yazıların yer aldığı broşürlerin dağıtılması ya da ırkçılığı konu olan filmlerin gösterilmesi (bkz. **Ringel Kurt**, *Rechtsextremistische Propaganda aus dem Ausland im Internet*, CR 5/1997, 302 vd., özellikle s.304 vd) ve bunun gibi bir vitrinde pornografik resimlerin teşhir edilmesi gibi. Tüm bu fiillerde failin hareketinin somut etkisi dikkate alınmaz. Bu anlamda böyle bir broşürü okuyan kişinin azınlık mensubuna saldırması ya da filmi seyreden yabancıya sövmesi ve nihayet pornografik resimleri gören küçüğün psikolojik olarak şoka girmesi tipin gerçekleşmesi bakımından önemli değildir.

<sup>71</sup> **Schönke/Schröder**, § 9, no.6; **Tröndle/Fischer**, § 9, no.3. Karsl. OLG München, StV 1991, 504

da yurt dışında yapılan bir hareketin Almanya'da sebep olduğu neticenin sadece hareketin ülke dışında da ceza tehdidi altında bulunması halinde cezalandırılabilirliği söylenir<sup>72</sup>.

- *Genişletici görüş*: Buna karşılık genişletici görüş olarak adlandırılabilir olan karşı görüş, soyut tehlike suçlarında *soyut tehlikenin gerçekleşebileceği her yeri* "neticenin gerçekleştiği yer" olarak kabul eder<sup>73</sup>. Tüm dünyayı içine alan internette işlenen beyan suçları bakımından soyut olarak tehlikeye girmiş alanın sınırlandırılması kesinlikle mümkün değildir. Bu durumda, eğer tehlikenin meydana geldiği her yerin neticenin de meydana geldiği yer olduğu kabul edilecek olursa, Türkiye'den de ulaşılabilir olduğuna göre, TCK tüm dünyaya yayılmış bulunun internet üzerindeki verilere uygulanabilir ve bu veriler hakkında Türkiye'de ceza takibatı yapılabilir hale gelecektir. Buna göre, ülke dışında hareket eden bir kişi, sadece ponografik yazı ya da hakaret içeren açıklamaları ülkeye mail ile göndermekle ülke hukukuna göre cezalandırılabilir olmakla kalmaz, aynı zamanda gönderme dahi yurt dışındaki sunucuda yer alan bu içeriğin orada bulunuyor olması, bu sunucunun ülke ile hiç bir ilgisi olmaması halinde dahi yine ülke hukukuna göre cezalandırılabilir. Çünkü internet yolu ile tüm bilgisayarların birbirine bağlanabilmesinin mümkün olması, böyle bir sunucuda saklanmış olan veriye ülkeden ulaşılabilmesi son derece kolay olduğundan soyut bir tehlike oluşturacaktır. Bu durum, ülkenin cezalandırma yetkisinin global bir şekilde genişlemesi sonucunu doğuracağı gibi, böyle bir kabul elbette devletler hukuku bakımından bazı problemleri de beraberinde getirecektir. Çünkü, söz konusu soyut tehlike tüm dünyada eşit şekilde ortaya çıkacağından münferit her bir ülkenin cezalandırma yetkisi bakımından yeterli bir bağlanma sebebi oluşturacaktır<sup>74</sup>.

Görüldüğü üzere, bu görüş de ülke hukukunun uygulanabilme olanağını olağanüstü derecede genişletmiş ve pratik olarak dünyadaki internet üzerindeki tüm verileri ülke ceza hukukunun uygulanabilirliği içine almış

<sup>72</sup> **Kienle**, Internationale Strafrecht und Straftaten im Internet 1998, 173 vd.

<sup>73</sup> **Beisel Daniel/Heinrich Bernd**, Die Strafbarkeit der Ausstrahlung pornografischer Sendungen in codierter Form durch das Fernsehen, JR 1996, s.96; **Heinrich Bernd**, Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999, s.83 vd.; **Kuner**, CR 1996, 456; **Martin Jörg**, Grenzüberschreitende Umweltbeeinträchtigungen im deutschen Strafrecht, ZRP 1992, s.19 vd.. Bu yöndeki yargı kararları için BGHSt 42, 235 (242) (NJW 1997, 138); BGH, NStZ 1990, 36 /37)

<sup>74</sup> **Cornils Karin**, Der Begehungsort von Äußerungsdelikten im Internet, JZ 1999, s.395.

bulunmaktadır<sup>75</sup>. Böyle bir sonuç kısmen kabul de görmüştür<sup>76</sup>. Ancak, bu kabul bizi ülke ceza hukukunun oldukça geniş bir uygulama alanı bulması sonucuna götürür. Bu uygulama, hem ülke soruşturma makamlarının suçu takip yükümlülüğünü koşturma mecburiyeti ilkesi gereği dünya çapında genişletir, hem de bazı devletler hukuku sorunları çıkarabilir. Şayet diğer ülkeler de bu görüşü benimseyecek olursa, hemen hemen tüm ülkeler internet üzerinde yer alan verileri takip etmekle yükümlü hale geleceklerdir. Böylece, teorik de olsa, ulusal ceza hukuku düzenleri internet alanında dünya çapında uygulama alanı bulacaktır. O halde, neticeye üstünlük veren karma teori internet üzerinde işlenen bu şekildeki fiiller bakımından tatmin edici olmaktan uzaktır.

- *Yeni çözüm denemesi*: Bu konudaki en yeni teoriye göre, hareketten zaman ve yer olarak ayrılabilen dış etkilenme olarak dar anlamda netice yanında, hareket tarafından yaratılan, hareketin realize ettiği her etki hareketin neticesi olarak anlaşılmalıdır<sup>77</sup>. Bu görüşe göre, esas alınması gereken şey tehlike suçu-zarar suçu gibi fiillerin belirli dogmatik kategorilerde tasnif edilmesi değil, sadece söz konusu suç tipinin lafzıdır. *Her somut olayda hareketin neticesi olarak failin hareketinin etkisi değerlendirilmeli* ve böylece neticenin meydana geldiği yer belirlenmeye çalışılmalıdır. Buna göre, mesela, pornografik yazıların «girilebilir kılınması» tipe ilişkin bir neticedir ve böylece bu şekildeki yazıların Türkiye'ye gönderilmesi durumunda netice Türkiye'de meydana gelmiş sayılır ve Türk ceza kanunlarının uygulanması mümkün hale gelir. Kaldı ki, burada söz konusu olan hareketler bakımından önemli olan husus verilerin görülebilir, ulaşılabilir kılınmış olması; böyle bir imkanın bulunmasıdır.

Gerçekten yasakoyucu suç tiplerinin yaratılması ile iç hukuktaki hukuki menfaatlerin korunması amacıyla normlar çıkarmıştır. Bu normlar vasıtasıyla yurt dışından da kaynaklanmış olan hareketler ile bu hukuki menfaatlerin ihlal edilmesi önlenmelidir. Bu koruma beyan suçlarında olduğu gibi soyut tehlike suçlarının yaratılması için yasakoyucuyu harekete geçiren hususlardan birini oluşturmuştur. Bu yasal düzenlemeler ilgili hukuki menfaat üzerinde böyle bir etkilenmenin ve bu suretle ortaya çıkacak tehlikenin engellenmesini amaçlar. Burada failin bulunduğu yerin ülke içinde veya dışında olmasının önemi bulunmaz. Karma teori bakımından temel düşünce, ilgili ceza normu ile

<sup>75</sup> Karsl. Collardin, CR 1995, 620; Conradi/Schlömer, NSTZ 1996, 368 vd.; Flechsig/Gabel, CR 1998, 351 vd.

<sup>76</sup> Flechsig/Gabel, CR 1998, 352; Heinrich, GA 1999, 76, 82.

<sup>77</sup> Hoeren/Sieber, no.405



korunması gerekli olan hukuki menfaatin zarar görmesi ya da tehlikeye uğraması olup, bu ülke içinde gerçekleşmişse daima ülke ceza hukuku uygulanmalıdır. *Ülke ceza hukukunun uygulanması için tespit edilebilir bir etkinin varlığı yeterlidir.* Bu anlamda tipiklik kavramı altında sadece maddi anlamda bir netice değil, biçimsel anlamda bir netice de anlaşılmalıdır. Yasakoyucu soyut tehlike suçlarında belirli faaliyetleri genel olarak tehlikeli ve cezalandırılabilir olarak kabul etmiştir. Bu tür suçlar bakımından failin yurt dışında ya da yurt içinde hareket etmiş olmasının önemi bulunmaz. Aksi halde, yurt dışından ülke üzerine hiç bir rizokoya girmeksizin etkide bulunma imkanı doğar. Böylede sınırdan sadece bir kaç metre ötede de olsa, yurt dışında bulunuyor kabul edileceğinden failin cezalandırılmayacağı bir durum ortaya çıkmış olacaktır. Halbuki, karma teorinin ve bunu kabul eden yasakoyucunun amacının bu olamayacağı açıktır. Çünkü, böyle bir kabulün amacı “ülkede işlenen fiil” kavramını mümkün olduğu kadar genişletebilmehtir. O halde, bir içeriği internete bilinçli olarak veren, bunların ülke dışında da okunabileceğini bilir. Bu kişi söz konusu içeriğin çağrılabilceğini ve okunabileceğini hesaplamak zorundadır. Tıpe ait neticenin “dış dünyada değışiklik meydana getirmesi” ile sınırlandırılması gerekli değildir<sup>78</sup>.

O halde, sonuç olarak, failin hareketinin etki doğurduğu her yer suçun işlendiği yer olarak kabul edilmelidir. Bu durumda hareketin yapıldığı yer yanında, ülke dışında ülkeye etkide bulunmuş ise, ülke söz konusu tehlikenin ortaya çıktığı yer olarak soyut tehlike suçlarının maddi neticesinin meydana geldiği yerdir. Soyut tehlike suçları bakımından ülke ceza kanununun uygulanma imkanını daraltmak da ülkeyi hedef alan bazı suçların cezasız kalmasına yol açacağı için kabul edilemez. Ancak, ülke ceza kanunlarının da gereksiz bir şekilde her fiil için uygulanmasını engellemek bakımından bir “orta yol” tutulmalı, failin fiilinin etkilerinden habersiz bir şekilde hareket etmiş ve bu şekilde hareket etmiş olmakla ülke içinde etki etmeyi istememiş ise artık ülke kanununun uygulanması kabul edilmemelidir<sup>79</sup>. Bununla birlikte, failin ülkede faaliyet ve etkide bulunmak amacıyla hareket ettiği belirlenebiliyorsa, artık ülke kanunu uygulanmalıdır. Bu konuda örnek olarak söz konusu içerikte *kullanılan dil* verilebilir.

Ne var ki, getirilen bu çözümün kusursuz olduğu iddia edilemez<sup>80</sup>. Tüm bu tartışmalara son vermek bakımından burada en iyi çözüm tarzı, yasakoyucunun bu konuda açık bir düzenleme getirmesidir. Hemen şunu

<sup>78</sup> Finke, 49 vd.

<sup>79</sup> Karşl. Finke, 58.

<sup>80</sup> Karşl. Derksen, NJW 1997, 1880

söylemeliyiz ki, yurt içinde faaliyet gösteren servis sağlayıcı ya da içerik sahibi bakımından ülke soruşturma makamlarının yetkili olduğu hususunda herhangi bir problem mevcut değildir. Doğal olarak bunlar ülke ceza hukukunun uygulama alanı içinde bulunacaklardır. Bu, kullanıcının yurt dışında olması halinde de geçerlidir. Bu durumda, içeriğin internet ortamına verildiği, yani hareketin yapıldığı yerin yurt içinde olması yeterlidir.

***b. Bağlanma Noktası Olarak Hareketin Yapıldığı Yerin Esas Alınması***

***- "Gizli (Hayali) mevcudiyet" önerisi***

Geleneksel anlayışa göre hareketin yapıldığı yer, failin fiili işlediği sırada bedensel, cismani olarak bulunduğu yerdir. Mesela, İranlı bir radikal islamcı Tahrandaki web sayfasından devletin dini temellere göre kurulmasını içeren verileri internete sunuyor ise hareketin yapıldığı yer Tahran'dır. İnternetin yere (mekana) bağlı olmayan özel yapısı ile bulunulan yer unsurunun telif edilebilmesi amacıyla "gizli, hayali mevcudiyet" önerisi geliştirilmiştir. Buna göre, internet üzerinden veriyi sunan her kişi dünyanın her yerinde, her ülkesinde sunduğu verilerine ulaşılabilen bir kişi olarak aslında "saklı" olarak bulunmaktadır<sup>81</sup>. Bu sonuç, elbette verilerin suç niteliği taşıyan içeriklere sahip olması halinde cezalandırma yetkisi bakımında dünya çapında bir çatışmanın oluşmasına yol açacaktır. Çünkü böyle bir kabul bizi hareketin her ülkede yapıldığı sonucuna götürecektir ve iç hukuk bakımından suç teşkil ettiği sürece soruşturulabilir kılacaktır. Böylece her ülke internette dolaşan ve he zaman girilebilen illegal verileri soruşturabilir bir hale dönüşecektir.

Görüldüğü üzere, bu görüş de aynen neticeye ilişkin görüşlerde olduğu gibi kabul edilemez sonuçlara yol açmaktadır.

***- Hareketin yapıldığı yer-bulunulan yer ayrımı***

Birbirinden uzak mesafede bulunan iki kullanıcı arasındaki bağlantının özel teknik işleyiş şekli, birinin sakladığı verilere diğerinin tecavüz edebilmesini mümkün kılabilir. Verilere ulaşılması yanında, verilerin kaydedilmesi ya da silinmesi uzaklık ne olursa olsun mümkün olabilir. Bu durumda vasıta araç ile interneti kullanan yani hareket eden kişinin, bu sırada bulunduğu yer ile amaç aracın yani üzerinde hareketin gerçekleştirildiği aracın bulunduğu yer birbirinden farklıdır. Bu suretle, hareket yer olarak

<sup>81</sup> Kuner, CR 1996, 454.

birbirinden ayrılır. Yani, bunun anlamı şudur; her iki kullanıcının bulunduğu yer, hareketin yapıldığı yer olarak kabul edilir. Örnekler:

- Paris'te bulunan bir İspanyol internet üzerinden Frankfurt'taki bir Alman bankanın ana bilgisayarına girer ve oradaki hesabından bir havale yapar. Bu durumda makine Almanya'da olduğu için bu İspanyol Almanya'da imiş gibi hareket etmiştir.

