İNTERNETTE GÜVENLİK ve DENETİM: MASUMİYET YİTİRİLİYOR MU?

Yrd.Doç.Dr.İsmail Güneş
Çukurova Üniversitesi İİBF
Maliye Bölümü

Berfu Salıcı
Avukat
Ç.Ü. Sos.Bil.Enstitüsü
Maliye Anabilim Dalı Öğrencisi

GİRİŞ

Ondokuzuncu yüzyılın ilk yarısında telgrafın,ikinci yarısında telefonun,yirminci yüzyıl başında ise telsiz iletişiminin keşfedilmesi insanlar,ekonomiler ve devletler arasındaki uzaklıkların ortadan kalkmasında en önemli dönemeçler olarak vurgulanmışlardır (Özdemir,2001). 20. yüzyıl boyunca gelişmeler devam etmiş,iletişim radyo ve televizyondan sonra bilgisayar teknolojisiyle buluşmuş ve bu da gelişme hızının katlanarak artmasına yol açmıştır.

İlk olarak ABD'de askeri amaçlı bir proje olarak ortaya çıkan ve birden fazla haberleşme ağının (network),birlikte meydana getirdikleri bir iletişim ortamını temsil eden İnternet,ABD Yüksek Mahkemesi tarafından bir kararında şöyle tanımlanmıştır."İnternet birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslar arası ağdır....İnternet,bireylerin dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortamdır...." (Beceni,2001)

Bu tanımdan da açıkça görüleceği üzere,İnternet iletişim alanında bu güne değin ulaşılan en son ve en farklı kavramı temsil etmektedir. Çalışmamızın amacı; işte bu tanımdan yola çıkarak "tamamen yeni ve benzeri olmayan bir ortamdır" ifadesinin gerçekliğinin, birey ve devleti nasıl bir ilişkiye soktuğunu ve bu ilişkinin beraberinde getirdiği veya getirmeye zorunlu olduğu düzenlemelere ,bazı kavramlarla değinmek olacaktır.

Bu bağlamda yakın zamanda gündemimizde ilk sırayı alan ve tarihe damgasını "11 Eylül Saldırıları" olarak vuran terörist eylemlerde, iletişimin olumlu olumsuz yanları İnternet penceresinden ele alınacak ve İnternette denetimin var olup olmamasının gerekleri,uluslar arası örnek kurumlar,olası bir durumda kim tarafından,hangi hukuksal dayanaklarla yapılabileceği yine Türkiye'den de somut örneklerle tartışmaya açılırken,ülkemizde hukuki

güvenceden yoksun bu kavramın, nasıl da *ehli keyif* şekilde ele alındığına dikkat çekilmeye çalışılacaktır.

Bu arada hemen belirtmemiz gerekir ki,çalışmamızda teknik ve işlevsel özelliklere zorunlu kalmadıkça değinmek yerine,artık bazı yazarlarca da ,sanayi devriminden sonra "bilgi toplumuna" geçişimizin ,enformasyon devriminin en büyük işareti sayılan Internet'in sosyal yönü ele alınmaya çalışılmıştır. Zira teknik ve işlevsel yönü geniş bir bilgi birikimi gerektirip, apayrı bir çalışmanın konusunu oluşturabilecektir.

I. INTERNET'İN DENETİMİ

1.1)YİTİRİLEN MASUMİYET

Dünya Ticaret Merkezi ve Pentagon'a yapılan 11 Eylül saldırılarının ardından,sadece konuyla ilgili uzmanlar tarafından bilinen ,Amerika'nın birçok sırrı kamuoyu gündemine gelmeye başlamıştır. Bu sırlar beraberinde, gerek bireyler gerek sivil örgütler için bir kaos oluşturmuş, Internet'in saldırılarda teröristler tarafından iletişim amaçlı olarak kullanıldığının da açıklanması üzerine, Internet'in bilinen fakat çok yoğun tartışılmayan masum olmayan yönleri gündeme gelmiş ve yoğun olarak tartışılmaya başlanmıştır. Bu bağlamda etkin denetim yolları aranmaya başlanmıştır. Ve Patriot Yasası olarak adlandırılan "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" özgürlüklerin koruyucusu,denetim karşıtı ABD'de ,26 Ekim 2001'de, Başkan Bush tarafından ,bir takım özgürlükleri kısıtlamak ve teknolojik denetimi etkinleştirmek için imzalanmıştır (Ucla Üniversitesi, 2001).

11 Eylülün planlanmasından uygulanmasına kadar geçen aşamalarda ileri teknolojik olanakların kullanıldığı görülmektedir. Bu eylem sürecinde Dünya Ticaret Merkezi, Amerikan Havayolları ve Pentagonûn bilgi/yönetim organizasyonunu sağlayan bilgisayar sistemlerine sızılma olasılığı göz ardı edilmemelidir. Amerikan istihbarat birimleri saldırganların e-mail ve benzeri iletişimlerinde gelişmiş şifreleme yöntemleri kullandıklarını açıklamaktadır. Elektronik ortamda gelişmiş stenografi (gizli yazı) teknolojisi son derece popüler olmaya başlamıştır. Geleneksel olarak şifrelenmiş yazılar kolayca fark edilirken ,

stenografi, iletilecek mesajı ses veya resim dosyalarının içine saklayarak tespitini güçleştirmektedir. (Büke, 2002) Örneğin Adana'dan kalkan bir uçağın kaçta Paris'te olacağı ile ilgili bir mesaj Çukurova üniversitesinin göl manzaralı bir fotoğrafının içerisine yerleştirilerek gönderilebilmektedir.

Tüm bu yaşanan somut kaygılar;soyut olarak yaratılması gereken bir denetimin varolması gerektiği üzerinde,zaten süren tartışmaların ,yoğunlaşmasına neden olmuştur. Özgürlük alanı bu kadar geniş olan İnternette,varolan tek iktidarın klavye karşısındaki birey olduğu düşünülecek olursa ,İngiliz filozof Lord Acton'un "iktidar yozlaşır ,mutlak iktidar mutlaka yozlaşır" sözünden de yola çıkarak, İnternette bir denetim ve kontrol mekanizmasına ihtiyaç olduğu varsayımıyla hareket edilebilecektir.

1.2)DENETİM: HANGİ SUÇLAR İÇİN?

İnternette yapılacak denetim için klasik suçlar ve bilişim suçları ayırımı mutlaka yapılması gerekmektedir. Örneğin hakaret,sövme,bayrağa hakaret,çocuk Pornosu klasik suçlardır ve bireysel özgürlük kılıfı altında ,bu fiillerin İnternet kanalıyla korunması savunulabilecek bir seçim olmayacaktır. Klasik suçlarda tartışılması gereken ;yazıyı yazan kişi ile birlikte İnternet servis sağlayıcılarının da sorumlu olup olmayacağı konusudur (Yazıcıoğlu,2001).

Ancak asıl problem; gerek bireysel kullanıcı gerek hükümetler tarafından gerçekleştirilen ve bilgisayardaki verilere girmek gibi özel bilişim suçlarını temsil eden suç tipleridir. Bu suçlar, suç terminolojisine ,hayatımıza İnternet kavramının girmesiyle beraber kazandırılmışlardır. Bilişim suçlarının gerçekleşen bir çok somut olayda mahremiyet,iletişim özgürlüğü,bireysel gizlilik kavramları gibi hakları koruma altına alan, uluslararası birçok bildiri ve yasayı hiçe saydığına inanmak ,varolan uluslararası hukuk düzeniyle uyuşmaktadır.