- Bir Alman Madrid'e yaptığı gezi sırasında Almanya'da bulunan mail servisindeki elektronik posta kutusundaki maili kontrol etmiş ise, doğrudan doğruya mail servisi üzerinde yani Almanya'da hareket emiş sayılacaktır.

- Aşırı sağcı bir Danimarkalı ırkçı içeriğe sahip web sayfasını Hamburg'ta kurulmuş bulunan servis sağlayıcı üzerinde saklamışsa, Almanya'da hareket etmiş sayılır ve hakkında Alman ceza hukuku uygulanır.

İnternette işlenmiş olan mesela cürüm fiilini övmek, halkı kin ve düşmanlığa sevk etmek, devletin gizli bilgilerini açıklamak, halkı isyana teşvik, cumhurbaşkanına hakaret, dost bayrağına hakaret, müstehcen şey yazmak ve yayınlamak gibi suçlarda kamuya yönelik bir hareket tarzı söz konusudur. Bu suçlar bakımından suçun işlendiği yer - failin ikamet ettiği yerden ayrı olarak- failin söz konusu içeriğe sahip bilgileri belirsiz pek çok ve kişisel olarak tespit edilmeyen kişiler için ulaşılabilir olmayı mümkün kıldığı yer sunucudur. Bu çerçevede, yurt dışından bu tür verileri Türkiye'de kurulmuş olan bir server üzerinde kontrol eden ve saklayan kişi de Türkiye'de hareket etmiş sayılır. Bu nedenle fiili Türkiye'de işlenmiş gibi takip edilmelidir<sup>82</sup>.

Girilebilir kılmak failin üçüncü kişileri onun verilerine müdahaleyi mümkün kılan hareketi nedeniyle cezalandırılabilir. Fail illegal verileri belirli ya da belirsiz kişiler için ulaşılabilir kılmıştır. Fail, verileri mail-server üzerinde saklamak ve bu suretle sunucu ya da server üzerine kaydetmek suretiyle illegal içeriğe belirli kişilerin girmesini mümkün kılmıştır. Hareket sadece failin ikamet ettiği yerde değil, aynı zamanda failin verileri girilmesi amacıyla hazır tuttuğu söz konusu server ın bulunduğu yerde de yapılmış sayılır.

**Sonuç olarak;** internette işlenmiş olan fiillerin işlendiği yerin tesbiti ve Türk ceza hukukunun uygulanabilirliği bakımından aşağıdaki sonuçlara ulaşılır:

- Ağ, Türkiye'den besleniyorsa, yani veri girişi Türkiye'den yapılıyor ise suç daima ülkede işlenmiş sayılır ve Türk ceza hukuku uygulanır.

<sup>82</sup> Cornils, 397

- Yurt dışından gönderilmiş olsa bile, hukuka aykırı içerik taşıyan bir veri Türkiye’de kurulmuş bir sunucu üzerinde dosyalanmış ise, yine yurt içinde işlenmiş olan bir suçtan söz edilir. Çünkü, fail doğrudan doğruya bu sunucu üzerinde hareket etmiştir ve bu nedenle suçun ülke içinde işlendiği kabul edilir.

- Veri içeriği yurt dışı kaynaklı ve veri fail tarafından yurt dışındaki bir sunucu üzerinde saklanıyorsa yabancı ülkede hareket edilmiş sayılır. Bu durumda Türk ceza hukukunun geçerliliği sadece belli koşullar altında yani, özellikle fail ya da mağdurun Türk vatandaşı olması diğer bir deyişle şahsılık prensibi, korunma prensibi veya evrensellik prensibinin koşulları gerçekleşmiş ise kabul edilebilir. Örneğin, çocukları konu alan pornografik resimler gibi.

## II. İNTERNET VE CEZA MUHAKEMESİ HUKUKU: İNTERNET YOLUYLA YAPILAN HABERLEŞMENİN DENETLENMESİ

### A. KAVRAM

İletişim teknolojisinde kaydedilen olağanüstü gelişim ve bu gelişimin hızla günlük hayata ve davranış şekillerine yansımaları, ceza muhakemesinde internet üzerinde yapılan haberleşmenin denetlenmesi yoluyla delil elde edilmesi zorunluluğunu da beraberinde getirmiştir.

İnternet üzerinde gerçekleştirilen haberleşme şekillerinden en yaygını e-mail olmakla birlikte, söz konusu haberleşmenin bununla sınırlı olmadığı söylenmelidir. *Elektronik posta* ya da e-mail kağıtsız, dijital bir posta sistemi olarak tanımlanabilir. Bunun için, önce kullanıcının bir e-mail adresine sahip olması gerekir. E-mail adresi, servis sağlayıcıları yanında, internet üzerinde bulunan çok sayıdaki e-mail sistemlerinden elde edilebilir. E-mail içine, sadece yazı değil, resim, grafik, görüntü ve hatta ses eklenebilir<sup>83</sup>. E-mail, kural olarak, en güvenilir iletişim araçları içinde yer alır. Çünkü, kullanıcı ismi ve şifre olmadan okunabilmesi mümkün değildir. E-mail yoluyla haberleşmek için bilgisayarın açık olması da gerekmez. E-mail alıcı için ayrılan dijital posta kutusunda depolanır ve istenildiği zaman internet bağlantısı kullanılarak ilgili mesajlara ulaşılabilir. Böylece e-mail iki kişi arasında eşzamanlı olmayan iletişim olarak karşımıza çıkar<sup>84</sup>. Ancak, e-mailin anonim iletişimi mümkün kılması, bu iletişim yönteminin kriminal amaçlar

<sup>83</sup> Gercke, 12.

<sup>84</sup> Atabek, Amme İdaresi Dergisi, C.34, Mart 2001, s.55.

için kullanılması bakımından onu oldukça cazip hale getirmektedir. Yine internet üzerinde en fazla kullanılan haberleşme araçlarından birisi de sohbet, yani *chat*<sup>85</sup> dir. Chat, kullanıcıların eşzamanlı olarak internet üzerinden konuşmalarını sağlayan sohbet ortamıdır. Bunun için, sohbet odası denen platformlara katılmak gerekir. Chat de e-mail gibi anonim bir haberleşmeyi mümkün kılmakta olup, teati edilen içeriğin kontrolü de oldukça zordur<sup>86</sup>. Nihayet, belli konularda grup oluşturan çok sayıda kişi arasında görüş alışverişi veya tartışma olanağı sağlayan *forumlar* ve konularına göre hiyerarşik olarak sınıflanmış binlerce haber grubundan oluşan ve dünya üzerindeki milyonlarca kullanıcının görüş ve düşüncelerini açıklamak üzere yazı ve haber gönderdiği tartışma platformları olarak tanımlanabilen, çok kişi arasında eşzamanlı olmayan iletişim olan *usenet* de söz konusu haberleşme araçları arasında sayılmalıdır. Bu haberleşme araçları da daha çok çocuk pornografisi içeren resim vb. nin sunulduğu ortamlar olarak kötüye kullanılabilir<sup>87</sup>.

İnternet üzerinden yapılan haberleşmenin denetlenmesi aslında, aynı yerde bulunmayan iki kişi arasında araya telefon, teleks, faks, bilgisayar gibi bir vasıta sokularak yapılan haberleşmenin ceza koğuşturması amacıyla denetlenmesi olarak tanımlanabilecek olan *uzakla haberleşmenin denetlenmesinin*<sup>88</sup> değişik bir görünümü olarak ortaya çıkar.

<sup>85</sup> IRC= Internet Relay Chat

<sup>86</sup> Gercke, 12.

<sup>87</sup> Gercke, 13.

<sup>88</sup> Terim hakkındaki tartışma ve kavram ile ilgili olarak bkz. Erdem M.Ruhan/Özbek, V.Özer, 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu Çerçevesinde Uzakla Haberleşmenin Denetlenmesi, Edis'e Armağan, İzmir 2000, s.250. Buradaki uzak terimi, araya bir vasıta sokulması anlamına gelmektedir. Yoksa haberleşen kişilerin uzak mesafelerde olması anlamına gelmez. Pekala yanyana bulunan iki ayrı odadaki kişilerin telefon vb. araçlarla haberleşmeleri de uzakla haberleşmedir. "Telefon, teleks, faks gibi haberleşme araçları" terimi yetersizdir. Çünkü, bilgisayar bir haberleşme aracı değildir. Ancak internet ortamının kullanılması halinde bir haberleşme aracı haline gelebilmektedir. "Telekomünikasyon" terimi de açıklanmaya muhtaç bir terimdir. Ancak mehazı oluşturan Alman CMUK bu konuda "Fernmeldeverkehr" terimini kullanmakta olup, konuyu düzenleyen § 100a'nın başlığı "Überwachung des Fernmeldeverkehrs"dir. Bu terim, doktrinde de aynı şekilde kullanılmaktaydı (Bkz. Kleinknecht/Meyer-Goßner, Strafprozessordnung, Mit GVG und Nebengesetzen, 44. Aufl., München 1999, § 100a no.1 vd.; Roxin, Strafverfahrensrecht, 25. Aufl., München 1998, § C IV 3; Löwe-Rosenberg, StPO Grosskommentar, 24.Aufl.,Berlin Newyork 1986, s.134 vd). Ne var ki, 17.12.1997 tarihli Alman Tekekomunikasyon Yasası İçin Eşlik Yasası (BegleitG-BGBl. 1997 I, s.3108) § 2 IX b.2, A1.CMUK § 100a'yı değiştirmiş, başlık aynı kalmakla birlikte, ilk

Ülkemizde uzakla haberleşmenin denetlenmesi etrafındaki tartışma uzunca bir süre devam etmiş, hakkında yasal düzenleme bulunmayan bu tedbir ile ilgili eleştiri ve görüşler yasakoyucuda yankı bulmuş ve nihayet 30.07.1999 tarih ve 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2.maddesinde "**iletişimin dinlenmesi ve tesbiti**" başlığı altında yasalaşmıştır. Aşağıda da belirtileceği üzere, söz konusu tedbir ile ilgili düzenleme kaynak ülke Almanya'da olduğu gibi her suç bakımından uygulanabilen CMUK içinde yapılmış olsa, daha iyi olurdu. Çünkü, şu an ki düzenleme karşısında ÇASÖMK kapsamına girmeyen suçlar bakımından internet üzerinde yapılan e-mail vb. haberleşmenin denetlenmesi, bu anlamda örneğin, elektronik posta kutularındaki (mail-box) verilerin denetlenmesi mümkün değildir.

ÇASÖMK m.2/1'e göre "*Bu Kanunda öngörülen suçları işleme veya bunlara iştirak yahut işlendikten sonra faillere her ne suretle olursa olsun yardım veya aracılık veya yataklık etme kuşkusu altında bulunan kimselerin kullandıkları telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyalleri, yazıları, resimleri, görüntü veya sesleri ve diğer nitelikteki bilgileri dinlenebilir veya tespit edilebilir*". Görüldüğü üzere yasada açıkça e-mail ile yapılan haberleşmeden bahsedilmemekle birlikte, hükümde yer alan "**... bilgisayar gibi ... elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyaller, yazılar, resimler, görüntü veya sesler ve diğer nitelikteki bilgilere** e-mailin de dahil olacağı açıktır<sup>89</sup>. Zira e-mail de madde kapsamına giren iletişim araçlarından biridir. O halde, söz konusu düzenleme, internet üzerinden e-mail vb. ile yapılan haberleşmenin denetlenmesini mümkün hale getirmiştir. Alman Yargıtayı da uzakla haberleşmenin denetlenmesi tedbirini düzenleyen Alman CMUK § 100a'nın haber gönderiminin her şekli bakımından uzakla haberleşmenin denetlenmesini mümkün hale getirdiği görüşündedir<sup>90</sup>. Aynı görüş, öğreti tarafından da desteklenmektedir<sup>91</sup>.

fıkradaki "*uzakla haberleşme*" terimi yerine "*telekomünikasyon*" terimini getirmiştir. Alman Teleservisler Yasası § 3 no.16 "*telekomünikasyon*" terimini tanımlamak suretiyle modern iletişim araçlarının Al.CMUK § 100a kapsamına girip girmediği üzerindeki şüpheleri tamamen ortadan kaldırmıştır (Bär Wolfgang, EDV-Beweissicherung im Strafverfahrensrecht, CR 1998/7, s.435; Bär Wolfgang, Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, MMR 8/2000, s.473).

<sup>89</sup> Aslında bu tanım ile "*Telekomünikasyon*" terimini tanımlayan Alman Teleservisler Yasası § 3 no.16 arasında çok büyük fark bulunmamaktadır. ÇASÖMK Uygulanmasına İlişkin Yönetmelik m.4 de iletişim kavramını tanımlamış bulunmaktadır.

<sup>90</sup> BGH, NJW 1997, 1934.

Gerçekten hukuki anlamda verilerin hangi şekilde nakledildiği, bu anlamda ses ya da yazı arasında bir fark bulunmamaktadır.

Bir elektronik posta kutusunun denetlenmesi teknik olarak üç farklı aşamada gerçekleştirilebilir<sup>92</sup>: *Birinci aşamayı* söz konusu verinin göndericinin bilgisayarından internet sunucusunun mail-server'ına ulaşması oluşturur. *İkinci aşama*, verinin "beklemesi" yani, adres sahibinin bu maili açması anına kadar, mailbox'ı işletenin (sunucunun) saklama alanı üzerinde saklanmasıdır. Nihayet *üçüncü aşama*, mailin alıcı tarafından çağırılması, yani, mailbox işletenin ağından alıcının ağına aktarılmasıdır. İkinci aşama birkaç saat olabileceği gibi günler de sürebilir. Birinci ve üçüncü aşamalardaki denetim konusunda ÇASÖMK m.2'nin geçerli olacağı söylenmelidir<sup>93</sup>. Burada asıl tartışma konusu, mailboxı işleten sağlayıcının (sunucu) hafızasında (deposunda) "bekleyen" veri bakımındandır. Dikkat edilirse, burada haber (veri) erişim sağlayıcı tarafından, onun nezdinde saklanıyor olmakla birlikte, henüz alıcıya ulaşmış değildir. Alman hukukunda bu konuda doktrin<sup>94</sup> Al.CMUK § 94 ve § 102 yani elkoyma ve aramaya ilişkin hükmün, Alman Yargıtay'ı<sup>95</sup> ise haberleşmenin denetlenmesine ilişkin § 100a ve

<sup>91</sup> **Nack** Armin, Strafprozeßordnung, Gerichtsverfassungsgesetz, in: Karlsruher Kommentar, 4.Aufl., München 1999, § 100a, no.6, 7 vd.; **Pfeiffer** Gerd, StPO, Strafprozessordnung, 3.Aufl., München 2001, § 100a, no.4; **Bär**, CR 7/1998, 435; **Bär**, MMR 8/2000, 473; **Kleinknecht/Meyer-Göbner**, § 100a no.2. Aksi **Hoeren**, no.363

<sup>92</sup> **Nack**, in: Karlsruher Kommentar, § 100a, no.7; **Bär**, MMR 8/2000, 474; ayrıca karşı. **Palm Franz/Roy** Rudolf, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, s.1791; **Kleinknecht/Meyer-Göbner**, § 100a, no.2

<sup>93</sup> **Nack**, in: Karlsruher Kommentar, 100a, no.7; **Palm/Roy**, NJW 1996, 1791.

<sup>94</sup> **Nack**, in: Karlsruher Kommentar, 100a, no.8. Ayrıca karşı. **Bär** Wolfgang, Polizeilicher Zugriff auf kriminelle Mailboxen, CR 1995, s.489; **Palm/Roy**, NJW 1996, 1791; **Kleinknecht/Meyer-Göbner**, § 100a, no.2; **Palm Franz/Roy** Rudolf, Der BGH und der Zugriff auf Mailboxen, NJW 1997, 1905; karşı. **Bär**, MMR 8/2000, 475; **Gercke**, 185, 187.

<sup>95</sup> BGH, CuR 1996, 488. Mahkeme, bu şekilde müdahaleleri de "uzakla haberleşmeye müdahale" olarak kabul etmekte olup, § 100a Al.CMUK un uygulanma alanı sadece aktüel gönderimlerle sınırlanmaz. Aksine mail-box'da henüz açılmamış, ancak ulaşılabilir bulunan mailleri de kapsamına alır. Ancak bu müdahale iki açıdan sınırlandırılmalıdır. Birincisi, aramaya ilişkin § 103 Al.CMUK daki koşullar ilave olarak aranmalıdır. Yani soruşturmanın amacına hizmet eden tamamen belirli verilerle sınırlı olmalıdır. İkincisi, verilere bu şekildeki müdahale § 100a da belirtildiği gibi 3 ay değil, sadece bir defa yapılabilir. Al.CMUK § 103 ye tekabül eden ve benzer düzenleme içeren m.95'e göre aramanın yapılabilmesi m.94'e nazaran daha farklı ve ağır koşullar içermektedir (Karşı.

aramaya ilişkin § 102 ve § 103. ün (m.94, 95 türk.CMUK) uygulanması gerektiğini ileri sürmektedir. **Kanımca**, elkoymaya ilişkin hükmün ya da hükümlerin uygulanması mümkün değildir. Çünkü, elkoymanın konusunu oluşturan “eşya” maddi varlığı olan şeyleri kapsamaktadır<sup>96</sup>. Öte yandan, tedbir postada elkoyma bakımından değerlendirildiğinde, CMUK m.91 elkonulabilecek şeyleri sınırlı bir şekilde saymış olup, sair mersule terimi içinde e-mail vb. haberleşme araçlarının sokulması, sınırlayıcı hükümlerde kıyas yasak olduğu için mümkün değildir. Öte yandan, aramanın konusunu şüpheli ya da sanığın *evi ile ona ait sair mahaller, üzeri ve eşyası* oluşturur (m.94/1 CMUK). Eşya kavramı içine aramaya maruz kalanın kişisel bilgisayarını yani, bilgisayarın hard diski girebilir<sup>97</sup>; ancak, mail-box hard disk üzerinde değil, mail servisi üzerinde bulunduğu için eşya kavramı içinde değerlendirilmesi mümkün değildir kanısındayım. Bu söylenenler bir yana bırakılsa dahi, CMUK m.98’e göre arama sırasında aramaya maruz kalan kişi ya da bir ilgili arama sırasında “fiziksel olarak” hazır bulunmalıdır. O halde, arama hiç bir zaman “gizli” bir şekilde icra edilemez<sup>98</sup>. Yine, sınırlayıcı hükümlerde kıyas yasağı olması nedeniyle elkoymada olduğu gibi aramaya ilişkin hükümlerin kıyasen uygulanması da olanaksızdır.

Kanımca, ikinci aşama olarak ifade edilen bu aşamada ÇASÖMK m.2’ye göre de denetim yapılması mümkün değildir. Hüküm yakından incelendiğinde “... **ALINAN VEYA İLETİLEN**” sinyallerin, yazıların, resimlerin, görüntü veya seslerin ve diğer nitelikteki bilgilerin dinlenebilir veya tespit edilebilirliğinden söz etmektedir. Dolayısıyla, verinin mail boxta bulunması “iletişim” ya da “uzakla haberleşme” olarak nitelenemez<sup>99</sup>. Gerçekten 2.m.’de izin verilmiş olan, devletin, üçüncü kişi olarak, kontrol edilecek olan

**Özbek** Veli Özer, Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Arama, Ankara 1999, s.86).

<sup>96</sup> **Gökçen** Ahmet, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma, Ankara 1994, s.79.

<sup>97</sup> **Özbek**, 118.

<sup>98</sup> Aksi **Gercke**, 187. Gerçekten yazar CMUK m.98 ve 99 hükmünün düzenleyici nitelikte olduğunu, on-line müdahalenin yoğunluğunun klasik aramadan daha az olduğunu ileri sürmektedir. CMUK m.97, aramanın ne şekilde yapılması gerektiği hususunda uygulayana direktif verir niteliktedir. Nitekim, “bulundurulur” diyerek tedbiri uygulayana başka bir alternatif bırakmamaktadır. Öte yandan, on-line müdahale ilgilinin haberi olmayacağı için, diğer “açık” tedbirlere nazaran tam tersine daha yoğun bir müdahale içerir (Karşl. **Özbek**, 129).

<sup>99</sup> Karşl. **Bär** Wolfgang, Anmerkung zum Beschluß des BGH vom 31.07.1995, CR 1996, s.491.



iletişimin akışına katılması olup, burada, bağlantı aksine soruşturmayı yürüten memurca bizzatihi oluşturulmaktadır. Öyle ki, burada denetleyenden üçüncü kişi olarak bahsetmek olanaksız olup, denetleyen ve denetlenen olarak iki kişi söz konusudur. Bu nedenle mail-box ın m.2'ye göre denetlenmesi olanaksızdır. Bu durumda, ancak m.4'e göre "kayıt ve verilerin incelenmesi" söz konusu olabilir. Buna göre, "Bu Kanunda öngörülen suçların veya delillerinin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumdaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenebilir".

Öte yandan, burada tartışılacak olan husus hangi hükmün uygulanacağı yanında, mailbox ı işleten nezdinde denetim yapılması için tedbirin uygulanması bakımından gerekli koşulların oluşup oluşmadığıdır. Çünkü, bu durumda, tedbire maruz kalacak olan mailboxı işleten olduğundan ve mailboxı işletenin her maili denetlemesi gibi bir yükümlülüğü bulunmadığından ve bu teknik olarak da mümkün olmadığından şüpheli olarak kabul edilmesi mümkün değildir. Dolayısıyla, denetim ya gönderici ya da alıcının mailboxında yapılabilir.

Böyle bir tespitten sonra elde edilen, örneğin, cd ya da disketin artık keşif konusu (m.78 vd. CMUK) olacağı açıktır. Bu durumda mahkeme gerekirse bilirkişiye başvurabilir.

### B. AMAÇ

Bir koruma tedbiri olan e-mail ile iletişimin denetlenmesinin amacı yapılmakta olan ceza soruşturması çerçevesinde **delil araçlarının elde edilmesidir**. Bununla birlikte, söz konusu tedbire zaman zaman **önleyici amaçla** başvurulduğu da görülmektedir<sup>100</sup>. Tehlikeye karşı koyma amacıyla, yani e-mailin önleyici amaçla denetlenmesi ile, koğuşturma amacıyla yapılan

<sup>100</sup> **Bär** Wolfgang, in:Wabnitz/Janovsky, Handbuch der Wirtschaftskriminalität, no.253 vd. Nitekim Alman Federal Suç Dairesi ayrı bir birim oluşturmak suretiyle 1999 Ocak'ından bu yana ülke çapında internet üzerinde gerçekleştirilen özellikle çocuk pornografisi, aşırı siyasi faaliyetler, kredi kartı dolandırıcılığı gibi fiillerin izini sürmektedir. Bu çerçevede 12 memur herhangi bir şüphe sebebinden bağımsız olarak internette sörf yapmaktadır. Bunlara ilave olarak 8 "internet-polisi" de aşırı sağ ve sol grupların yayınlarını araştırmaktadır. Böylece internetteki bu sıkı polisiye önlemler interneti potansiyel suçlular için güvensiz bir ortam haline getirmiştir. Nitekim 1999 Ekiminde bu tedbirler özellikle çocuk pornografisi fiiline ilişkin şüphe sebeplerinin varlığını ortaya koyan 1000 civarında olayı ortaya çıkartmıştır (**Zöller**, 567; karşı. **Gercke**, 170 vd.).

denetlemeyi birbirinden ayırmak oldukça güçtür. Bu yönüyle, tedbire zaman zaman istihbarat amacıyla da başvurulmaktadır. Bugün, gizli yollarla bilgi elde etme amacını güden müdahalelerin, önleyici alana da yaygınlaştırılması gerektiği anlayışı gittikçe daha fazla taraftar bulmaktadır. Özellikle organize suçluluğun giderek arttığı gerekçesiyle, muhakeme hukukuna ilişkin bastırıcı ve polis hukukuna ilişkin önleyici yetkiler arasındaki sıkı ayırım artık yerinde görülmemekte ve **suçla önleyici mücadele** ve **ileride yapılacak ceza koşturması için şimdiden önlem alma** amacıyla kolluğa yetki veren yeni düzenlemelere gerek bulunduğu ileri sürülmektedir<sup>101</sup>. Hukukumuzda PVSK ek m.7 ile polise bu konuda yetki verilmeye çalışılmış ise de, hükmün uygulama koşullarının ve sınırlarının belirsiz olduğu söylenmelidir.

### **C. ORANLILIK İLKESİ VE İNTERNET İLE YAPILAN İLETİŞİMİN DENETLENMESİ**

Bir tedbire başvurulmakla elde edilmek istenen yarar ve verilmek imkan dahilinde bulunan zarar arasında makul bir oranın bulunması gerektiğini, oransızlık halinde söz konusu tedbire başvurulmamasını ifade eden ilkeye oranlılık ilkesi denir. Bu çerçevede tedbiri düzenleyen ÇASÖMK "*Başka bir tedbir ile failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesi mümkün ise, iletişimin dinlenmesine veya tespitine karar verilemez*"yeceğini belirtmek suretiyle (m.2/3) oranlılık ilkesini açık bir şekilde kabul etmiş bulunmaktadır.

Her koruma tedbiri gibi internet üzerinde yapılan haberleşmenin denetlenmesi de henüz bir yargı kararı bulunmadan önce bazı temel hak ve özgürlükleri özellikle de haberleşmenin ve özel hayatın gizliliğini ihlal etmektedir. Bu yönüyle oldukça ağır bir koruma tedbiridir. Üstelik tedbirin, tedbire maruz kalanın hiç bir haberi olmaksızın uygulanabilme olanağı, hatta zorunluluğu bu ağırlığı bir kat daha artırmaktadır. Bu çerçevede söz konusu tedbir olayın önemi, yani sanığa yüklenen fiilin ağırlığı ve o fiilden dolayı sanığa verilecek cezanın az ya da çok oluşuna göre değişebilmeli ve bununla orantılı olmalıdır. O halde isnad edilen fiil ağır değilse, bu tür bir tedbire başvurmak mümkün olmamalıdır. Zira aynı amaca daha hafif bir başka koruma tedbiri ile ulaşabilmek olanak dahilinde ise, artık daha ağır bir tedbire başvurulmamalıdır. Bu anlamda oranlılık ilkesi ikincilliği ya da ikinci derece uygulanabilirliği sonuçlamaktadır.

<sup>101</sup> Ayrıntı için bkz. **Wolter** Jürgen, Heimliche und automatisierte Informationseingriffe wider Datengrundrechtsschutz, Teil I, GA 1988, 53 vd.

Oranlılık ilkesi, uzakla haberleşmenin denetlenmesi ile bireyin özel hayatı arasındaki ilişkide, herşeyden önce çatışan bu menfaatler arasında adil bir değerler tartımını gerekli kılmaktadır. İlke, tedbire başvurulması için biçimsel ve maddi koşullar getirilmek suretiyle müdahale yetkisinin kanunla sınırlandırılmasını gerektirdiği gibi, somut olayda tedbirin gerekliliği açısından da düzeltici bir rol oynamaktadır. Bu ilke uyarınca, başka tedbirlere başvurulduğunda delilin elde edilmesi **sonuçsuz kalacak** veya en azından **önemli ölçüde güçleşecekse**, ancak bu takdirde uzakla haberleşmenin denetlenmesi mümkün olmaktadır. Bu durum, somut olayda başka tedbirlerin uygulanabilirliğine yönelik bir değerlendirme yapma zorunluluğunu da beraberinde getirmektedir<sup>102</sup>. “Son çare” (ultima ratio) olarak tedbirin gerekliliği açısından bir değerlendirme yapılmalı; bu nedenle, başka bir tedbire başvurulduğunda da olayın aydınlatılması şansının eşit olduğu durumlarda e-mail ile haberleşmenin denetlenmesi yoluna gidilmemelidir.

#### **D. İNTERNET ÜZERİNDE YAPILAN HABERLEŞMENİN DENETLENMESİNİN KOŞULLARI**

Denetim ister ÇASÖMK m.2 ve isterse m.4 çerçevesinde gerçekleşsin her iki hükmün de uygulama koşulları aynı olduğundan aşağıda birlikte incelenecektir (m.8 ÇASÖMK).