Sonuç olarak klasik suçlar ile benzerlik göstermeyen ihlaller ve muhtemel yeni ihlal biçimleri hakkında ,bu ihlallerin tanımlanması ve bunlara ilişkin ceza sorumluluğu kurallarının belirlenmesi konusunda yeni düzenlemelerin yapılması gerektiği kanaatindeyiz. Eğer gerçek dünyada işlenen klasik suçlar ile sanal dünyada işlenen özel bilişim suçları

arasında yapısal olarak bir faklılık çıkmıyorsa , klasik suçlara ilişkin normun ,söz konusu siber-suça da uygulanması mümkün olabilecektir. Temel kriter alınması gereken İnternet aracılığıyla gerçekleştirilen eylemler ve İnternete özgü eylemlerin farklılığı olmalıdır (Sınar,70-77).

BİLİŞİM SUÇLARI

Teknoloji bir yandan hayatımıza yeni bir yaşam tarzı getirirken diğer yandan yeni suç şekilleri yaşamımıza girmeye başlamıştır. Bilişim suçlarıyla ilgili olarak karşımıza pek çok tanım çıkmaktadır. Bilgisayar suçları, digital suçlar, internet suçları, siber suçlar, ileri teknoloji suçları, ağ suçları gibi yeni terimler kullanılmaya başlanmıştır.

Bu suç türleri bilgisayar aracılığıyla yapılacağı gibi bir ağ veya internet üzerinden de olabilmekte küçük bir elektrik devresi veya kredi kartı da kullanılabilmektedir. Bilişim kelimesi bilgisayar, bilgisayar teknolojileri ve iletişim teknolojilerini kapsadığından ‘’bu ortamda gerçekleşen ve değişik şekillerde adlandırılan bu suç türlerinin ‘’Bilişim Suçları ‘’olarak adlandırılması daha uygun olacaktır (Yılmaz, 2002).

Teknolojik gelişim ve karmaşıklaşan dünya sisteminde bilginin değerinin arttırdığını görüyoruz. Ülkeler bilgi tabanlı işlemcileri, bilgi sistemlerini ve bilgisayar tabanlı ağ sistemlerini etkileyecek çalışmalar yaparak, bilgi savaşında kendilerini avantajlı konuma getirecek gelişimler peşindeler. Her türlü üretimin önünde yer alan bilgi üretimi, her ülke için en stratejik sektör olma özelliği taşımaktadır. Piyasaya yeni çıkacak bir araba, üretilen yeni bir buğday tohumu veya hazırlanan bir verimlilik raporu "karşı taraf" için yoğun bir bombardımandan daha kötü sonuçlar doğurabilir. Hatta o bilginin diğer karşı tarafın eline geçmesi ise daha büyük bir etki yapabilir.Bu nedenle Bond filmlerinde izlediğimiz sokak aralarındaki kovalamacalar, artık sibernetik ortamda, Internet’te yaşanmaktadır. Belki de bir süre sonra savaşlar, klasik mühimmat ve düzenli veya düzensiz birliklerle dağlarda veya ovalarda değil, telefon hatları üzerinde internet gezegeninde yaşanabilecektir.İnternet dünyasında siteleri çökerten, bilgisayarları boşaltan virüs, worm ve tanımadığımız daha bir çok siber silah bunun için gereken altyapıyı hazırlamıştır. Bir yandan vergi borcuna kızıp, vergi dairesinin sitesini çökertenler olurken diğer yandan FBI ve Pentagon'un da sitelerinin

çökertildiğini görebiliyoruz.. Site kuran terör örgütleri karşısında o siteleri çökertmeye çalışan istihbarat örgütleri görülüyor. Porno sitelerinin chat odalarında örgütlenen teröristleri , internette miting yapan neo-naziler görülüyor. (Diplomatik Gözlem Gazetesi,26.01.2003) http://diplomatikgozlem.com/turkish/terorizm/20020430_02.html)

Bilişim suçlarını örneklendirmek istersek:

1-Bilgisayar Sistemlerine ve servislerine yetkisiz erişim ve Bilgisayarların sabote edilmesi: Anayasamızda da 'Özel Hayatın Gizliliği' başlığı altında ele alınan duruma aykırı olarak yasal olmayan yollardan kişilerin izlenmesi, dinlenmesi, yazışmalarının takibi gibi durumlar günümüz teknolojisi ile mümkün duruma gelmiştir.Bu bağlamda echelon sistemi ilerleyen bölümlerde daha ayrıntılı olarak ele alınacaktır. Bunun yanı sıra kamu ve özel sektör bilgisayarlarına izinsiz erişim ve web sitelerinin hack edilmesi gibi eylemlerde son yıllarda gözle görülür artışlar ortaya çıkmıştır.

2-Bilgisayar yoluyla Dolandırıcılık ve Sahtecilik: Uyuşturucu ticareti, kara para aklama, çocuk pornografisi, yasadışı silah ticareti, kumar, fuhuş alanlarında organize suç örgütleri bilişim teknolojilerini yoğun olarak kullanmaktadır. Şifreleme teknikleriyle desteklenen eylemlerin takibi çoğu kez zorlaşmaktadır. Yine bu organize suç örgütleri dijital teknoloji araçlarını kullanarak kalpazanlık, kimlik, resmi belge, pasaport gibi önemli belgelerin sahtesini üretebilmektedir. Bir diğer dolandırıcılık yöntemi olarak elektronik postalar karşımıza çıkmaktadır. ABD'deki Tüketici Birliğine göre elektronik posta ile yapılan dolandırıcılığa yönelik en sık görülen 10 sahte e-posta arasında en hızlı yayılan spam, 'Nijerya mesajı'. NCL'nin yayınladığı listede en hızlı artışı gösteren internet dolandırıcılığı, ünlü 'Nijerya para teklifi'nin online versiyonu. Gönderildiği kişilerden, paralarını katlama vaadiyle banka hesaplarının ayrıntısını isteyen bu mesaj, 2000-2001 yılları arasında tam yüzde 900'lük bir artış göstermiştir.İlk 10 online dolandırıcılık ise şöyle sıralanmaktadır.

•sahte online müzeler

• İnternetten alınan genel amaçlı malların kasıtlı olarak yanlış tanıtılması ya da satın alana gönderilmemesi.

•Parayı katlamayı vadeden Nijerya mesajı

• İnternetten alınan bilgisayar donanım-yazılımının kasıtlı olarak yanlış tanıtımı ya da

dağıtımının yapılmaması.

• İnternet servis sağlayıcıların talep edilmeyen ya da kullanılmayan servisler için para istemesi.

• Kullanılmayan ya da yanlış tanıtımı yapılan bilgi/adult servisleri için kredi kartından para çekilmesi.

•Yüksek kar ve maaş vaat eden 'evde çalışın' projeleri.

• Tüketicilerden belirli bir miktarda para talep edilen, ön ödemeli 'cazip' kredi teklifleri.

•Düşük faiz oranlı sahte kredi kartı teklifleri.

• Aşırı derecede abartılı kar vadeden iş fırsatları ve franchise olanakları (Dikey 8:2001)

Değişimden payını mafya örgütlenmesi de alıyor. Mafyanın bilgisayar uzmanlarına yüksek paralar teklif etmesi ve kabul edilmemesi durumunda kaçırmaları artık sıkça görülen bir olay haline gelmeye başlıyor. Bugün pek çok sitede ortadan kaybolmuş bilgisayar uzmanları ile ilgili ilanlar bulunuyor. Elektronik ticaretin gelişmesiyle kara para aklama konusunda mafyaya geniş bir hareket alanı sağlanmışta oldu. Diğer yandan özellikle Rus mafyası ve banka soygunları artık kitaplara ve filmlere konu olmaya başlıyor. Bunların en ünlüsü olan Vlademir Levin, Rus mafyası tarafından kaçırıldıktan sonra Citibank'ın dünyanın pek çok yerindeki şubelerini soyarak kimilerine göre 10 kimilerine göre 17 milyon dolarlık bir soygun gerçekleştirdi. Leningrad Mafyasının üyeleri yakalanamazken hacker Vlademir Levin halen Londra'da tutuklu bulunmaktadır.(Radikal, 03/03/1999)

3.Fikir ve Sanat Eserlerini izinsiz kullanımı: (İzinsiz Yazılım kullanımı): Yaşanan teknolojik gelişimlerle beraber internet alanında hukuksal bazı düzenlemelerin gerekliliği ortaya çıkmıştır. Fikir ve Sanat Eserlerini izinsiz kullanımı İnternette en çok rastlanan durumundur. Bilimsel ve edebi eserlerin izinsiz yayımı ve dağıtımı, bilgisayar programları, bilimsel ve teknik nitelikteki fotoğraflar, haritalar, planlar, projeler, krokiler, resimler, maketler, mimarlık ve şehircilik tasarımları, sahne tasarımları bu kategoride sayılabilir. İkinci olarak Müzik eserlerin yasaya aykırı yayın ve dağıtımı sorunu gündeme gelmektedir. Güzel Sanat eserleri ve Sinema eserleri de sıkça internet üzerinde yasa dışı olarak dağıtımı yapılabilen ürünler olarak karşımıza çıkmaktadır.