##### **1. Kişi Bakımından**

ÇASÖMK internet üzerinde yapılan haberleşmenin denetlenmesi bakımından üç kişi grubu kabul etmiştir:

- Bu kanunda öngörülen suçları işlediği kuşkusu altında bulunanlar,
- Bu kanunda öngörülen suçlara iştirak ettiği kuşkusu altına bulunanlar ve
- Bu kanunda öngörülen suçlar işlendikten sonra faillere her ne suretle olursa olsun yardım, aracılık ya da yataklık etme kuşkusu altında bulunanlar.

O halde, böyle bir tedbire maruz kalmak bakımından şüpheli olmak yeterlidir. Ancak, şüphenin ortaya çıkması bakımından belli ağırlıkta delil bulunması zorunluluğu gözden uzak tutulmamalıdır.

Görüldüğü üzere fail yanında, iştirak şekline bakılmaksızın şerikler de ÇASÖMK m.1’de belirtilen suçlar bakımından haklarında şüphe mevcutsa tedbire maruz kalabilir.

<sup>102</sup> **Lücking** Erica, Die strafprozessuale Überwachung des Fernmeldeverkehrs - Eine rechtsvergleichende Untersuchung, Freiburg 1992, s.159.

Ancak, şüpheliden başka, haberleşmenin karşı tarafında yer alan ve yine haberleşmeye aracılık yapan hakkında da tedbir uygulanabilecektir. Yine bu denetleme sırasında olayla ilgisi bulunmayan **iyiniyetli üçüncü kişilerin** de temel hak ve özgürlüklerine müdahale edilebilir.

Bu çerçevede **tanıklıktan çekinme hakkı olan kişiler** ile şüpheli ya da sanık arasındaki bu şekildeki bir haberleşmenin denetlenebilip denetlenemeyeceği tartışılabilir. Özellikle müdafî ile şüpheli arasındaki haberleşmelerin denetlenip denetlenemeyeceği son derece önemlidir. CMUK m.89 kıyasen uygulandığında bu sonucun CMUK m.47 ve 48'de düzenlenmiş bulunan tanıklıktan çekinme hakkında sahip olan diğer kişiler bakımından da geçerli olduğu söylenebilir ise de, habere aracılık eden kişiler ve haberleşme aracı sahiplerinin tanıklıktan çekinme hakkına dayanabilecekleri yönündeki bu görüş, aksi takdirde tedbir pratik olarak işlevini yitireceği için haklı olarak yerinde görülmemiştir<sup>103</sup>. Buna karşılık içinde sosyal menfaat barındıran bir kamu görevini yerine getirdikleri düşüncesiyle özel nitelikli belirli mesleki faaliyetleri yürüten kişilerle bireyler arasındaki güven ilişkisinin korunması gerektiği ve bu çerçevede özellikle **müdafî** ile sanık arasında yapılan haberleşmenin denetlenemeyeceği sonucuna varılmalıdır. Aynı sonuca "yakalanan ve tutuklu bulunan kişilerin müdafî ile yazışmaları denetime tabi tutulamaz" hükmünü getiren CMUK m.144 ile de ulaşılabacaktır. Zira buradaki yazışma tabiri içine internet üzerinde yapılan haberleşme de dahil olmalıdır. Ancak eğer müdafîin müvekkilin suçuna müdafîin müvekkilin suçuna **iştirak ettiği şüphesi varsa** bu durumda bunlar arasında yapılan haberleşmelerin denetlenebilmesi mümkün olmalıdır. Müdafî dışında meslek sırrı taşıyan avukat, mali müşavir, hekimler ve gazetecilik mesleğini yürüten kişiler gibi diğer kişiler bakımından, tedbir etkinliğini yitireceğinden bir denetleme yasağının varlığı kabul edilmemelidir. Ancak hukuk devleti açısından oldukça önemli olan bu sorun hakkında özel düzenlemenin gerekli olduğu vurgulanmalıdır.

## 2. Şüphe Bakımından

Bir ceza muhakemesi ancak şüphe üzerine başlayabilir. Ceza muhakemesi işlemlerine başvurmak bakımından ceza muhakemesinin değişik aşamalarında farklı ağırlıkta şüphe aranmaktadır. Gerçekten Ceza Muhakemesi Hukukunda şüphe, hazırlık soruşturmasının başında sadece soruşturma makamlarının delillere dayanan tahmini iken, soruşturmanın ilerleyen safhalarında iddiaya ve savunmaya ilişkin delillerin eşit değerde

<sup>103</sup> Kleinknecht/Meyer-Goßner, § 100a nr.10; Lücking, 23

görünmesi ve bu nedenle ilgililerin iddia veya savunma leyh veya aleyhinde kesin bir kaniya sahip olamamalarıdır<sup>104</sup>. Bu anlamda ceza muhakemesinde şüphe, basit şüphe ve yoğun şüphe olarak ikiye ayrılabilir<sup>105</sup>. Basit şüphe hazırlık soruşturmasına başlanmak için yeterli olan sayıca az ve/veya yetersiz bulunan delillere dayanan şüphedir. Yoğun şüphe ise, yeterli ve kuvvetli şüphe olmak üzere ikiye ayrılabilir: Buna göre sanığın mahkum olma ihtimalinin beraat etmesi ihtimalinden daha kuvvetli olduğunu ortaya koyan delillere dayanan şüphe yeterli şüphe iken, yapılacak duruşmada sanığın mahkum olması ihtimalinin kuvvetli olduğunu ortaya koyan delillere dayanan şüphe ise kuvvetli şüphedir.

**Tedbire başvurmak için** tutuklamada olduğunun aksine, soruşturmanın hali hazırdaki durumuna göre sanığın suçu işleme olasılığının yüksek olması<sup>106</sup> da gerekmemektedir. Öte yandan kamu davasının açılması için gerekli olan ve hazırlık soruşturması sonunda sanığın mahkum olmasının beraat etmesine göre daha yüksek bir olasılık oluşturması anlamında<sup>107</sup> yeterli şüphenin mevcudiyeti de aranmamaktadır. Çünkü bu şüphe derecesine ancak uzakla haberleşmenin denetlenmesinden sonra ulaşılma olasılığı vardır<sup>108</sup>.

ÇASÖMK göre, “İletişimin dinlenmesi veya tespitiyle ilişkin kararlar, ancak **kuvvetli belirtilerin varlığı halinde verilebilir**” (m.2/2). O halde, e-mail ile haberleşmenin denetlenmesi ancak kuvvetli belirtinin bulunması halinde söz konusu olabilir. Yasa koyucunun kuvvetli şüphe değil, kuvvetli belirti terimini kabul etmiş olmasının bir anlamı bulunmalıdır. Esasen tutuklama koruma tedbirini düzenleyen CMUK m.104 bu tedbirin uygulanması bakımından “kuvvetli belirti” terimini kullanmakta ve terim “kuvvetli şüphe” olarak anlaşılmaktadır. Kişi özgürlüğünü sınırlandıran böyle bir tedbir bakımından aksi de düşünülemez. Ne var ki, ÇASÖMK m.2 anlamında “kuvvetli belirti”, kuvvetli şüphe olarak anlaşılmamalıdır. Çünkü, kuvvetli şüphe, sanığın mahkum olma ihtimalinin kuvvetli olması anlamına geleceğinden ve böyle bir ihtimal de sayıca çok ya da değer olarak fazla delilin bulunmasını gerektireceğinden ya da neredeyse muhakemenin sonuna doğru oluşacağından tedbire başvurmak ile ulaşılma istenen amaç

<sup>104</sup> Karşl. Öztürk Bahri/Erdem M.Ruhan/Özbek Veli Özer, Uygulamalı Ceza Muhakemesi Hukuku, 6.Bası, Ankara 2001, no.627; Kunter Nurullah/Yenisey Feridun, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 11.Baskı, no.141.

<sup>105</sup> Öztürk/Erdem/Özbek, Ceza Muhakemesi, no.628 vd.

<sup>106</sup> Kleinknecht/Meyer-Goßner, § 112 nr.5.

<sup>107</sup> Kleinknecht/Meyer-Goßner, § 203 nr.2.

<sup>108</sup> Lücking, 18

bakımından geç kalınmış olabileceği gibi tedbire başvurmak oransız ya da gereksiz bir hale de dönüşebilir. Yasa koyucu basit şüphe ya da sadece şüphe terimini kullanmaktan da özenle kaçınmış, tedbire maruz kalanın haberinin dahi bulunmadığı ve özel hayatın gizliliğini ve haberleşme özgürlüğünü önemli ölçüde sınırlayan böyle bir tedbire kolayca başvurulmasının önüne geçmek için kuvvetli belirti terimini tercih etmiştir. **Belirti**, teknik anlamda, bir olayın dolaylı olarak ispatına yardımcı olan vakıalar veya izlerdir<sup>109</sup>. Bu anlamda bir fren izi, parmak izi vb. belirtidir ve kaslik deliller olan tanık açıklaması, yazılı belge gibi delillerden daha az önemli değildir. Belirti de bu anlamda delildir. Bu durum karşısında, yasa koyucunun burada kastettiğinin basit bir tahminden öte, yaşanmış somut olaylara dayanan şüphe olduğu kanısındayım<sup>110</sup>.

### 3. Suç Bakımından

ÇASÖMK m.2’de genel bir formül getirilmek suretiyle tedbirin, “*Bu kanunda öngörülen suçları*” işleyenlere uygulanacağı ifade edilmektedir. Ancak Kanunun hiç bir maddesinde tedbirin uygulanacağı suçlar gösterilmiş değildir. Kanun, tedbirin uygulanabileceği suçlar bakımından bir katalog öngörmek yerine, 1.m.sinde “*çıkart amaçlı suç örgütü*”nü tanımlamış ve böyle bir örgüt kurmayı, yönetmeyi, adına faaliyette bulunmayı, bilerek hizmet yüklenmeyi ve örgüte üye olmayı suç haline getirerek, cezalandırmıştır. O halde, buradaki suç, çıkart amaçlı suç örgütü oluşturmak, adına faaliyette bulunmak ve üye olmaktır<sup>111</sup>. Ancak, söz konusu suçun araç suç niteliğinde olduğu söylenmelidir. Gerçekten kanun belli amaçlara ulaşmak maksadını da öngörmek suretiyle örgütün işlemesi muhtemel amaç suçların da bulunabileceğini düzenlemiş bulunmaktadır. Elbette amaç suçlar ceza hukuku mevzuatımızda düzenlenmiş bulunan herhangi bir suç olabilir. Bu konuda yasada bir açıklık bulunmamaktadır. Böylece kanundaki tanıma uyan “çıkart amaçlı suç örgütü”nün işlemiş olduğu her suç bakımından yasada öngörülen tedbirlerin uygulanması mümkün hale gelmiştir. Ancak, kanımca, böyle bir araç suçun işlenmesi yetmez, bu suçun mutlaka 1.m.de tanımı verilmiş olan

<sup>109</sup> Öztürk/Erdem/Özbek, Ceza Muhakemesi, no.447.

<sup>110</sup> Karşl. Erdem/Özbek, Edis’e Armağan, 279.; Dönmezer, Yargı Reformu 2000, 551.

<sup>111</sup> Suçun unsurları yönünden karşl. Yenisey Feridun, Organize Suçlulukla Mücadelede Özel Ceza Muhakemesi Tedbirleri, Hukuk Kurultayı 2000, 12/16 Ocak 2000 Ankara, C.2, Ankara 2000, s.103 vd.; Dönmezer Sulhi, Çetelerle Mücadele Amacıyla 4422 Sayılı Yasayla Kabul Edilen Koruma Tedbirleri, Yargı Reformu 2000 Sempozyumu, İzmir 2000, s.547. Ayrıca organize suç kavramı hakkında Özek Çetin, Organize Suç, Kunter’e Armağan, İstanbul 1998, s.195 vd.

“çıkar amaçlı suç örgütü” tarafından işlenmesi gerekir ki, yasadaki tedbirler uygulanabilsin.

Yasanın 1.m.sindeki suçun maddi unsurunun *hareket kısmını çıkar amaçlı suç örgütü kurmak, örgütü yönetmek, örgüt adına faaliyette bulunmak, bilerek hizmet yüklenmek veya örgüte üye olmak* oluşturmaktadır. Bununla birlikte, yasa “yıldırma veya korkutma veya sindirme gücünün” ne şekilde kullanılacağını yani yöntemini de belirtmiştir. Buna göre, “yıldırma veya korkutma veya sindirme gücünü kullanarak suç işlemek”, “tehdit, baskı, cebir ve şiddet uygulamak” yöntemi kullanılmak suretiyle gerçekleştirilmelidir<sup>112</sup>. Suçun oluşması ve cezalandırılması için **neticenin** gerçekleşmesi şart değildir. Zira bu suç tehlike suçudur<sup>113</sup>.

Söz konusu suçun manevi unsuru kastın bulunmasıdır. Ancak burada yasakoyucu genel kastla yetinmemiş, özel kast aramıştır. Nitekim “... maksadıyla” demek suretiyle bunu belirtmiştir. Buna göre, çıkar amaçlı suç örgütü kurmak, örgütü yönetmek, örgüt adına faaliyette bulunmak, bilerek hizmet yüklenmek veya örgüte üye olmak suçu;

- Doğrudan veya dolaylı biçimde bir kurumun, kuruluşun veya teşebbüsün yönetim ve denetimini ele geçirmek,
- Kamu hizmetlerinde, basın ve yayın kuruluşları üzerinde, ihale, imtiyaz ve ruhsat işlemlerinde nüfuz ve denetim elde etmek,
- Ekonomik faaliyetlerde kartel ve tröst yaratmak,
- Madde ve eşyanın azalmasını ve darlığını, fiyatların düşmesini veya artmasını temin etmek,
- Kendilerine veya başkalarına haksız çıkar sağlamak,
- Seçimlerde oy elde etmek veya seçimleri engellemek

**maksadıyla** işlenmelidir<sup>114</sup>.

<sup>112</sup> 4422 sayılı ÇASÖMK 4723 sayılı Kanunla değiştirilmiş 1.m.nin 1.fikrasındaki “*zor veya tehdit*” ibaresi, “*tehdit, baskı, cebir ve şiddet*” şeklinde değiştirilmiş; aynı fıkradaki “*veya kişileri kendilerine tabi kılmaya zorlamak veya mensupları arasında her ne suretle olursa olsun açık veya gizli işbirliği yapmak*” ibaresi madde metninden çıkarılmıştır (RG).