4.Siber Terörizm: Pek çok devletin en önemli kurumlarının internet sitelerinin "hacker" lar tarafından çökertilmesi 21. yüzyılda bilişim suçlarının, ulusal güvenliği tehdit eden en önemli suç türleri arasında yer alacağını söyleyebiliriz.

Terörist grupların iletişimlerinde gizliliği sağlamak,propagandalarını yapmak ve finansal kaynaklarını artırabilmek amacıyla teknolojiyi ve Internet'i kullanmaktadırlar.Dünya Ticaret Örgütünün bombalanması eyleminin planlayıcısı Remzi Yusuf Amerikan Hava Yollarının şifrelenmiş olan dosyalarını diz üstü bilgisayarını kullanarak yok etmeyi planladığını itiraf etmiştir. Özellikle bir çok ülkede örgütlenen terörist gruplar ve uyuşturucu,silah ve insan ticareti yapan organize suç örgütleri fonlarını internet üzerinden transfer edebilmektedirler.(Fahlman, 1998)

Terörizme ilişkin suç unsuru taşıyan faaliyetler şu an için propaganda çerçeveli olarak yürütülüyor olsa da, sosyal hayatın tamamıyla sanal ortama geçtiği bir dönemde şiddet içerikli (patlayan bombalar, acil servis hizmetlerinin sekteye uğratılması, ekonomik zararların verilmesi, insan öldürülmesi, baskı-cebir uygulanması gibi) uygulamalar da görülebilecektir. Teröristler siber terörizmle;

- Kentin bütün trafik ışıklarını durdurabilirler..
- Telefonları felç edebilirler..
- Elektrik ve doğalgazı kapatabilirler..
- Bilgisayar sistemlerini karmakarışık hale getirebilirler..
- Ulaşım ve su sistemlerini allak bullak edebilirler..
- Bankacılık ve finans sektörünü çökertebilirler..
- Acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilirler..
- Ve nihayet hükümet kurumlarını alt üst edebilirler(Yamaç, 2001,3-4).

5.Yasadışı Yayınlar: Irkçılık, Çocuk Pornosu: Bir diğer durum da pornografi,ırkçılılık ve şiddet içerikli internet üzerinden yapılan yayınların durumudur. Bu yayınlar bütün ülkelerin kamu düzenini ihlal eden bir durum ortaya koymaktadır. Uluslararası platformda ülkeler bu yayınların yasaklanması konusunda işbirliğine gitmek yönünde çalışmalarını sürdürmektedirler. Teknik zorluklar , ISS 'larının sorumluluk rejiminin tespit edilememesi ve soruşturmada yaşanan güçlükler bu suçlulukla mücadelede karşılaşılan sorunların

başlıcalarıdır(Beceni,2002). İnternette faaliyet gösteren nefret ve şiddet içerikli ırkçı sitelere karşı Konvansiyon'a bir protokol eklenmesi konusunda çalışmalar yapılmaktadır. Net ortamında 2500'ü ABD'de olmak üzere toplam 4000 civarında ırkçı site olduğu bilinmektedir(Özcan , 2002)Tüm dünyada çocuk pornosunu önlemek için tedbir alınırken, ülkemizde kasetler posta ve kurye vasıtasıyla adrese teslim ediliyor olması ve bu CD'ler için satıcıların internet ve porno dergilerine ilan veriyor olması bir çelişkiyi ortaya koymaktadır. (http://www.aksam.com.tr/arsiv/aksam/2002/03/25/dunya/dunya4.html.)

1.3)DENETİM MÜMKÜN MÜ?

O halde temel sorun; kişi mahremiyeti,iletişim özgürlüğü gibi, demokratik toplumların olmazsa olmaz unsurlarının kısıtlanmadan ,bir denetim mekanizmasının kurulup kurulamayacağıdır. İkilem;özgürlüklerin temsilcisi olarak tanımlanan İnternetteki ,suçlarla mücadelenin, kişilik haklarının özüne dokunulmadan nasıl başarılacağıdır?

Aslında Internet'in global yapısı ,teknik olarak etkin bir denetim oluşturulmasına müsaade etmeyecektir. Diğer taraftan yasadışı eylemin siber-uzayda yapılmış olması soruna bir de adeta "görünmezlik" ve "ele geçirilemezlik" boyutu eklemektedir. Siber-uzayda gerçekleşen bir olayın kimin tarafından ve nerede yapıldığını ve sonuçlarının nerelerde etkili olduğunu saptamak bugünkü teknolojinin sağladığı araçlarla zor da olsa büyük ölçüde mümkün bulunmakla beraber, bunun için ilgili ülke makamlarının işbirliği yapmaları ihtiyacı ortaya çıkmaktadır (Kesmez,2001).

İşte bu gerçek, Internet'i özgürlüğün simgelerinden biri haline getirmiştir. Diğer yandan da yasa dışılığa göz yumulamaz. Şüphesiz ki;varolan bu özgürlük ortamı belirli kişilerce veya gruplarca kötüye kullanılmaya,suç teşkil eden fiiller için kaynak ve ortam oluşturmaya çok müsaittir. Örneğin çocuk pornosu içeren yayınlar yazılı,görsel basında kesinlikle yasakken,İnternet kanalıyla bu yayınlar dağıtılmakta hatta web siteleri kurulmaktadır. Oldukça yeni tarihli bir habere göre, Bursa'da bir ilkokul öğretmeninin İnternet kanalıyla çocuk pornosu kayıtlarını dağıttığı ,İngiliz Hükümetinin uluslar arası çalışmaları sonunda olayın Türkiye ayağında ortaya çıkarılmıştır (Özkan,Milliyet Gazetesi,28 Aralık 2001,sf:16). İngiltere'de ABD gizli servisinin yardımıyla gerçekleştirilen

operasyonda ünlü isimlerin yanı sıra polis memurlarının, milletvekillerinin, hakimlerin de yer alıyor olması olayın boyutunu ortaya koymaktadır. (Milliyet 26 Ocak 2003 nevsal Elezli)

Sorunun ikinci ayağını ,bu denetimin kimler tarafından yapılacağı oluşturmaktadır.

a) İnternet kullanıcılarının bizzat kendilerinin bu denetime katılmaları mümkündür. "Örneğin siber uzay ortamındaki yasadışı içerikli yayınlarla mücadele etmek üzere örgütlenmiş gönüllü bir sivil toplum örgütü olan IRRT(Internet Rapid Response Team),1998 yılında bir çocuk pornografisi koleksiyonunun reklamını yapan ve New York'taki bir adresten,dünyanın dört bir yanındaki İnternet kullanıcılarına gönderilen bir e-posta mesajını afişe etmiş ve elindeki bilgileri derhal New York polisine aktararak ,sorumlular hakkında soruşturma açılmasını sağlamıştır." (Sınar ,2001,s:50)

b)Yine sistem içersinde birinci derece öneme sahip İnternet servis sağlayıcıları(ISS) bireylerin Internet'e bağlanmalarını ,İnternet üzerinden iletişim kurmalarını ve Internet'in sağladığı olanakları kullanmalarını temin eden aracı unsurlardır. Bunlar kendi koydukları kurallarla ,hukuk düzeninin ana ilkelerini uygulayabileceklerdir (Sınar,2001 ,s:52).

c)Elbette ,tespiti yapılan suç unsurlarını değerlendirmeye yetkili emniyet birimlerinin de, uzmanlaştırılarak yeterli teknik bilgi ve donanıma sahip olmaları sağlanmalıdır (Sınar,2001,s:52).

d)Mekanizmanın en önemli ve ilk sujesi olması gereken "hükümet" son olarak belirtilse de,aslında sistemin etkili işlemesini sağlayacak hukuk düzenini oluşturacak suje olarak en önemlisidir. Türkiye de oluşturulmaya çalışılan hukuk sistemi, alt başlıklarda, Coşkun Ak davası örneğiyle incelenmeye çalışılacaktır.