<sup>113</sup> Bkz. dpn.70. Ayrıca karşı. Sözüer Adem, “Çıkar Amaçlı Suç Örgütü” Kavramı ve Özel Yargılama Önlemlerinin Türkiye’deki Boyutları, in: Avrupa Birliğine Uyum Süreci Bağlamında Organize Suçlulukla Mücadele, Panel 05 Ekim 2001, İstanbul 2002, s.61.

<sup>114</sup> “*Korkutma ve sindirme gücünü kullanarak ihale işlerinde çıkar sağlamak amacıyla örgütlenmek 4422 sayılı yasanın 1.m.sindeki suçu oluşturur*” (8.CD. 17.5.2001, 8873/10780; **Köroğlu** Hasan, Örgütlü Suçluluk, Ankara 2001, s.87); “*Şirket görüntüsü altında örgütlenip inşaat ihaleleri üzerinde nüfuz ve denetim elde etmek 4422 sayılı Yasanın 1.m.sindeki suçu oluşturur*” (8.CD. 22.1.2001, 23680/1432; **Köroğlu**, 89); “*Çıkar*

Öte yandan, örgüt bu amaçlara ulaşmak maksadıyla “yıldırma veya korkutma veya sindirme gücünü kullanarak **SUÇ İŞLEMEK**” amacına da sahip olmalıdır. O halde bu maksatlar yetmez, bu maksatlara ulaşmak için “suç işlemek” kastına da sahip olunmalıdır. Ancak bu suçların ne olduğu belirsizdir. Bu yönüyle kanunilik ilkesi ve onun bir sonucu olan belirlilik prensibine aykırı olduğu söylenmelidir<sup>115</sup>. Bu bağlamda suç yağma, müessir fiil, tehdit, adam öldürme vb suçlar olabilir.

Yasakoyucunun bu düzenleme tarzı haklı olarak eleştirilmektedir. Çünkü suç örgütü tanımından hareketle hakkında tedbir uygulanacak suçları önceden belirlemek mümkün değildir. Yasakoyucu çıkar amaçlı suç örgütü için belli amaçlar öngörmek suretiyle, işlenmesi muhtemel suçlar bakımından kriterler tespit etmeye çalışmıştır; ancak, bu yeterli değildir. Zaten yasada düzenlenmiş olan bir tedbire başvurmadan örgütün bu amaçlardan biriyle hareket edip etmediğini saptamak da mümkün değildir<sup>116</sup>. Mümkünse, zaten bu tedbirlere başvurulmamalıdır (m.2/3 ÇASÖMK). O halde, yapılması gereken çıkar amaçlı suç örgütünün işlemesi olası suçların kataloğunun düzenlenmesidir. Bir başka öneri de tedbirlerin ancak belli ağırlıktaki suçlar bakımından uygulanması olanağının sağlanması olabilir.

Nihayet ÇASÖMK nun 16.m.sine göre Kanununun 2 ila 10. maddeleri, Terörle Mücadele Kanunu kapsamına giren suçlarla, 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanunu, 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanun ve TCK nun 403, 404 ve 406. maddelerinde yer alan suçların **tesekkül halinde işlenmesinde** de uygulanacağını belirtmek suretiyle tedbirin uygulama alanını genişletmiş bulunmaktadır<sup>117</sup>. Bu düzenleme yasa yapma tekniğine uygun olmamıştır. Çünkü, böylece siyasi amaç güden örgütler, yani terör örgütleri bakımından da yasa uygulanır hale gelmiştir ki, madem ki böyle bir amaç güdülmekte idi, o zaman yasanın isminin “suç örgütleriyle mücadele” olması daha uygun olurdu.

*sağlamak amacıyla örgütlenip silahlı olarak yıldırma, korkutma ve sindirme gücünü kullanmak 4422 s.K. nun 1.m.sindeki suçu oluşturur” (8.CD. 18.12.200, 20133/21170; Köroğlu, 92).*

<sup>115</sup> Sözüer, 64.

<sup>116</sup> Erdem M.Ruhan, Ceza Muhakemesinde, Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri, Ankara 2001, s.314

<sup>117</sup> Karşl. Yönetmelik m.5



#### 4. Kararı Verecek Makam

Tedbire *kural olarak hakim, gecikmede sakınca bulunması halinde C.Savcısı* karar verir. İşlem derhal yapılmadığında suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması halinde gecikmede sakınca vardır (m.4 ÇASÖMK Uygulanmasına İlişkin Yönetmelik). Buradaki yetkili hakim DGM yedek hakimi, C.Savcısı ise DGM Savcısıdır (m.11 ÇASÖMK; m.4 Yönetmelik). Görüldüğü üzere, kolluğa bu konuda bir yetki verilmiş değildir. Gecikmede sakınca olsa bile, kolluk kendiliğinden bu tedbire başvuramaz. Uygulamada çoğu zaman tedbire başvurma konusundaki talep kolluktan gelmektedir. Bu durumda talep C.Savcılığı'na iletilir. Hakime gidilip, gidilmemesinde değerlendirme yapmak savcının yetki ve görevi içindedir<sup>118</sup>. Dolayısıyla, savcı gerek görmezse koluğun talebini reddedebilir. Savcı yapacağı değerlendirme sonunda iletişimin dinlenmesi ya da tesbitine gerek duyarsa hakimden bu konuda karar vermesini ister. Bununla birlikte, “gecikmede sakınca” varsa artık tedbire kendisi de karar verebilir. Ancak, tedbire C.Savcısı karar vermiş ise, 24 saat içinde hakim onayına sunulmalıdır; sürenin dolması veya hakim tarafından onay verilmemesi halinde tedbir uygulanamaz (m.2/4 ÇASÖMK). Burada başlıca iki sorun ortaya çıkacaktır: Bunlardan ilki 24 saatlik sürenin ne zaman başlayacağı, diğeri de onay verilmemesi halinde arada geçen süre içinde elde edilen verilerin delil olarak değerlendirilebilip, değerlendirilemeyeceğidir. Bunlardan ilkinde sürenin karardan itibaren başlayacağı, diğeri de bu şekilde elde edilen verilerin artık kullanılamayacağı şeklinde yanıt verilebilir. Ancak en iyisi yasada bu konuda açık bir düzenleme getirilmesidir.

#### 5. İlgiliye Haber Verme

ÇASÖMK da tedbire son verilmesi halinde hakkında tedbir uygulanan kişilere bu konuda bilgi verilmesi yükümlülüğü getiren herhangi bir düzenleme mevcut değildir. Bu durum ilgilinin söz konusu tedbiri denetleyebilme imkanını ortadan kaldırmaktadır. Zira ilgili çoğu zaman

<sup>118</sup> “İletişimin dinlenmesi veya tesbiti ile ilgili olarak hakim kararı alınıp alınmamasının değerlendirilmesi C.savcılığına ait bir yetki ve görevdir ... Yapılacak değerlendirme sonucunda (tedbire) gerek duyulduğu takdirde hakimden karar istenecektir. Aksi halde kolluk tarafından Cumhuriyet Savcılığına bu konuda yapılan başvurulardan Cumhuriyet Savcılığınca katılmayanlar da Cumhuriyet Savcılığı düşüncesi ile hakime havale edilir duruma gelinir ki yasalarımızda böyle bir usul mevcut değildir (8.CD., 21.12.2000, 27613/21500; YKD., Ağustos 2001, s.1295 vd.)

internet üzerinde yapılan haberleşmenin denetlendiğinin farkında bile olmayacaktır. Halbuki her tedbir gibi bu tedbirin de hukuka aykırı uygulanma ihtimaline karşılık ilgiliye buna karşı denetim muhakemesine başvurabilme olanağı tanınmalıydı. Bu durum hak arama özgürlüğünü düzenleyen AY m.38/4 ve İHAS ne aykırıdır.

#### ***E. TEDBİRİN SÜRESİ, SONA ERMESİ VE DÖKÜMANLARIN YOK EDİLMESİ***

ÇASÖMK e-mail ile haberleşmenin denetlenmesinin en fazla 3 ay için söz konusu olabileceğini, bu sürenin üçer aydan fazla olmamak üzere en fazla iki defa uzatılabileceğini öngörmüştür (m.2/6). O halde toplam süre en çok 9 ay olabilir. Tedbirin ağırlığı dikkate alındığında bu sürenin makul olduğu söylenebilir.

Ancak tedbire son verilmesi için mutlaka bu sürenin tamamlanmasını beklemek gerekmez. Suçun işlendiğine ilişkin şüphenin ortadan kalkması da tedbire son verilmesi için bir neden olarak karşımıza çıkar (m.2/7). Ancak, kanımca sadece yasada açıkça yer alması da tedbirin uygulanma koşullarından herhangi birinin ortadan kalkmış olması da tedbirin sona erdirilmesi için gerekir ve yeterlidir. Bunun ne zaman ortaya çıktığı konusunda ise oranlılık ilkesi her zaman yardımcı olabilecek bir kriterdir.

Yasada tedbirin sona ermesine ilişkin olarak ilginç olan tedbire karar verme yetkisinin hakimde olduğu kabul edilmiş olmasına rağmen, tedbire son verme kararının savcı tarafından veriliyor olmasıdır. Bu durum hakim tarafından verilen kararın savcı tarafından ortadan kaldırılması sonucuna yol açacağından sakıncalıdır. Tedbirin sona ermesi yönündeki karar da hakim tarafından verilmeliydi.

Tedbirin uygulanması sonucu elde edilen veriler, C.Savcısının denetimi altında yok edilir ve durum bir tutanakla belirlenir. Buna göre, veriler derhal ve nihayet 10 gün içinde yok edilir(m.2/7 ÇASÖMK). Buradaki derhal ibaresi belirsiz olmakla birlikte denetim işleminin başladığı ve bitirildiği tarih ve saat bir tutanakla saptanacağından (m.2/ son ÇASÖMK), verilerin ne zaman yok edileceği de bu tutanak esas alınarak belirlenebilir<sup>119</sup>.

<sup>119</sup> Erdem/Özbek, Edis'e Armağan, 292.

## **F. ELDE EDİLEN BİLGİLERİN DEĞERLENDİRİLMESİ**

### **1. Elde Edilen Verilerin Delil Değeri, Değerlendirme Yöntemi ve Kapsamı**

E-mail ile haberleşmenin denetlenmesinin amacı, yapılmakta olan ceza soruşturması çerçevesinde *delil araçlarının elde edilmesi* olduğu yukarıda söylenmişti. Bilindiği üzere, ceza muhakemesinde fiilin fail tarafından işlendiği veya işlenmediği hususunda yargılama makamının tam bir kanaate ulaşmasını temin yönündeki faaliyete ispat, bu faaliyette hukuk düzeninin kabul ettiği olayı temsil eden akla, maddi gerçeğe ve hukuka uygun olan vasıtalara da ispat vasıtaları, yani delil denir.<sup>120</sup> Bu yönüyle internet üzerinde yapılan haberleşme genellikle yazı, resim, şekil vb. olacağı için ispat vasıtaları bakımından yapılacak olan bir sınıflamada hangi kategori içine sokulacağı sorun teşkil edebilir. Bu sorun, özellikle, bu şekilde elde edilen verinin yazılı açıklamalar ya da belgeler içinde mi, yoksa görüntü ve ses kaydeden araçlarla yapılan tespitler içinde mi kabul edilmesi gerektiği noktasındadır. Bazı yazarlar<sup>121</sup>, ses ve/veya görüntü bantlarının aslında bir çeşit yazılı açıklama, yani belge olduğunu, bazıları<sup>122</sup> ise, bant kayıtlarının ancak keşif konusu olabileceğini, belge delilin hakime doğrudan ispat konusu vakıa hakkında kanaat verebilen deliller olması nedeniyle bant kayıtlarının belge delili olarak değerlendirilmesinin mümkün olmadığını kabul etmektedir. İnternet üzerinde yapılan haberleşmenin tespiti sonucu elde edilen verilerin tespitinin bilgisayar disketi ve CD ile yapılmakta olması, hatta gerekirse bir printer ile yazılı belge haline de dönüştürülebilmesi bunları yazılı belge durumuna sokmaz. Çünkü, söz konusu gönderinin içeriğinin değiştirilebilme ve yine göndericinin adı bulunan şahıs yerine bir başkası olma ihtimali söz konusu verinin tek başına delil olma gücünü zayıflatmakta, hatta ortadan kaldırmaktadır. Bu durumda, bu şekilde elde edilmiş olan tespitler tek başına mahkumiyet kararı verilmesi için yeterli olmayıp, bunların başka delillerle desteklenmesi gerekir<sup>123</sup>. O

<sup>120</sup> Öztürk/Erdem/Özbek, Ceza Muhakemesi, no.392, 398; Kunter/Yenisey, no.321.

<sup>121</sup> Öztürk Bahri, Ses ve/veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukundaki Değeri, Edis'e Armağan, İzmir 2000, s.226, 230; Kunter/Yenisey, no.356.

<sup>122</sup> Yurtcan Erdener, Ceza Yargılaması Hukuku, 7.Baskı, İstanbul 1998, s.302.

<sup>123</sup> Yargıtayın geçmiş dönemlerde teyp bantlarına ilişkin vermiş olduğu karar ile karşı. 9.CD 5.10.1984, 1835/2346 (Erdurak Yılmaz, Notlu-İçtihatlı Ceza Muhakemeleri usulü Kanunu, Ankara 1985, s.239) Yine karşı. Anayasa Mahkemesi'nin 19.8.1971 tarih ve kararı (RG-15 Ocak 1972).

halde, bunlar sadece ispat edilecek olayın dolaylı olarak ispatına yardımcı olan vakıa ve iz şeklinde tanımlanan<sup>124</sup> bir belirti olabilir. Disket veya CD ise keşif konusu olabilir ve çözümü özel ve teknik bir bilgiyi gerektirdiği için bu konuda bilirkişiye başvurulmalıdır (m.66/1 CMUK).

Gerçekten, internet üzerinde yapılan haberleşmenin denetlenmesi yoluyla elde edilen bilgilerin ceza muhakemesinde değerlendirilmesi, kayıtların keşif konusu olarak ele alınması, tutanakların okunması veya denetlemeyi yapan polis memurunun tanık olarak dinlenmesi suretiyle olabilir. Ancak, gerek *vasıtasızlık ilkesi* nedeniyle ve gerekse içeriğin değiştirilmesi ihtimali karşısında bu şekilde elde edilen delillere ihtiyatla yaklaşılması gerekir. Herhalukarda burada da esas itibariyle *delillerin serbestçe değerlendirilmesi* ilkesinin geçerli olduğu gözden uzak tutulmamalıdır. Ancak, bu şekilde delil olarak değerlendirilebilecek olan verilerin ÇASÖMK'ndaki koşullara, yani usulüne uygun olarak elde edilmiş olması gerekir. Aksi halde, aşağıda ele alınacağı gibi elde edilen veriler delil yasağı ile karşılaşacağından delil olarak kabul edilip, değerlendirilemez (m.254/2 CMUK).