1.4) ETKİN DENETİMİN KRİTERLERİ

Bu kriterleri belirlerken,"teknolojik denetim" kavramını özelleştirmek yerine, genel olarak "iyi bir düzenlemenin" nasıl olması gerektiğinden yola çıkmak ,konuyu belki de kulağa hoş gelmeyen, hatta ürkütücü "yasak kavramından" uzaklaştırabilecektir. Zira

çalışmamızda çeşitli yerlerde ısrarla vurgulamaktan kaçınmadığımız "özgürlük ortamı İnternet" ifadesinin, getirilecek denetim düzenlemeleriyle zarar görmesi,anlamını yitirmesi, bilime inanan,teknolojik gelişmeye açık bireyler için savunulacak bir sonuç olmayacaktır.

O halde; hükümetlerin onayıyla hukuksal yaptırıma kavuşacak düzenlemelerin etkinliği için toplumdan,kamuoyundan geniş bir destek görmesi gerekir. Bu desteğin sağlanabilmesi için de ilk şart; düzenlemelerin anlaşılabilir ve maksada uygun olması gerektiğidir. Bunun manası; toplumsal bir konsensüsle, uzlaşma sağlanarak bireylerin getirilecek düzenlemelere ihtiyaç duyduğu ve bunların temel özgürlüklerine zarar vermeyeceği kanaatinde birleşmeleridir.Ancak bu kriterler,kamuoyunun zamanla fikir değiştirebileceği, yeni düzenlemeleri de kabullenebileceği olasılığını tamamen göz ardı etmeden, popülist politikalardan arınmayı da içermelidir (Akdeniz,1998).

Bilişim teknolojisinin dinamik yapısı,hukuk yaptırımlarına meydan okumaktadır adeta. Yeni düzenlemelerin aldığı riskler, teknolojik gelişmeleri engelleyici veya sınırlayıcı olmamalıdır çünkü şartlar zamanla değişecek ve bazı uyarlamalar anlamsız veya yetersiz kalabilecektir (Akdeniz,1998).

Denetimden etkilenecek ilk suje olan bireysel kullanıcıları denetimin olumsuzluklarından korumak ,belki de İnternet ve diğer dijital teknolojilerin, anayasal koruma alanını genişleterek mümkün olabilecektir. Hükümetlerin İnternette gözetim ve bilgilere girme yetkilerinin sınırları açıkça belirlenerek, bireysel kullanıcıların mahremiyeti korunmalı ve buna paralel olarak özgür ortam İnternete güvenleri sarsılmamalıdır. Aksi durum dünyasında her konuyu barındıran, kimi zaman hastane,okul,işyeri; kimi zaman açık platform,borsa ve kimi zaman da "diğer her şeyi" temsil eden Internet'in gelişimine, daha da önemlisi insanlığın gelişim hızına vurulan ağır bir darbe olabilecektir(http://cdt.org)4.1.02.

II. AMERİKA ve BAZI AVRUPA DEVLETLERİNDE DENETİM KURUMLARI

2.1)Amerika Birleşik Devletleri (ABD)

Kişisel özgürlükler prensibinin neredeyse anane haline geldiği bu ülkede,devlet haberleşme mahremiyeti hakları ile terörizm,kaçakçılık ve devlete karşı işlenen diğer suçların önlenmesi konusunda dengeyi NSA (National Security Agency) ile kurmuştur. Başkan Harry S. Truman'ın 1952'de imzaladığı çok gizli genelgeyle kurulan NSA, istihbarat faaliyetleri yanında ülkenin bilgi güvenliğini de sağlamaktadır.(Türkiye Kriptografi Sayfaları,2001)

NSA denetimlerini ve istihbaratlarını kendi vatandaşları,oturma izni olan yabancılar ve Amerikan özel sektör kurumlarının gizlilik haklarına aykırı istihbarat faaliyetinde bulunması anayasa ve NSA'nın kuruluş yasasıyla kesinlikle yasaklanmıştır. Faaliyetleri ancak "diğer uluslar ve onların tarafları için istihbarat ve karşı istihbarat" etkinlikleriyle kısıtlıdır (Tübitak,Odtü,Bilten,2001)

Ancak NSA'nın çalışmaları hakkında kamuoyu gündemine zaman zaman yasalara uygun oluyor mu konusunda çeşitli iddialar da atılmıştır. Spiegel Dergisi Şubat 1989'da Almanya'da "Amerika'nın büyük kulağı" başlıklı bir haberi kapak yaptı. İddiaya göre Kuzey Denizi ile Alpler arasında her kim telefon ahizesini kaldırıyorsa NSA'nın öbür uçta oturduğunu bilmesi gerektiğini ,bu yüzden de anayasal olarak garanti altına alınan haberleşme özgürlüğünün boş bir söz olduğunu iddia etmişti.(Gökçin,2001)

15 Nisan 1993 günü NSA tarafından önerilen yeni bir kriptoloji politikasıyla "Public Encryption Management" (Amme Kodlama İdaresi) başlıklı bir kararname imzalamıştır. Bu çalışmaların odak noktası hükümet tarafından geliştirilen "Clipper" adlı bir kripto çipidir. Bu çipten beklenen, Amerikan donanım üreticileri tarafından üretilen her türlü güvenli iletişim ürünlerine yerleştirilerek ülkenin veri güvenliğinin artırılması, ihracatın sağlanmasıyla yabancı gizli servislerin casusluk faaliyetlerinin de alt-üst edilebilmesiydi. Ancak her çip için özel olarak üretilen anahtarların bir kopyasının hükümet tarafından tutulması ve tamamen yasal olmayan hiçbir nedene dayanılarak bu çipler üzerinden geçen trafiğin dinlenemeyeceğinin hükümet tarafından garanti edilmesi dahi ,projeye yeterli güveni oluşturamamıştır(Tübitak,Odtü,Bilten,2001).

Konuyla ilgili olarak Amerikan CPSR Vakfı (Computer Professionals for Social Responsibility),Hükümetin hizmet içi belgelerine dayanarak bir rapor yayımlamış ve NSA'nın

bu projeyle kendisine yeni sızma kanalları aradığını belirterek, yurtiçinde totaliter bir gözetim,yurtdışında ise devlet eliyle sanayi casusluğuna sebep olacağını ileri sürmüştür.(Gökçin,2001)

ABD'de yaşamsal altyapılarının korunması (critical infrastructure protection) amacıyla Başkan Bill Clinton ,1998 yılında Beyaz Belge direktifleri yayınlamıştır. Bu kavram ekonominin ve devletin minimum düzeyde işleyişi için gerekli fiziksel ve ağsal sistemleri kastetmektedir. Amaç ; devletin elektronikleşmesi ve açık ağları kullanmasının yaygınlaşmasıyla varolan tehditlerin ,saldırıların engellenmesidir (Tübitak,Odtü,Bilten,2001).