## 2. Tesadüfen Ele Geçen Veriler

Burada ortaya çıkabilecek diğer bir sorun da *tesadüfen ele geçen verilerin* değerlendirilip değerlendirilemeyeceğidir. Gerçekten hukuka uygun bir şekilde başvuru bir tedbirde, tedbirin konusunu oluşturan suç dışında bir başka suça ilişkin veriler elde edilebilir. *Tesadüfen ele geçen şeyler* adı verilen bu tür bilgilerin değerlendirilmesi, yalnızca temel hak ve özgürlüklere müdahale alanını genişletmekle kalmadığı; aynı zamanda özel hayata yeni ve bağımsız bir müdahale olarak nitelendirildiği için<sup>125</sup>, bugün genel olarak bu tür bilgilerin değerlendirme çerçevesinin sınırlı tutulması zorunlu görülmektedir<sup>126</sup>. Almanya'da 1992 CMUK değişikliği ile, bundan böyle bu tür bilgiler bir başka ceza muhakemesinde kullanılabilir. Buna göre, sanığa veya onun suç ortağına karşı yapılan ceza koşturmasında, kararda yer verilen katalog suçundan başka bir suç hakkında bile olsa, tesadüfen ele geçen bilgiler sınırsız olarak değerlendirilebilirken, katalogda yer almayan bir suç hakkında ele geçen bu tür bilgilerden delil amacıyla yararlanılmamaktadır. Böylece değişiklikten önce, katalogda yer almayan suçlar hakkında ele geçirilen bu tür bilgilerden yararlanılmasını, şayet bu suç *katalogda*

<sup>124</sup> Öztürk/Erdem/Özbek, Ceza Muhakemesi, no.447; Kunter/Yenisey, no.357.

<sup>125</sup> BGHst 26, 298, 302

<sup>126</sup> Lücking, 36

**belirtilen suç şüphesi ile bağlantı içinde bulunuyorsa** ancak bu takdirde mümkün gören Alman Federal Mahkemesinin görüşü<sup>127</sup> yeni düzenlemede dikkate alınmamış olmaktadır. Buna karşılık sanık veya onun suç ortağı dışındaki kişilere karşı ceza koşturmasında da, elde edilmiş olan bilgiler, sanığa karşı hangi koşullar altında değerlendirilebiliyorsa, aynı çerçevede değerlendirilebilmelidir. Demek oluyor ki, katalogda yer alan herhangi bir suç hakkında ele geçirilen bilgiler üçüncü kişiler hakkında da sınırsız olarak delil amacıyla kullanılabilir. Fakat bunun için üçüncü kişiye karşı da bilginin elde edildiği anda uzakla haberleşmenin denetlenmesine ilişkin hükümler çerçevesinde işlemde bulunma olanağının mevcut olması aranmaktadır. Başka bir ifadeyle, objektif olarak katalogda yer alan bir suçun işlendiği şüphesinin mevcut olması ve elde edilmiş olan bilgilerin bununla bağlantı içerisinde bulunması zorunludur.<sup>128</sup>

Tedbiri düzenleyen ÇASÖMK’nda bu konuda bir düzenleme bulunmamaktadır. Bununla birlikte benzer soruna ilişkin bir hüküm “muvakkat zabıt” başlığını taşıyan arama koruma tedbirine ilişkin CMUK m.100 ile getirilmiş bulunmaktadır. Buna göre, *arama sonunda yapılan soruşturma ile ilgisi bulunmayan ve fakat diğer bir suçun işlendiği şüphesini uyandırabilecek olan eşya bulunursa bu eşya da muvakkaten elkonur ve durum savcılığa bildirilir.* Ancak, söz konusu hükmün internet ile yapılan haberleşmeye de kıyasen uygulanabilmesi mümkün olmamalıdır. Çünkü, kural olarak, ceza muhakemesi hukukunda kıyas serbest olmakla birlikte sınırlayıcı hükümlerde kıyas yasaktır. Yukarıda da belirtildiği üzere tesadüfen ele geçen verilerin denetlenmesi tedbirin uygulama sınırını genişleteceğinden ve bu tedbir de temel hak ve özgürlükleri sınırlandırdığından artık uygulanması için açık bir yasal düzenlemeye ihtiyaç bulunmaktadır. Şayet böyle bir düzenleme yapılacaksa önce ÇASÖMK nun uygulanacağı suçlar tek tek gösterilerek bir katalog yapılmalı ve uygulama sadece ÇASÖMK na giren suçlar bakımından mümkün olmalıdır.

### 3. Hukuka Aykırı Olarak Yapılan Denetleme

#### a) Delil Yasağı Durumu

Hukukumuzda gerek öğretide ve gerekse uygulamada CMUK m. 254/2’nin hukuka aykırı olarak elde edilen delillerin değerlendirilemeyeceği

<sup>127</sup> BGHSt 26, 298, 302; 28, 122, 125.

<sup>128</sup> BGHSt 28, 122, 129; 32, 10, 15.

yönündeki mutlak düzenlemeyi sınırlama çabalarına rağmen<sup>129</sup>, maddenin açıklığı karşısında en küçük aykırılıklar dahi delil yasağı ile karşılaşacaktır. Bununla birlikte, 1982 Anayasasının 38.m.si 3.10.2001 tarih ve 4709 sayılı Kanun ile değiştirilmiş, 6.fıkra olarak “**Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez**” hükmü eklenmiştir. Kanımca, söz konusu hüküm 254/2’yi zımnen yürürlükten kaldırmış olup, ayrıca hükmün doğrudan uygulanabilir bir hüküm olduğu da söylenmelidir. Öncelikle Anayasa CMUK m.254/2’den farklı olarak **hukuka değil, kanuna aykırılıktan** söz etmektedir. Bu durum karşısında, elde edilen delilin kanuna aykırı olarak elde edilmiş olup olmadığını belirlemek yeterlidir; ayrıca, hukuka aykırı olup olmadığını incelemenin gereği kalmamıştır. Yine Anayasa CMUK dan farklı olarak elde edilmiş **delilden değil, bulgulardan** söz etmektedir. O halde, delil yanında iz ve eser de yasak kapsamı içine sokulmuş olmaktadır. Bunun dışında, Anayasa yasak delilin **hükme esas alınmayacağını değil, delil olarak kabul edilemeyeceğini** ifade etmektedir. Bunun sonucu olarak, delilin yasak delil olup olmadığını, hakim yanında savcı ve kolluk da araştırmak zorundadır. Çünkü, bu geniş ifade karşısında kolluk delilden bir başka delile ulaşırken ya da fezleke hazırlarken, hazırlık soruşturmasından sonuç çıkarmak yetkisine sahip olan savcı da iddianame düzenlerken dayanılan delilin yasak olup olmadığını araştırmak zorundadır. Nihayet, Anayasa yasak delili elde eden soruşturma ve koğuşturma organı ile özel kişi arasında ayırım da yapmış değildir. Buna göre, ister soruşturma veya koğuşturma organı olsun isterse özel kişi olsun elde edilen delil yasak ise kullanılması mümkün değildir.

Öte yandan, *kanımca*, mağdurun rızası yani haberleşmesi denetlenen kişinin denetime razı olması denetimi hukuka aykırı olmaktan çıkarır. O halde, internet üzerinden haberleşen kişinin bu haberleşmeyi özel kişi ya da polis olabilen üçüncü bir kişinin o sırada denetlediği konusunda açık ya da örtülü onayı mevcutsa, artık aslında hukuka aykırı bu müdahale artık hukuka aykırı olmaktan çıkar<sup>130</sup>.

#### **b) Hukuka Aykırı Denetlemenin Suç Oluşturup Oluşturmadığı Sorunu**

TCK m.195 “haberleşme dokunulmazlığını ihlal” suçunu düzenlemektedir. Buna göre, “bir kimse kendisine gönderilmiş olmayan bir mektup veya telgrafi veya kapalı bir zarfi kasden açar veya başka bir şahsın posta veya telgraf ile açık muhabere varakası münderecatını anlamak için usul ve

<sup>129</sup> Bkz. Öztürk, Delil Yasakları, 40; CGK. 18.10.1993, 6-236/255; YKD. 1994, S.5, s.804.

<sup>130</sup> Karşl. BGH 42, 139, 154; 39, 335; NJW 1994, 496

nizam hilafına ele geçirecek olursa” cezalandırılır. Maddede suçun maddi konusuna giren şeyler “mektup”, “telgraf” veya “kapalı zarf” olarak belirtilmiştir. Bu durum karşısında, sayılanlar dışındaki haberleşme araçlarının bu suçun konusunu oluşturması mümkün değildir. O halde, e-mail ile yapılan haberleşmenin hukuka aykırı olarak denetlenmesi hukukumuzda suç olarak düzenlenmiş bulunmamaktadır<sup>131</sup>. Hukuka aykırı denetlemenin kolluk ya da özel kişi tarafından yapılmış olmasının da önemi bulunmamaktadır. Bu durum hukukumuz için büyük bir eksikliklerdir. Ancak, TCK Öntasarısında söz konusu fiilin suç olarak kabul edildiği söylenmelidir.

#### 4. Delil Yasaklarının Uzak Etkisi

CMUK m.254/2 karşısında delil yasaklarının uzak etkisi sorunu kesin bir çözüme kavuşturulmuştur. Yasanın bu düzenlemesi eleştirilse de<sup>132</sup>, elde edilme biçimi hukuka aykırı olan delil hukuken yok hükmündedir ve böyle bir delil de hükme esas alınmaz. Bu açıklık karşısında hukuka aykırı yolla elde edilmiş deliller yanında, bu delillere dayanılarak ortaya çıkan diğer delillerin de muhakemede kullanılması mümkün değildir. Anayasanın bu yeni düzenlemesi karşısında da bu konudaki görüşümüzde herhangi bir değişiklik olmamıştır.

#### G. E-MAİL İLE YAPILAN HABERLEŞMENİN ÖZEL KİŞİLERCE DENETLENMESİ

Doktrinde, delil değerlendirme yasağı getiren CMUK m.254/2, “**oruşturma ve koşturma organları**” tarafından hukuka aykırı şekilde elde edilen delillerin hükme esas alınamayacağından söz ettiğine göre, özel kişilerin hukuka aykırı olarak elde ettikleri delillerin değerlendirilebileceğinin kabul edilmesi gerektiği, bunun, kanunla yasaklanmayan serbest olduğunu kabul eden özgürlükçü demokrasinin bir gereği olduğu<sup>133</sup> ve yine hukuka aykırı deliller teorisinin devlet ajanları tarafından yapılan hukuka aykırılıklardan doğan devlet sorumluluğuna dayanan bir teori olduğu ileri sürülmektedir<sup>134</sup>. Kanımca, yasakoyucunun oruşturma ve koşturma

<sup>131</sup> Karşl. **Tezcan Durmuş/Erdem** M.Ruhan, teorik ve Pratik Ceza Özel Hukuku, İzmir 2000, s.105; **Artuk** M.Emin/**Gökçen** Ahmet/**Yenidünya** Caner, Ceza Hukuku Özel Hükümler, İstanbul 2000, s.265. Telefon dinleme açısından aynı yönde **Kunter/Yenisey**, no.41.5

<sup>132</sup> **Demirbaş** Timur, Sanığın Hazırlık Soruşturmasında İfadesinin Alınması, İzmir 1996, s.302 vd.; **Öztürk**, Delil Yasakları, 47 vd.

<sup>133</sup> **Öztürk/Erdem/Özbek**, Ceza Muhakemesi, no.657

<sup>134</sup> **Kunter/Yenisey**, no.41.5 ve 6.

organları için yasakladığı bir tedbiri özel kişiler için kapalı da olsa kabul ettiği söylenemez. Nitekim delil yasaklarının özel kişiler için bulunmadığını kabul eden görüş de hukuka aykırılığın ağır olması halinde söz konusu yasağın özel kişi için de geçerli olacağını kabul etmektedir. Öte yandan, özel kişiler bakımından bir kısıtlamanın bulunmamış olması polisin delil elde etme bakımından özel kişilerden yararlanmasını deyim yerindeyse bu kişilerin taşeron olarak kullanılmasını sonuçlamıştır. Nitekim, Avrupa İnsan Hakları Mahkemesi bir kararında polisin özel bir kişi ile önceden işbirliği yaparak telefon konuşmasını banda kaydetmesine yardımcı olmasını, resmi makamların özel hayata müdahalesi olarak kabul etmiştir<sup>135</sup>. Yine, delil yasaklarının özel kişiler için geçerli olmadığını söylemek, özel kişinin suç işleyerek elde etmesi ihtimali bulunan delilin de kullanılmasını sonuçlayacaktır. Bu konuda mahkemelerce verilen kararların da tutarlı olmadığı görülmektedir<sup>136</sup>.

Bu tartışmaya son vermenin en iyi yolu kanunda değişiklik yapılmak suretiyle “koğuşturma ve soruşturma organları” ibaresinin hükümden çıkarılması olacaktır. Nitekim 1982 Anayasası 38.m.si 3.10.2001 tarih ve 4709 sayılı Kanun ile değiştirilmiş 6.fıkra olarak “**Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez**” hükmü eklenmiştir. Kanımca söz konusu hüküm 254/2’yi zımnen yürürlükten kaldırmış olup, özel kişi-koğuşturma organı ayrımı da yapmamaktadır. Söz konusu hükmün doğrudan uygulanabilir bir hüküm olduğu söylenmelidir.