2.2İngiltere ve Almanya

"NSA dışında gelişmiş ülkelerden anılan iki diğer örnek kurum İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters) ve Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumudur (Bundesamt für Sicherheit in der Informationstechnik). İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters), NSA'ya çok yakın işlevler yürütmektedir. GCHQ'nun da oluşumu soğuk savaş dönemine dayandırılmaktadır.

Enformasyon Teknolojileri Güvenlik Kurumu (BSI) ise NSA ve GCHQ örneklerinden farklı olarak, istihbarat işlevi olmayan bir kurumdur. BSI bir Alman kamu kurumu olarak, bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürüten bir kurumdur. Araştırma sonuçları, kamuda söz konusu güvenlik uygulamalarının yapılmasına yarar sağlamaya çalışmaktadır. Kurum adli olaylarda da emniyete talep olduğu takdirde danışmanlık hizmeti verebilmektedir.

Alman Hükümeti de söz konusu teknolojiyi yasaklamak üzere girişimlerde bulunmaya başlamıştır. 4 Mayıs 1995 tarihinde Alman Parlamentosu "Telekomünikasyon İzleme Kanunu" adı altında ,ülkede tasarlanan ve kullanılan telefon, GSM, ISDN ve bilgisayar şebekesi tarayıcılarının, devlet birimleri tarafından gerektiğinde dinlenmesini sağlamak için standart bir ara bağlantı sağlamaları konusunda bir kanun teklifini onaylamıştır. Kanunun özünü, güçlü delillere dayanarak bağımsız bir yargıç kararı olmadan özel haberleşmenin

dinlenememesi oluşturmaktadır. Yargıcın gerekli gördüğü durumlarda, bu kanuna göre çağrı oluşturma bilgilerine ve GSM kullanıcılarının hücreler arasında izlenmesini sağlayacak bilgilere erişilmesi mümkün hale gelmektedir. Almanya, bu düzenlemesiyle, Avrupa ülkeleri arasında bireyi devlete karşı üst düzeyde güvenceye alan bir ülkelerin öncülüğünü yapmaktadır."(Tübitak,Odtü,Bilten,2001)

2.3)ECHELON: ÖRNEK OLAY

ECHELON, Amerika'nın öncülüğünde beş devlete (ABD, İngiltere, Kanada, Avustralya, Yeni Zelanda) ait istihbarat örgütlerinin dünya üzerindeki iletişimi kontrol etmek üzere oluşturduğu uluslararası bir istihbarat sistemidir. 1947'deki UKUSA anlaşmasıyla temelleri atılan ve 1971'de hayata geçirilen proje, o günden bu yana ABD Ulusal Güvenlik Dairesi NSA'nın yürütücülüğünde telefon görüşmelerinden internet haberleşmesine kadar bütün iletişim modellerini takip etmektedir.

Özellikle ABD, İtalya, İngiltere, Türkiye, Yeni Zelanda, Kanada, Avustralya, Pakistan ve Kenya topraklarında kurulan gelişmiş dinleme ve filtreleme sistemleriyle çalışan ECHELON'un varlığı uzun yıllar yadsınmasına karşın 1988 yılında Avrupa Parlamentosu'nun bir raporuyla kanıtlandı. Avrupa Parlamentosu raporu (http://cryptome.org/echelon-ep.htm) resmî, sivil tüm iletişimin kontrol edildiğini gösteriyordu. Bu tarihten sonra, çoğu Avrupa ülkelerinden olmak üzere birçok parlamento bu sistem hakkında araştırma ve soruşturma başlattı

Echelon'la ilgili yapılan araştırmalar ,İkinci Dünya Savaşı sonrasında İngiltere'yle istihbarat faaliyetlerini sürdürmek isteyen ABD'nin ,Echelon'un adımını ilk olarak "Shamrock Projesi" ile ortaya attığını göstermektedir. Daha sonra Kanada,Avustralya ve Yeni Zelenda da katılmıştır (Canbazoğlu,2001).

Bugün artık Yeni Zelenda ve Avustralya Hükümetlerinin de resmen kabul ettikleri Echelon Projesi ,iletişim istihbaratı konusunda soğuk savaş döneminde bilinen en büyük projedir. Pek bilinmemesine karşın Jam ECHELON Day olarak bilinen 21 Ekim 'Dünya ECHELON'u Örseleme Günü' olarak anılmaktadır.ilk kez 1999 yılında denenmiş ve

ECHELON'un filtreleme sistemine takılması kesin olan milyonlarca mail internet üzerinde serbest bırakılmıştır. (Süvari,2001)

Echelon'un Çalışma Sistemi

Echelon sistemi,istihbarat sağlama ,bilgiye ulaşma yolunda nasıl bir usul izlemektedir diye düşünüldüğünde sistemin basit ama nasıl etkin olduğuyla karşılaşılmaktadır. Sistemin ana parçasını,"Sözlük" (Dictionary) olarak adlandırılan ve içinde isimler,ilgili konu başlıkları,adresler,telefon numaraları ve belirlenen diğer kriterleri çok geniş bir veri tabanında depolayan bilgisayar oluşturmaktadır. Gelen mesajlar bu belirlenen kriterlerle karşılaştırılıp,bu kriterlere uyan mesajlar varsa, ham bilgi şeklinde otomatik olarak gönderilmektedir. Bu Sözlüklerin çalışmalarını, anahtar kelimeyle ilişki kurarak web sayfalarına ulaşan arama motorlarının çalışma usulüne benzetmek mümkündür. Yine aynı sistematikle ulaşılan ham bilgilerin gönderilmesini de e-mail yani elektronik posta olarak algılayabiliriz.

Sistemde üzerinde durulması gereken bir nokta da daha önceki kullanılan istihbarat metotlarında ,sisteme üye olmayan devletler veya birimler ,hangi bilgiler kime gönderiliyor bilirlerken;bugün kriterlere uyan küçük bir bölümü SÖZLÜK (Dictionary) bilgisayar tarafından seçilen mesajların ,kimse tarafından okunamadan direk NSA(Amerikan Ulusal Güvenlik Ajansı)veya sisteme dahil olan diğer devletlere gönderiliyor olmasıdır.(Cyber Rights,2001)

Echelon'u Nasıl Duyduk?

Projeye ortak beş devlet 10 adet yer ve 120 adet uydu istasyonuyla telefon,faks,e-posta,telsiz,teleks,cep telefonu ve benzeri her türlü data iletişimini takip edebilmektedir. Ancak dikkati ve tepkiyi çeken Echelon'u sadece bir istihbarat ağı olup askeri bilgileri ve ulusal güvenliğin gereği bilgileri filtrelemek yerine resmi daireler,şirketler,organizasyonlar ve bireyler gibi kaynakları da dinlediğinin iddia edilmesidir. İşte bu noktada haberleşme özgürlüğü ve mahremiyeti gibi birçok konuda sivil bir tepki doğacağı yanlış bir öngörü olmasa gerekir.

Bu konuya sivil dünyada ilk kez İngiliz Gazeteci Duncan Campbell değindiğinde başı belaya girmiş ancak yıllar sonra Avrupa Parlementosu'na danışmanlık yaptığında hazırlanan raporların sonuçları açıkça göstermiştir ki;artık birçok kimse Echelon'un varlığı,gücü ve en önemlisi istihbarat toplama konusundaki yaklaşımının**, "özgürlükleri tehdit edici boyutu"** konusunda Campbell'la aynı fikirdedir (Artan,2001).

Echelon: Denetim Mi?

Echelon'un ulusal güvenliğin korunması yanında,endüstriyel casusluk ,sivil oluşumların denetlenmesi (Greenpeace,Amnesty İnternational,vs) ve kişisel iletişimin kontrol altında tutulması gibi otoriter amaçlarla da kullanıldığı konusunda artık çeşitli kanıtlar ileri sürülebilmektedir. Tüm bu kaygılar, yaşanan somut olaylarla birleşince, Avrupa Parlamentosu'nun kişisel mahremiyetlerin korunmasına yönelik bir araştırma komitesi kurmasına sebep olmuştur (Campbell,2000).

İletişimde denetime karşı tüm bu raporları hazırlayan Avrupa Devletleri,İnternet üzerindeki faaliyetleri ve iletişimi sınırsızca izleme olanağı verme anlamına gelecek bir "Avrupa Mevzuatını",Avrupa Birliği'nde ne zamandır hazırlamaya çalışmaktadır. Mevzuatta telefon,faks,cep telefonu ve İnternet iletişimi verilerinin ,gerektiğinde yedi yıl süreyle saklanmasını zorunlu kılabilecek bu mevzuat üzerinde tartışmalar devam etmektedir(Artan,2001).

III: ÜÇÜNCÜ BÖLÜM: TÜRKİYE ve INTERNET'İN DENETİMİ

3.1)İNTERNET (ÜST) KURULU

Ulaştırma Bakanlığı'na danışmanlık hizmeti vermek üzere yapılandırılan kurulun, Başbakanlıkça hazırlanan "İnternet Üst Kurulu Görevleri ve Teşkilat Yapısı Hakkında Kanun Tasarısı Taslağı" ilk madde de amaçları açıkça belirtiliştir. Buna göre kurul: (Bilişim Stk Platformu,2001)

- Ulusal sınırlarımız içerisinde kişi ve kurumlara ait bilgelerin korunması,güvenli bir şekilde transfer edilmesi,izinsiz kullanımının önlenmesi
- Adli ve polis birimlerine yardımcı olmak,ulusal güvenliği tehdit eden bilgi ve yayın transferine engel olmak
- Kişi hak ve özgürlüklerini etkileyici bilgi ve belgelerin izinsiz yayılmasını önleyici tedbir almak
- Uluslar arası İnternet suç ihlallerine karşı işbirliği ve koordinasyon görevi yapmak
- Gelenek ve kültür mirasımızı etkileyici bilgi,haber ve belgeyi temel dayanak olmadan yayımlamamayı amaç edinen bir çalışma yürütmek

Taslağın ilk maddesinde kurulun amaçlarının İnterneti geliştirmek ve hayatımıza koordinasyonunu sağlamak ve yeni ortamda varolabilecek olumsuzlukları gidermek olduğu çok açıktır. Ancak çalışmamızın genelinde ifade etmeye çalıştığımız gibi,maksada uygunluk büyük bir önem içermektedir. İnternet suç işlenen ve özgürlüklerin ihlal edildiği ,orman kanunlarının hakim olduğu bir alana dönüşmesin derken, kişi haklarının bizzat idari organlarca devlet eliyle ihlal edildiği düzenlemelerden kaçınma zorunluluğu vardır. Kurumlara verilen yetkiler hukuksal düzenlemelerle özgürlükler lehine sınırlanmalıdır. Bu konu anayasamızda da güvence altına alınmak istenmiştir. Anayasa'nın Genel Esaslar Kısmında bulunan Devletin Temel Amaç ve Görevleri başlıklı beşinci maddesine göre :

"Devletin temel amaç ve görevleri,.....;kişinin temel hak ve hürriyetlerini,sosyal hukuk devleti ve adalet ilkeleriyle bağdaşmayacak surette sınırlayan siyasal,sosyal ve ekonomik engelleri kaldırmaya ,insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmaktır." (DEÜHF,1993)

3.2) RTÜK ve ULUSAL BİLGİ YASA TASARISI

Peki düzenleme neler getiriyor: Eğer tasarı yasalaşırsa, bundan böyle web sayfası açmak isteyenler valilik veya kaymakamlıklara bunu bildirmek zorunda olacaklar, beyanname vermeden açılan web sayfaları için valilik Asliye Ceza Mahkemesi'nde yayın durdurma davası açabilecek, web sayfalarının içeriğinin ikişer kopyası her gün cumhuriyet savcılığı ve

valiliğe teslim edilecek. Web sayfalarını en az lise mezunu ve 21 yaşından büyük sorumlu müdürü olacak ve yabancılar web sitesi açmak için Dışişleri Bakanlığı'ndan görüş ve İçişleri Bakanlığı'ndan izin almaları gerekecektir.

Kurumların oluşturulması yanında ,hedeflerine ulaşabilmeleri ,projeler üretebilmeleri için gerekli imkan ve altyapıyı da oluşturmak gereklidir. Konuyla ilgili uzman kişi ve kurumların görüşlerinin alınması gerektiğini belirtmiş idik. Ancak bir danışman kurul olarak kurulmuş olan İnternet (Üst) Kurulu ,mecliste RTÜK Yasa Tasarısı görüşmeleri sırasında Internet'in de RTÜK kapsamına alınması konusu değerlendirilirken etkin olamamıştır. İnternet Üst Kurulu üyesi Doç. Dr. Mustafa Akgül ve TBMM Bilgi ve Bilgi Teknolojileri Grubu Başkanı Prof. Dr. Ziya Aktaş tasarının gereksiz bürokrasi getirdiği gibi yeni maddi külfetleri de olduğunu belirterek,İnternete uğraşan kişilerin önlerini tıkadığını ,olumsuz etkilediğini vurgulamışlardır (Akgül,Aktaş,2001) Nitekim, Internet'in anavatanı olan Amerika Birleşik Devletleri'nde; "İletişim Ahlakı Yasası" (Communications Decency Act), yasada ne tür eylemlerin suç haline getirildiğinin tam olarak belirlenmediği gerekçesiyle Yüksek Mahkeme tarafından iptal edilmiş, "Çocukları Online Yayınlardan Koruma Yasası" (Child Online Protection Act) da, düşünce ve fikir özgürlüğünü ihlal ettiği gerekçesiyle Amerikan Federal Mahkemesi tarafından anayasaya aykırı bulunmuştur. Ülkemizde ise, İnterneti bir bütün halinde Basın Kanunu kapsamına alacak olan yasa değişikliğine kamuoyundan büyük tepkiler gelmiş ve söz konusu yasa değişikliği Cumhurbaşkanınca veto edilerek yürürlüğe girememiştir (www.bilisimsurasi.org.tr/listeler/tbs-hukuk/ Feb/att-0027/01-yoneticiozeti1.doc)

Vetoya gerekçe olarak Sezer,Internet'in özelliklerinin yazılı basına uygulanan kısıtlamalarla bağdaşmadığı,demokrasi geleneklerine,temel hak ve özgürlüklere ve Anayasa'ya aykırı olduğu,yasakların çok belirsiz tanımlandığı ve bunun suçların yorumu konusunda belirsizlikler yaratacağını göstermiştir. Konuyla ilgili olarak Fransa'da "Le Figaro",İsviçre'de "Neue Zürcher Zeitung" ve Tokyo'da "Yomiuri Shimbun" gazeteleri için yazılan İstanbul çıkışlı yazılarda,Cumhurbaşkanının vetosu "özgürlükler" adına olumlu değerlendirilmişlerdir.(Başbakanlık Basın-Yayın ve Enformasyon Genel Müdürlüğü,2001)