## SONUÇ

**1- İnternet modern toplumun en önemli kazanımlarından birisidir. Ne var ki, internetin toplum ve hukuk bakımından bazı sorunları da beraberinde getirdiği göz ardı edilemez. Bugün internet gittikçe artan oranda çocuk pornografisi, özellikle şiddet içeren suç filini övme, radikal politik ve dini görüşlerin propagandasını içeren fiillerin işlendiği bir alan haline gelmiştir. Öte yandan, bu tür suçların daha çok organize suç örgütleri tarafından işleniyor olması, konunun ciddiyetini daha da artırmaktadır. İnternetin milyonlarca kullanıcısının olduğu, bunların çoğunun kendi sayfasının bulunduğu ve her birinin kendine özgü içeriklerinin bulunduğu hatırlandığında bu fiilleri kimin işlediğini belirlemek ve özellikle ne şekilde cezalandırılacağını**

<sup>135</sup> Schenk Kararı. Div.K.A./23.11.1993, A 277, § 36 (**Gölcüklü/Gözübüyük**, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 4.Bası, Ankara 2001, s.320).

<sup>136</sup> Bkz. **Kunter/Yenisey**, no.41.



ortaya koyabilmek son derece önemlidir. Yine internet üzerinde işlenen suçların nerede işlendiği, hangi ülke kanununun uygulanacağını tespit bakımından büyük önem taşımaktadır. Nihayet, böylesine özgür bir ortamda soruşturma makamlarının nasıl ve hangi koşullar altında delil elde edebileceği de ayrı bir tartışma konusudur.

**2- Haber ve düşüncelerin internet aracılığı ile kitlelere ulaştırılması özgürlüğünü “internet özgürlüğü” olarak tanımlamak mümkündür. Bu anlamda sansür bu özgürlüğü kısıtlayacak en tehlikeli araçlardan biridir.**

**3- İletişim, düşünce ve ifade özgürlüğünün en rahat kullanıldığı ortam olduğu şüphesiz olan internetin sınırlarüstü yapısı, üstünde etkin bir yönetim ve denetim mekanizması kurulmasını en azından teknik olarak olanaksız kılmaktadır. Bilindiği üzere, sınırsız özgürlük kargaşaya ve bir süre sonra özgürlüklerin bir başka özgürlüğün kullanılması ile sınırlandırılmasına, hatta yok edilmesine yol açar. Hukukun bu anlamda özgürlüklerin hakkaniyet ve adalete uygun bir şekilde kullanılması amacıyla devreye girmesi kaçınılmaz olmaktadır. Bu anlamda, internet de “hukukun tanınmadığı” ya da “hukuk tanımayan” bir alan olarak kabul edilemez. Özellikle, özel hayatın gizliliğine internet vasıtasıyla yapılacak müdahaleler konunun önemini daha da artırmaktadır. O halde, internetin de belli kuralları ve düzeni olmalıdır. Ancak, Ceza hukuku bunu sağlamak için son çare olarak başvurulabilen bir hukuk dalı olmalıdır.**

**4- İnternetin kötüye kullanılması suretiyle işlenen suçların daha çok şu şekillerde ortaya çıktığı görülür: - Çocuk pornografisi içeren verilerin yayılması, - Aşırı sağ ya da sol grupların görüşlerinin yayınlanması, - Patlayıcı madde yapımına ilişkin bilgiler verilmesi, -Hakaret içeren verilerin yayılması, - Dolandırıcılık ve kara para aklama ya da talih oyunu düzenlenmesi gibi diğer ticari ya da ekonomik suçluluk türleri, - Bilgisayar ve müzik ürünlerinin izinsiz kullanım ve ticareti, -Uyuşturucu madde ve silah ticareti, - Politik muhaliflerin öldürülmesi gibi bazı suçların işlenmesine çağrı niteliği taşıyan verilerin yayımı. Bununla birlikte, internet suçları ikiye ayrılarak incelenebilir: İnternet aracılığı ile işlenen suçlar ve internete özgü suçlar.**

**5- İnternet suçlarının faili, internet hizmetlerinden faydalanan kullanıcılarıdır. Kullanıcı, internette sunulmuş olan hizmetleri bilgi elde etmek ya da bilgiyi ulaşılabilir kılmak amacıyla talep eden gerçek ya da tüzel kişilerdir. Bu anlamda, kullanıcı olarak internet ortamından faydalanan herkes, bu ortamda işlenebilecek suçun/suçların faili olabilir. Ancak, internet kendine özgü sühler de yaratmıştır. Web sayfasını hazırlayan ve/veya internet**

kullanıcıları için erişilebilir kılan sùjelere *internet sùjeleri* denir. internet sùjeleri üçe ayrılabilir;- içerik sağlayıcı, - erişim sağlayıcı ve - servis sağlayıcı. Ülkemizde henüz, internet sùjelerinin kim ve hukuki, idari ve cezai sorumluluklarının ne ve hangi kapsamda olduđu konusunda yasal bir düzenleme getirilmiş değildir.

**6- Mülkîlik prensibinin Türkiye Cumhuriyeti sınırları içinde işlenmiş olan her fiil bakımından Türkiye Cumhuriyeti devletinin cezalandırma yetkisinin bulunduđunu belirlemiş olması karşısında, hareketin yabancı bir ülkede yapılmış olması durumunda bazı hallerde yine de suçun Türkiye’de işlenmiş sayılması mümkün olabilecek midir? İnternet vasıtasıyla işlenen cezalandırılabilen bir hareketin dünyanın hangi yerinde yapıldığı ve nihai olarak nerede etkili olduđunun tesbit edilmesi oldukça zor bir konudur. İnternetin kendine özgü yapısı ve işleyiş tarzı bu zorluğu daha da artırmaktadır. Gerçekten, diğer iletişim araçlarından farklı olarak internet tüm dünyaya yayılmış, her yerden ulaşılabilir olup, etki gücü de radyo ve TV gibi belli bir alanla sınırlanmış değildir. Halen yürürlükte bulunan TCK’da bu konuda bir açıklık olmamakla birlikte TCK Tasarısı da karma görüşü benimsemiştir. Buna göre; 1- Hareketin kısmen veya tamamen Türkiye’de icrası ya da 2- Neticenin Türkiye’de gerçekleşmesi halinde TCK uygulanır(m.6/1). Karma teorisinin kabulü mesela, suç işlemeye tahrik, tehdit, propoganda ya da pornografik yayın gibi suçların internet üzerinde işlenmesi halinde internette yapılan ve Türk Ceza Kanununda düzenlenmiş olan tipe uygun her harekete Türk CK nu uygulanır hale getirecektir. Koğuşturma mecburiyet ilkesi geređi bu tür fiillere ilişkin başlangıç şüphesinin varlığı halinde savcı derhal hazırlık soruşturmasına başlamak zorundadır. Bu yorum tarzı, neredeyse dünyada internet vasıtasıyla işlenen her suçta Türk kanununun uygulanması sonucunu doğurur. Karma teorisinin esas alınması halinde ülkenin cezalandırma yetkisi olađanüstü genişlemekte, ülke adeta dünya jandarması haline dönüşmektedir. Bu durum, her ülke kendi yasasını uygulamak isteyeceđinden, ülkeler arası sonu gelmez yetki çatışmalarının ortaya çıkmasına neden olabilecektir.**

**7- İnternette işlenmiş olan fiillerin işlendiđi yerin tesbiti ve Türk ceza hukukunun uygulanabilirliđi bakımından aşğıdaki sonuçlara ulaşılır: - Ağ, Türkiye’den besleniyorsa, yani veri girişı Türkiye’den yapılıyor ise suç daima ülkede işlenmiş sayılır ve Türk ceza hukuku uygulanır. - Yurt dışından gönderilmiş olsa bile, hukuka aykırı içerik taşıyan bir veri Türkiye’de kurulmuş bir sunucu üzerinde dosyalanmış ise, yine yurt içinde işlenmiş olan bir suçtan söz edilir. Çünkü, fail doğrudan doğruya bu sunucu üzerinde hareket etmiştir ve bu nedenle suçun ülke içinde işlendiđi kabul edilir. - Veri**

içeriği yurt dışı kaynaklı ve veri fail tarafından yurt dışındaki bir sunucu (server) üzerinde saklanıyorsa yabancı ülkede hareket edilmiş sayılır. Bu durumda Türk ceza hukukunun geçerliliği sadece belli koşullar altında yani, özellikle fail ya da mağdurun Türk vatandaşı olması diğer bir deyişle şahsiliğin prensibi, korunma prensibi veya evrensellik prensibinin koşulları gerçekleşmiş ise kabul edilebilir. Örneğin, çocukları konu alan pornografik resimler.

**8- İletişim teknolojisinde kaydedilen olağanüstü gelişim ve bu gelişimin hızla günlük hayata ve davranış şekillerine yansımaları, ceza muhakemesinde internet üzerinde yapılan haberleşmenin denetlenmesi yoluyla delil elde edilmesi zorunluluğunu da beraberinde getirmiştir. İnternet üzerinde gerçekleştirilen haberleşme şekillerinden en yaygını e-mail olmakla birlikte, söz konusu haberleşmenin bununla sınırlı olmadığı söylenmelidir.**

**9- İnternet üzerinden yapılan haberleşmenin denetlenmesi aslında, aynı yerde bulunmayan iki kişi arasında araya telefon, teleks, faks, bilgisayar gibi bir vasıta sokularak yapılan haberleşmenin ceza koşturması amacıyla denetlenmesi olarak tanımlanabilecek olan *uzakla haberleşmenin denetlenmesinin* değişik bir görünümü olarak ortaya çıkar.**

**10- Ülkemizde uzakla haberleşmenin denetlenmesi 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2.maddesinde "*iletişimin dinlenmesi ve tesbiti*" başlığı altında düzenlenmiştir. Yasada açıkça e-mail ile yapılan haberleşmeden bahsedilmemekle birlikte, hükümde yer alan " ... *bilgisayar gibi ... elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyaller, yazılar, resimler, görüntü veya sesler ve diğer nitelikteki bilgilere*" e-mailin de dahil olduğu kabul edilmektedir. Buna karşılık mailboxı işleten sağlayıcının (sunucu) hafızasında (deposunda) "bekleyen" veri bakımından, verinin mail boxta bulunması "iletişim" ya da "uzakla haberleşme" olarak nitelenemeyeceğinden ancak aynı kanunun 4.m.sine göre "*kayıt ve verilerin incelenmesi*" söz konusu olabilir. Gerek 2 ve gerekse 4.m.ye göre yapılacak bir tespitten sonra elde edilen, örneğin, cd ya da disketin artık keşif konusu (m.78 vd. CMUK) olacağı açıktır. Bu durumda mahkeme gerekirse bilirkişiye başvurabilir.**

**11- E-mail ile iletişimin denetlenmesinin amacı yapılmakta olan ceza soruşturması çerçevesinde *delil araçlarının elde edilmesi* olmakla birlikte, söz konusu tedbire zaman zaman *önleyici amaçla* başvurulduğu da görülmektedir.**

**12- Her koruma tedbiri gibi internet üzerinde yapılan haberleşmenin denetlenmesi de henüz bir yargı kararı bulunmadan önce bazı temel hak ve özgürlükleri özellikle de haberleşmenin ve özel hayatın gizliliğini ihlal**

etmektedir. Tedbirin, ona maruz kalanın hiç bir haberi olmaksızın uygulanabilme olanağı aynı amaca daha hafif bir başka koruma tedbiri ile ulaşabilmek olanak dahilinde ise, artık bu tedbire başvurulmamasını sonuçlar.

**13- Tedbire ancak kuvvetli belirtilerin varlığı halinde başvurulabilir.** *Belirti*, teknik anlamda, bir olayın dolaylı olarak ispatına yardımcı olan vakıalar veya izlerdir. Bu anlamda bir fren izi, parmak izi vb. belirtidir ve klasik deliller olan tanık açıklaması, yazılı belge gibi delillerden daha az önemli değildir. Belirti de bu anlamda delildir. Bu durum karşısında, yasa koyucunun burada kastettiğinin basit bir tahminden öte, yaşanmış somut olaylara dayanan şüphe olduğu kanısındayım. Ancak, e-mailin denetlenmesi bakımından basit şüphenin yeterli olduğunu ileri sürebilmek için tedbire neden olan suçun niteliği ve ağırlığına bakmak gerekir.

**14- Yasakoyucunun ÇASÖMK m.1'deki düzenleme tarzı eleştirilmelidir.** Çünkü, suç örgütü tanımından hareketle hakkında tedbir uygulanacak suçları önceden belirlemek mümkün değildir. Yasakoyucu, çıkar amaçlı suç örgütü için belli amaçlar öngörmek suretiyle, işlenmesi muhtemel suçlar bakımından kriterler tespit etmeye çalışmıştır; ancak, bu yeterli değildir. Zaten yasada düzenlenmiş olan bir tedbire başvurmadan, örgütün bu amaçlardan biriyle hareket edip etmediğini saptamak da mümkün değildir. Mümkünse, zaten bu tedbirlere başvurulmamalıdır (m.2/3 ÇASÖMK). O halde, yapılması gereken çıkar amaçlı suç örgütünün işlemesi olası suçların kataloğunun düzenlenmesidir. Bir başka öneri de, tedbirlerin ancak belli ağırlıktaki suçlar bakımından uygulanması olanağının sağlanması olabilir. ÇASÖMK nun 16.m.si siyasi amaç güden örgütler, yani terör örgütleri bakımından da yasadaki tedbirleri uygulanır hale getirmiştir. Madem ki, böyle bir amaç güdülmekte idi, o zaman yasanın isminin "**Suç Örgütleriyle Mücadele Kanunu**" olması daha uygun olurdu.

**15- ÇASÖMK'nda tedbire son verilmesi halinde hakkında tedbir uygulanan kişilere bu konuda bilgi verilmesi yükümlülüğü getiren herhangi bir düzenleme mevcut değildir.** Bu durum, ilgilinin söz konusu tedbiri denetleyebilme imkanını ortadan kaldırmaktadır.

**16- Tedbire karar verme yetkisi hakimde olmakla birlikte, tedbire son verme kararının savcı tarafından veriliyor olması hakim tarafından verilen kararın savcı tarafından ortadan kaldırılması sonucuna yol açacağından sakıncalıdır.** Tedbirin sona ermesi yönündeki karar da hakim tarafından verilmeliydi.