Bir başka yasalaşma çabası da ,yaklaşık üç yıldır gündemde olan tartışmalı Ulusal Bilgi Güvenliği (UBG) Yasasıdır. Geçtiğimiz mayıs ayında Başbakanlığa sunulan , bilgi güvenliği gerekçesiyle sektöre getireceği kısıtlamalar açısından tepki çeken tasarı,Genelkurmay Başkanlığı'nın koordinatörlüğündeki Güvenlik Çalışma Grubu tarafından Mart ayı sonunda tamamlanmıştır. Yasa "Ulusal Bilginin polisiye önlemlerle denetlenmesini ve korunmasını amaçlıyor ve ulusal güvenliği ilgilendiren gizli bilgiyle işlem yapan kamu kurum,kurul ve kuruluşları ile özel kuruluşlar ve diğer gerçek ve tüzel kişileri kapsıyor. (http://www.telepati.com.tr/mayis02/haber29.htm) 3.02.2003

Yasa mevcut durumu itibariyle hak ve özgürlüklere müdahale gücünü yargıç kararı olmadan bir kuruma verdiği gibi üstelik bu müdahalenin sınırlarını da çizmiyor. Yasa taslağı mevcut haliyle, hayatın her alanına müdahale etme niteliği taşıyan otoriter toplum yasası hüviyetine bürünüyor.(http://www.bthaber.net/274/menu_haber_06.htm) 3.02.2003

Sivil oluşumların konuyla ilgili yapmış olduğu bir çok çalışmalar da, uyuşmazlıklara çözüm önerileri getirme çabasının gereğidir. Rtük Yasası Hakkında Bilişim Sivil Toplum Kuruluşları Ortak Deklarasyonunda ,Türkiye'de İnternetle ilgili yapılması düşünülen ilk düzenlemelerden birinin teşvik değil kontrol ve ceza boyutunda olmasının hayal kırıklığı yarattığının vurgulanması ,tarafımızca, tasarıyla istenilen sonuca ulaşılamayacağının bir diğer ifadesi olarak yorumlanmıştır.Türk.internet.com tarafından düzenlenen geleneksel "İnternet Breakfast Forum"da da görüşler iki noktada ayrılmıştır:

-Internet'in ayrı bir yasası olmalı ---- İnternet için ayrı bir yasal düzenlemeye gerek yok

-RTÜK için eylem planı yapılmalı----RTÜK için eylem planına gerek yok,zaten internet için uygulanması imkansız bir yasal düzenleme (Tozkoparan,2001)

Tüm bu tartışmalar örnek bir olayla ele alınırsa cevabı da belki netleşebilecektir.

3.3) COŞKUN AK DAVASI

Coşkun Ak, Mayıs 1999 tarihinde Superonline da çalışırken interaktif bölümler koordinatörü olarak tartışma forumlarının teknik sorumlusudur. 26 Mayıs 1999 tarihinde forumun tartışma konusu Türkiye'de insan hakları ihlalleridir. Konuyla ilgili "bir insan"

rumuzuyla foruma gönderilen mesaj, diğer forum üyelerinin tepkisini çeker. Foruma katılan bir başka kişi Coşkun Ak'a mesajda suç unsuru bulunduğunu bildiren bir mesaj gönderir ve mesajın forum sayfalarından çıkarılmasını talep eder. Mesaj, Coşkun Ak tarafından forum sayfalarından çıkarılınca mesajdan rahatsız olan kişi Adalet Bakanlığına suç ihbarında bulunur. Böylece Coşkun Ak davası başlamıştır (Akdeniz, 2001).

Cumhuriyet Savcılığı düzenlediği iddianamede Ak'ı TCK madde 159'a göre sorumlu tutmuştur. Hazırlanan iddianameye göre:

"... ancak sanık Coşkun Ak, yazılanlarda suç unsuru bulunmadığını düşünerek ikaza rağmen İnternetteki sayfayı iptal etmemiş, yukarıda arz edilen bir haftalık sürenin bitmesini beklemiş ve bu süre içerisinde anayasal kuruluşları tahkir ve tezyif eden sözler içeren İnternet sayfası İnternet kullanıcılarının istifadelerine açık tutulmakla suçun unsurları gerçekleşmiş bulunmaktadır.

Ülkemizde İnternetle işlenen suçlar bakımından yasal bir düzenleme olmamakla birlikte sanığın durumu, yazı sahibinin kimliğini açıklamayan mevkute sorumlu müdürü veya yayınlatan durumuna benzemekte olup, suça konu İnternet sayfasının düzenlenmesine önayak olan, ikaza rağmen, o sayfada yayınlanan mesajları İnternet ortamında silmeyen ve İnternet kullanıcılarının hizmetine sunan Coşkun Ak'ın bu sayfada yer alan aşağıdaki sözlerle mesnet suçları işlediği kanaatine varılmıştır." (Tozkoparan, 2001).

Bu iddianameyle kırk ay hapis cezasına hükmedilen Ak'ın dosyası Avukatı Fikret İlkiz tarafından temyiz edilmiştir. Davayla ilgili temel sorunları analiz etmek çalışmamızın amacına uygun olacaktır (Akdeniz, 2001):

- " Kanunsuz suç olmaz" ilkesinden hareketle sanık, olmayan bir yasanın ve tanımı yapılmamış bir suç fiilinin faili olarak yargılanmıştır.

- Madde 159'a aykırı olan yazının sahibinin kimliği belli değildir.

- "Unmoderated" forumlarda hiç kimsenin mesajları okuma diye bir sorumluluğu yoktur. Hukuki açıdan olayın basın kanunundaki editör sorumlulukları ile kıyaslanması yanlıştır.

Bu çıkarımlarla Ak'ın sadece "kanunsuz suç olmaz" ilkesine dayanarak dahi sorumlu tutulamayacağı düşünülebilecektir. Burada Türkiye'de İnternet ortamında servis sağlayıcıların ceza sorumluluğu gündeme gelmektedir, tartışılması gereken asıl konu da bu olmalıdır. İnternet servis sağlayıcılarının hukuki durumları ve verdikleri hizmetler açısından internet ortamında gerçekleşen hukuka aykırı fiillerle ilgili olarak sorumluluk ve yükümlülüklerinin açık ve net bir şekilde düzenlemesi gerekmektedir.

SONUÇ

Çalışmamızın çıkış noktası olan Internet'in tanımı ,sonucu bağlamamızda da yine bize yol göstermelidir. Tamamen yeni,tamamen farklı, benzeri olmayan bir kavramın beşeri hayata bu kadar hızlı ve bu kadar etkin girmesi, tabiatıyla bir çok yeni sorunu da beraberinde getirmiştir. Soğuk savaş sırasında en sık sorulan soru şuydu:"Füzenizin büyüklüğü ne kadar?" Küreselleşme çağında ise en sık sorulan şudur: " Modeminizin hızı ne kadar?"(Friedman,2000) Internet'in koruma altına alınması prensibi bir çok ülkede kabul görmekteyse de, henüz yeterli düzenlemelerin yapılamadığı, etkin denetimin tam olarak sağlanamadığı açıktır.

Bu nedenle İnternetle hayatımıza giren her yeni kavram ve beraberinde getirdiği her problem için ulusal hatta uluslararası bir temel politika oluşturulması gerekir. Bunun da temel koşulu bu alandaki gelişmelerin tamamına hakim olmak ve bilmektir. Bilginin güç olduğu bir çağda, asıl olan bilgiyi doğru maksatlar için doğru alanlarda kullanabilmek olacaktır.

Internet'in zararlarına odaklanmak yerine, pozitif yönleriyle sunduğu olanakları ön plana çıkarıp ,olumsuzlukları bir pota içersinde eriterek, mutlak hukuka dayalı etkin denetimi sağlamak, daha rasyonel bir tutum olacaktır (Akgül,2001). "Genel eğilimlerin dışında geliştirilmeye çalışılacak uygulamalar sosyal ve ekonomik açıdan zararlı olabilecek,uluslar

arası standartlara uymayan yapılanmalar ülkeleri yalnızlığa itecektir."(Tübitak,Odtü,Bilten,2001)

Uluslar arası standartlar dendiğinde İnsan Hakları Evrensel Bildirgesi,Avrupa İnsan Hakları Sözleşmesi,Kişisel ve Siyasal Haklar Sözleşmesi düzenlemeler için kriter olarak alınması gereken hukuk belgeleri olarak akla ilk gelenlerdir. Özgürlük ve hakları kural; kısıtlamaları ise istisna kabul edip,denetim yöntemleri konusunda seçimler bu yönde yapılacak olursa,hukukun üstünlüğüne ve hukuk devleti ilkelerine olan inancımızı da ifade etmiş oluruz.

Yapılacak düzenlemelerin bilgiye tam erişmeden,yetkin olmayan kişi veya kurumlarca aceleci yaklaşımlarla düzenlenmesi denetim mekanizmasını amacından uzaklaştıracaktır. Zira denetimden amaç sansür değil,İnternette gelişimin önünün kesilmemesi olmalıdır ve global dünyada da yaygın inanış bu yöndedir. İnternet; dünyayla bütünleşme,ülkelerin rekabet gücünü artırma,bireylerin,başta kişisel bilgi alma özgürlükleri olmak üzere, "her şeyi" temsil etmektedir. Her şeyin olduğu bir dünyada çatışmalar ve kaoslar yaşanacaktır,denetim mekanizmalarına düşen; bu kaos ve çatışmaları yasak ve sansür gibi kavramlarla körüklemek yerine akılcı yaklaşımlarla çözüme kavuşturmak olmalıdır. Akılcı yaklaşımın en büyük kanıtı da,sadece iktidar güçleriyle değil,gerek üniversiteler gerek sivil toplum örgütleri gerek İnternet Kurullarının katılımlarıyla bu düzenlemelerin hazırlanması olacaktır (Bilişim Stk Platformu,2001)

Kanımızca özellikle devlete tanınacak denetim haklarının sınırları iyi belirlenmeli ve ancak yasal kanıt olması durumunda ve yine yasal mercilerden alınacak somut olaylara özgün izinlerle denetim yapmalarına olanak tanıyacak düzenlemelere gidilmelidir. Zira Dünya Ticaret Merkezi ve Pentagon'a gerçekleştirilen saldırının ardından bir İnternet servis sağlayıcısı olan AOL'ın (American Online) müşterilerine ait e-postalarını incelemesi için NSA'nın teklifi gelmeden vermesi ciddi rahatsızlıklara sebep olmuştur. Bu tepkiler de bireylerin konu temel özgürlükleri olduğunda , herkesçe lanetlenen "11 Eylül Saldırıları" karşısında bile bu haklardan vazgeçme şeklinde hareket etmeyeceklerini kanıtlamaktadır(Canbazoğlu,2001).

AKDENİZ,Y 2001,*Who Watches the Watchmen:Part II*
http://www.cyber-rights.org/watchmen-ii.htm#technology [4.01.02]

AKGÜL, AKTAŞ 2001, NTV, *İnternet,Suç ve Ceza*
http://www.ntvmsnbc.com/news/84859.asp?0m=-5qr [04.01.02]

ARTAN,Ş 2001,*Echelon Gerçek*
http://www.geocities.com/sahinartan/cyberman2505a.html [29.12.01]

BAŞBAKANLIK BASIN-YAYIN ve ENFORMASYON GENEL MÜDÜRLÜĞÜ,2001

http://www.byegm.gov.tr/YAYINLARIMIZ/DISBASIN/2001/06/21x06x01.HTM

BECENİ,Y 2001,Hukukçu
http://www.hukukcu.com/bilimsel/kitaplar/_yasinbeceni/bolum3.htm
[30.12.01]

BİLİŞİM STK PLATFORMU,2001,*İnternet Üst KuruluGörevleri ve Teşkilat Yapısı Hakkında Kanun Tasarı Taslağı*
http://bt-stk.inet-tr.org.tr/ust-kuruly.htm [09.01.02]

BÜKE,A 2002, Bilgi Çağının Başka bir yüzü:Siber Suçlar
http://www.izto.org.tr/rapor/sibersuc.htm

CAMPBELL,D 2000,*Flow In Human Rights Uncovered*
http://www.heise.de/tp/english/inhalt/co/6724/1.html [10.01.02]

CANBAZOĞLU,C 2001,*Amerika Apo'yu Bulduğu SistemleLadin'in Teröristlerinin Peşinde!*
http://www.yeniortam.com/haber.asp?h_id=3275 [29.01.01]

CDT 2001
http://cdt.org

CYBER RIGHTS	2001,*Interception Capabilities 2000* http://www.cyber-rights.org/interception/stoa/ic2kreport.htm [29.12.01]
DEÜ	1993, TC Anayasası ve İlgili Kanunlar,sf:11,Ankara: DEÜ Hukuk Fakültesi Döner Sermaye İşletmesi Yayınları no:36
DİKEY 8	2002, Dikey 8 Bilişim Güvenliği İletişim Platformu, 'İnternette ilk 10 Dolandırıcılık' http://www.dikey8.com/modules.php?op=modload&name=News&file=article&sid=179&mode=&order
FAHLMAN, ROBERT C.	1998 "Intelligence Led Policing and Key Role of Criminal intelligence Analysis : Preparing for the 21 st Century" www.interpol.int
FRIEDMAN,T	2002,Küreselleşmenin Geleceği,Boyner Yayınları,İstanbul
GÖKÇİN,M	2001,*ABD Bizi Niçin ve Nasıl Dinliyor?* http://www.komplo.com/komplo/istihbarat4html [08.01.02]
JAY,L	2001,*How Terrorists Use the Internet* http://www.newsfactor.com [31.12.01]
KESMEZ,N	2001,Türk Bilişim Derneği,*Avrupa Konseyi ve Siber-Uzay Suçları* http://tbd.org.tr/sayi79_html/hukuk_kesmez.html [6.01.02]
ÖZDEMİR,O	2001,Araf Dergisi http://araf.net/dergi/sapo/sp2_o_ozdemir/bolum0.shtml
ÖZKAN,T	28.12.01,Milliyet Gazetesi,*Çocuklara Kıymayın Efendiler,Sahip Çıkın*, sf:16
RADİKAL	Siber Mafyalar, Radikal Online 03/03/1999 http://www.radikal.comtr/diger/ekler/sanalalem/1999/03/03/kapak/sib.html
SINAR,H	2001,İnternet ve Ceza Hukuku,Beta Yayım,İstanbul Yayın No:1138,Hukuk Dizisi:458
SÜVARİ,Ö	2001, Zip İstanbul , Sayı 76 http://www.zipistanbul.com/iss/01-11-16/net/index.shtml)

TOZKOPARAN,G 2001,*Avukat Fikret İlkiz:Sansüre Hazır Olun!*

http://türk.internet.com/haber/yazigöster.php3?yaziid=1988

TÜBİTAK,ODTÜ,BİLTEN 2001,Raporlar,*Ulusal Bilgi Güvenliği*
http://bilten.metu.edu.tr/publications/ubg.html [07.01.02]

TÜRKİYE KRİPTOGRAFİ SAYFALARI 2001,*ABD'nin Küresel Gözetim Sistemi*
http://gsu.linux.org.tr/kripto-tr/echelon.html [29.12.01]

UCLA ÜNİVERSİTESİ 2001
http://www.gseis.ucla.edu/iclp/cyber-surveillance.htm [22.12.2001]

YAMAÇ FATİH 2001, Bilişim Suçları, Türkiye İnternet Konferansları 7, 1-3 Kasım 2001 İstanbul, http://inet-tr.org.tr/inetconf7/bildiriler/

YAZICIOĞLU,Y 2001,Sabah Online,*İnterneti de mi Türkleştiriyoruz*
http://garildi.sabah.com.tr/sayfa.cgi?w+30+/0105/13/t/z08.html [4.01.02]

YILMAZ, M 2001, Olympos Security 'Bilişim Suçları Hakkında'

http://www.olympos.org/article/articleview/261/1/2