17- E-mail ile yapılan haberleşmenin denetlenmesi sonucu elde edilen verinin yazılı açıklamalar ya da belgeler içinde mi, yoksa görüntü ve ses kaydeden araçlarla yapılan tespitler içinde mi kabul edilmesi gerektiği önemlidir. Kanımca, internet üzerinde yapılan haberleşmenin tespiti sonucu elde edilen verilerin tespitinin bilgisayar disketi ve CD ile yapılmakta olması, hatta gerekirse bir printer ile yazılı belge haline de dönüştürülebilmesi bunları yazılı belge durumuna sokmaz. Çünkü, söz konusu gönderinin içeriğinin değiştirilebilme ve yine göndericinin adı bulunan şahıs yerine bir başkası olma ihtimali söz konusu verinin tek başına delil olma gücünü zayıflatmakta, hatta ortadan kaldırmaktadır. Bu durumda, bu şekilde elde edilmiş olan tespitler tek başına mahkumiyet kararı verilmesi için yeterli olmayıp, bunların başka delillerle desteklenmesi gerekir. O halde, bunlar sadece ispat edilecek olayın dolaylı olarak ispatına yardımcı olan vakıa ve iz şeklinde tanımlanan bir *belirti* olabilir. Disket veya CD ise keşif konusu olabilir ve çözümü özel ve teknik bir bilgiyi gerektirdiği için bu konuda bilirkişiye başvurulmalıdır (m.66/1 CMUK).

18- *Tesadüfen ele geçen verilerin* değerlendirilip değerlendirilemeyeceği konusunda tedbiri düzenleyen ÇASÖMK'nda bir düzenleme bulunmamaktadır. Bununla birlikte, benzer soruna ilişkin bir hüküm "muvakkat zabıt" başlığını taşıyan arama koruma tedbirine ilişkin CMUK m.100 ile getirilmiş bulunmaktadır. Buna göre, *arama sonunda yapılan soruşturma ile ilgisi bulunmayan ve fakat diğer bir suçun işlendiği şüphesini uyandırabilecek olan eşya bulunursa bu eşya da muvakkaten elkonur ve durum savcılığa bildirilir.* Ancak, söz konusu hükmün internet ile yapılan haberleşmeye de kıyasen uygulanabilmesi mümkün olmamalıdır. Çünkü, kural olarak, ceza muhakemesi hukukunda kıyas serbest olmakla birlikte sınırlayıcı hükümlerde kıyas yasaktır.

19- CMUK m. 254/2'nin hukuka aykırı olarak elde edilen delillerin değerlendirilemeyeceği yönündeki mutlak düzenlemeyi sınırlama çabalarına rağmen, maddenin açıklığı karşısında en küçük aykırılıklar dahi delil yasağı ile karşılaşacaktır. Bununla birlikte, 1982 Anayasasının 38.m.si 3.10.2001 tarih ve 4709 sayılı Kanun ile değiştirilmiş, 6.fıkra olarak "*Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez*" hükmü eklenmiştir. Kanımca, söz konusu hüküm 254/2'yi zımnen yürürlükten kaldırmıştır. Yasakoyucu henüz bu konuda CMUK'da yeni bir düzenleme yapmış değildir. Ancak, hükmün doğrudan uygulanabilir bir hüküm olduğu söylenmelidir. Öte yandan, mağdurun rızası yani haberleşmesi denetlenen kişinin denetime razı olması denetimi hukuka aykırı olmaktan çıkarır. O halde, internet üzerinden haberleşen kişinin bu haberleşmeyi özel kişi ya da polis olabilen üçüncü bir

kişinin o sırada denetlediği konusunda açık ya da örtülü onayı mevcutsa, aslında hukuka aykırı bu müdahale artık hukuka aykırı olmaktan çıkar.

**20- ÇASÖMK m.2 ve 4** e-maillerin denetlenmesi bakımından yeterli değildir. Çünkü bu denetim sadece bu kanun kapsamına giren suçlar bakımından gerçekleştirilebilir. Halbuki, çoğu zaman e-mailin kontrolünü gerektiren fiiller bu kanun kapsamına girmez. Bu nedenle CMUK içinde bir hükme ihtiyaç vardır.

**KAYNAKÇA**

- Artuk M.Emin /Gökçen Ahmet /Yenidünya Caner**, Ceza Hukuku Genel Hükümler I, Ankara 2002.
- Artuk M.Emin/Gökçen Ahmet/Yenidünya Caner**, Ceza Hukuku Özel Hükümler, İstanbul 2000.
- Atabek Ümit**, İnternet ve Sosyal Bilimlerde Metodoloji, Amme İdaresi Dergisi, C.34, S. Mart 2001.
- Bär Wolfgang**, EDV-Beweissicherung im Strafverfahrensrecht, CR 1998/7.
- Bär Wolfgang**, Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation, MMR 8/2000.
- Bär Wolfgang**, Polizeilicher Zugriff auf kriminelle Mailboxen, CR 1995.
- Bär Wolfgang**, Anmerkung zum Beschluß des BGH vom 31.07.1995, CR 1996.
- Bär Wolfgang**, in: Wabnitz/Janovsky, Handbuch der Wirtschaftskriminalität,
- Beisel Daniel/Heinrich Bernd**, Die Strafbarkeit der Ausstrahlung pornografischer Sendungen in codierter Form durch das Fernsehen, JR 1996.
- Breuer Barbara**, Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer, MMR 1998.
- Collardin Markus**, Straftaten im Internet, CR 1995.
- Conradi Ulrich/Schlömer Uwe**, Die Strafbarkeit der Internet-Providern, NStZ 1996.
- Cornils Karin**, Der Begehungsort von Äußerungsdelikten im Internet, JZ 1999
- Demirbaş Timur**, Sanığın Hazırlık Soruşturmasında İfadesinin Alınması, İzmir 1996.
- Derksen Roland**, Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem Inhalt, NJW 1997.
- Dinç Güney**, Bilgisayar Çağında Özel Yaşamın Korunması, Ank.BD., S.1987/2.
- Dönmezer Sulhi**, Kişilere ve Mala Karşı Cürümler, 16.Bası, İstanbul 2001.
- Dönmezer Sulhi/Erman Sahir**, Nazari ve Tatbiki Ceza Hukuku, 11.Bası İstanbul
- Dönmezer Sulhi**, Çetelerle Mücadele Amacıyla 4422 Sayılı Yasayla Kabul Edilen Koruma Tedbirleri, Yargı Reformu 2000 Sempozyumu, İzmir 2000.
- Engel Christoph**, Inhaltskontrolle im Internet, AfP 3/1996.
- Erdem M.Ruhan**, Ceza Muhakemesinde, Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri, Ankara 2001.
- Erdem M.Ruhan/Özbek,V.Özer**, 4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu Çerçevesinde Uzakla Haberleşmenin Denetlenmesi, Edis'e Aramağan, İzmir 2000.
- Erdurak Yılmaz**, Notlu-İçtihatlı Ceza Muhakemeleri usulü Kanunu, Ankara 1985.

- Erman Sahir/Özek Çetin**, Açıklamalı Basın Kanunu ve İlgili Mevzuat, İstanbul 2000.
- Ersoy Yüksel**, Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, AÜSBFD. 1994, C.49, S.3-4.
- Finke Thorsten**, Die strafrechtliche Verantwortung von Internet-Providern, Tübingen 1998.
- Flehsig Norbert P./Gabel Detlev**, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, CR 1998/6.
- Gercke Marco**, Rechtswidrige Inhalte im Internet, Diss., Köln 2000.
- Gökçen Ahmet**, Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma, Ankara 1994.
- Gölcüklü/Gözübüyük**, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 4.Bası, Ankara 2001.
- Gözübüyük A.Pulat**, Türk Ceza Kanunu Açıklaması, C.I, 4.Bası, İstanbul 1980.
- Güran Sait/Akünel Teoman/Bayraktar Köksal/Yurtcan Erdener/Kendigelen Abuzer/Beller Önder/Sözer Bülent**, İnternet ve Hukuk Temel Metni, İstanbul 2000.
- Haft Fritjof/Eisele Jörg**, Zur Einführung: Rechtsfragen des Datenverkehrs im Internet, JuS 2001.
- Hegmanns Michael**, Strafrechtliche Verantwortlichkeit für illegale Inhalte im Internet, JA 2001, s. 71 vd.
- Heinrich Bernd**, Der Erfolgsort beim abstrakten Gefährdungsdelikt, GA 1999.
- Hilgendorf Eric**, Die Neuen Medien und das Strafrecht, ZStW 113 (2001).
- Hilgendorf Eric**, Überlegungen zur strafrechtlichen Interpretation des Ubiquitaetsprinzips im Zeitalter des Internet, NJW 1997.
- Hoeren Thomas/Sieber Ulrich**, Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, München 1999.
- Hoeren Thomas**, Rechtsfragen des Internet, Köln 1998.
- İçel Kayıhan**, Kitle Haberleşme Hukuku, 4.Baskı, İstanbul 1998.
- İçel Kayıhan**, Haberleşme Özgürlüğü, İHFM, C.XLI, S.1-2 den ayrı bası, İstanbul 1975.
- İçel Kayıhan/Donay Süheyl**, Karşılaştırmalı ve Uygulamalı Ceza Hukuku, Genel Kısım, 1.Kitap, 3.Bası, İstanbul 1999.
- İlkiz Fikret**, İnternet Ortamındaki Yayınlarda İki Olay ve İki Mahkumiyet Kararı ve Yasal Çalışmalar, İst.BD. 2001, S.10-11-12.
- İnanıcı Haluk**, Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü, İst.BD., 1996, C.70.
- Koroğlu Hasan**, Örgütlü Suçluluk, Ankara 2001.
- Löwe-Rosenberg**, StPO Grosskommentar, 24.Aufl.,Berlin Newyork 1986.



- Kienle**, Internationale Strafrecht und Straftaten im Internet 1998.
- Kleinknecht/Meyer-Goßner**, Strafprozessordnung, Mit GVG und Nebengesetzen, 44. Aufl., München 1999.
- Kuner** Christopher, Internationale Zuständigkeitskonflikte im Internet, CR 1996.
- Kunter** Nurullah, Suçun Maddi Unsurları Nazariyesi, İstanbul 1954.
- Kunter** Nurullah/**Yenisey** Feridun, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 11.Baskı
- Lackner** Karl/**Kühl** Kristian, Strafgesetzbuch, 23.Aufl., München 1999.
- Lücking** Erica, Die strafprozessuale Überwachung des Fernmeldeverkehrs -Eine rechtsvergleichende Untersuchung, Freiburg 1992.
- Martin** Jörg, Grenzüberschreitende Umweltbeeinträchtigungen im deutschen Strafrecht, ZRP 1992.
- Nack** Armin, Strafprozessordnung, Gerichtsverfassungsgesetz, in: Karlsruher Kommentar, 4.Aufl., München 1999.
- Önder** Ayhan, Ceza Hukuku Genel Hükümler, C.I, İstanbul 1991.
- Önder** Ayhan, Suçun İşlendiği Yer, AD., S.1-2.
- Önder** Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul 1994.
- Özbek** Veli Özer, Radyo-Televizyon Özgürlüğü ve Özel Radyo Televizyonlar, İzBD 1994, S.1.
- Özbek** Veli Özer, Ceza Muhakemesi Hukukunda Bir Koruma Tedbiri Olarak Arama, Ankara 1999.
- Özek** Çetin, Organize Suç, Kunter'e Armağan, İstanbul 1998.
- Öztürk** Bahri, Ses ve/veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukundaki Değeri, Edis'e Armağan, İzmir 2000.
- Öztürk** Bahri, Yeni Yargıtay Kararları Işığında Delil Yasakları, Ankara 1995.
- Öztürk** Bahri/**Erdem** Mustafa R./**Özbek** Veli Özer, Uygulamalı Ceza Hukuku ve Emniyet Tedbirleri Hukuku, 5.Baskı, Ankara 2001.
- Öztürk** Bahri/**Erdem** M.Ruhan/**Özbek** Veli Özer, Uygulamalı Ceza Muhakemesi Hukuku, 6.Bası, Ankara 2001.
- Palm** Franz/**Roy** Rudolf, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996.
- Palm** Franz/**Roy** Rudolf, Der BGH und der Zugriff auf Mailboxen, NJW 1997.
- Park** Tido, Die Strafbarkeit von Internet-Providern wegen rechtswidriger Internet-Inhalte, GA 2001/1.
- Pfeiffer** Gerd, StPO, Strafprozessordnung, 3.Aufl., München 2001.

- Ringel** Kurt, Rechtsextremistische Propaganda aus dem Ausland im Internet, CR 5/1997.
- Roxin** Claus, Strafverfahrensrecht, 25. Aufl., München 1998.
- Schönke** Adolf/**Schröder** Horst, Strafgesetzbuch - Kommentar, 25. Aufl., München 1997.
- Sınar** Hasan, İnternet ve Ceza Hukuku, İstanbul 2001.
- Sınar** Hasan, İnternet'in Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı, Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni (MHB), Yıl.17-18, S.1-2, 1997-1998, Yılmaz Altuğ'a Armağan, İstanbul 2000.
- Sieber** Ulrich, Strafrechtliche Verantwortung für den Datenverkehr in internationalen Computernetzen, JZ 1996.
- Sieber** Ulrich, Internationales Strafrecht im Internet, NJW 1999, s.2065.
- Sözüer** Adem, "Çıkar Amaçlı Suç Örgütü" Kavramı ve Özel Yargılama Önlemlerinin Türkiye'deki Boyutları, in: Avrupa Birliğine Uyum Süreci Bağlamında Organize Suçlulukla Mücadele, Panel 05 Ekim 2001, İstanbul 2002.
- Taner** Tahir, Ceza Muhakemesi Usulü, İstanbul 1950.
- Tezcan** Durmuş/**Erdem** M. Ruhan, Teorik ve Pratik Ceza Özel Hukuku, İzmir 2000.
- Tröndle**, Herbert/**Fischer** Thomas, Strafgesetzbuch und Nebengesetze, 49.Aufl., München 1999.
- Tiedeman** Klaus, Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi, çev. Feridun Yenisey, İÜHFM. 1975, C.XLI, S.1-2.
- Yazıcıoğlu** Yılmaz, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları İle, İstanbul 1997.
- Yenisey** Feridun, Organize Suçlulukla Mücadelede Özel Ceza Muhakemesi Tedbirleri, Hukuk Kurultayı 2000, 12/16 Ocak 2000 Ankara, C.2, Ankara 2000.
- Yurtcan** Erdener, Ceza Yargılaması Hukuku, 7.Baskı, İstanbul 1998
- Wolter** Jürgen, Heimliche und automatisierte Informationseingriffe wider Datengrundrechtsschutz, Teil I, GA 1988.
- Zöllner** Mark Alexander, Verdachtlose Recherchen und Ermittlungen im Internet, GA 12/2000.