BİLİŞİM ALANINDAKİ YENİ TEKNOLOJİLERİN HUKUKSAL YANSIMASI İTALYA'DAKİ DURUM*

Carlo Sarzana di S. IPPOLITO**

Çeviren: Vesile Sonay DARAGENLİ***

GİRİŞ

Hiç kuşkusuz bilişim sistemlerinin gelişimi, hukuk alanında yeni problemler ve önemli değişiklikler meydana getirdi. Örneğin telif haklarında, özel hayatın korunmasında, ceza ve ceza usul hukukunda, medeni hukukta, ticaret hukukunda ve telekomunikasyon hukukunda meydana gelen değişiklikleri sayabiliriz.

Hukuk ile teknolojik gelişme arasında bir açık var. Ulusal alanların da ötesine geçen ve dünya çapındaki kompütür ağlarında gerçekleşen bazı olaylarda bu açık oldukça belirgindir. Uluslararası hukuk burada yeterli önlem alamamaktadır. Bilişim suçluluğunun gelişimiyle mücadele etmek için, yetkili yargı makamını ve operatörlerin sorumluluğunu belirlemek için uluslararası işbirliğiyle uygun araçların öngörülmesi gerekir.

Multimedia sistemlerinin (istediğin an (video on demand), interaktif servisler, eletronik ticaret, teleödemeler vs.) kullanımına ilişkin özel hukuksal problemler bulunmaktadır.

Fransız uzman Pier Huet[1] multimedia servislerindeki problemlerden bazılarını inceledi. Kendisi söz konusu hizmetlerin hukuksal açıdan basın, telekomunikasyon, elektronik haberleşme ile duysal-görsel sistem arasında bulunduğunu saptadığı için multime-

---

* Bu konferans İstanbul Üniversitesi Hukuk Fakültesi'nde 2.10.1997 tarihinde verilmiştir.

** İtalyan Yüksek Temyiz Mahkemesi Ceza Dairesi Başkanı

*** İstanbul Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku Anabilim Dalı Araştırma Görevlisi.

1 Problèmes juridiques des services multimedias, Expertises, 1995, n.189.

dia işlemlerinin yapılması ve kullanılması, telif hakları hukuku, özel hayatın ve kişisel bilgilerin korunması, kamusal bilgilerin ticareti, haberleşmenin gizliliği, bilişim sistemlerinin güvenliği ve şifre anahtarlarının kullanılması gibi birçok alanı kapsamaktadır.

Güvenlik sistemlerinin kullanılmasına, bunların çalıştırılması ve yönetimine, programların hukuka aykırı olarak kopyalanması ve korsan yazılım (software) ticaretine ilişkin organize ve ekonomik sonuçlar olduğu muhakkak .... ama bu konumuzun dışına çıkar.

Kuşkusuz, bilişim suçları kompütür kullanımına ilişkin suçlardır. Özellikle 80'li yıllarda uluslararası organizasyonların dikkatini çekti ve sanayileşmiş ülkelerin kanun-koyucularının, ulusal hukuk sistemlerine müdahale etmelerini sağladı.

Bu konuda özellikle İtalya'ya daha sonra döneceğim. Hukukçuların dikkatini çekmesi gereken en azından üç alan vardır.

YENİ BİLİŞİM TEKNOLOJİSİNİN HUKUKSAL ALANDAKİ YANSIMASI: BUGÜN VE GELECEK

Kanaatime göre hukuk ile bilişim teknolojisinin gelişimi arasında üç alanda önemli etki vardır ve olacaktır. Bunlar: a) Çok kullanıcılı sistemler b) akıllı robotlar c) sanat gerçekler veya virtuel gerçekler.

1.1- Birinci konuda, her biri ayrı ama birbirini tamamlayan birden fazla kişinin işbirliğiyle meydana getirilen çok kullanıcılı sistemlerde[2], bilişim sistemlerinin kötüye kullanılmasından sorumlulukların araştırılmasına ilişkin problemlerin önemli ölçüde artacaklarını göz önünde tutmak gerekir.

Sistemin kötüye kullanılması halinde sorumluluk kime yüklenecektir? Bilgi bazını oluşturan kişi veya kişiler mi? veya sebebi gerçekleştiren kişi veya kişiler mi?

Sistemin hatalarını farkedebilen veya farketmesi gereken kullanıcının sorumluluğu var mıdır? Tıp alanında teşhis veya tedavi için kullanılan çok kullanıcılı sistemler

---

2 Bilindiği gibi çok kullanıcılı sistemler gün geçtikçe gelişmekte ve bugün tıp gibi bazı alanlarda özellikle mikrobik hastalıklar, iç hastalıklar ve katarakt (glucoma) teşhis ve tedavisinde oldukça sık kullanılmaktadır. Psikoloji, mühendislik, nükleer, endüstriyel ve hava ulaşımı vb. alanlarında önemli deneyler yürütülmektedir. Çok kullanıcılı sistemin kötüye kullanılması halinde neden olunan fiziksel veya ekonomik zararlardan ceza hukuku açısından sorumluluğu saptamak çok zordur. Hatalar, programcıların, bilginin bazını oluşturan uzmanların, dağıtıcıların, üreticilerin ve bazı hallerde bu sistemleri kullananların da hareketlerine bağlı olarak meydana gelebileceği gibi hareketlerinden ayrı olarak da meydana gelebilir.
Çok kullanıcılı sistemin hava ulaşımının kontrolü için kullanılması halinde, konuyla ilgili yazar Tod M. Turley bundan meydana gelen zararların dört hata kaynağının birleşimine dayandırılabileceğini açıkladı ve bunlar: a) programda hatalar (mantık veya yazım); b) bilgi bazındaki hatalar; c) programın kullanılması yetkisine ilişkin hatalar; d) donanım (hardware) yetersizlikleri. Çok kullanıcılı sistemlerin kullanılması sorumluluğu konusunda Amerikan doktrini için bakınız M. Gemignani, *Potential Liability for Use of Expert Systems, Idea*, cilt 29, n. 2. İtalyan doktrini için G. Corrias Lucente, *"Prime considerazioni in tema di responsabilita penale e gestione di sistemi informatizzati con particolare riguardo ai sistemi esperti*, "Il diritto dell'informatica" dergisi, 1989, 117vd.

veya nükleer tesislerin gözetimi vs. söz konusu olduğunda konu ciddi boyutlara varmaktadır.

Dünyanın en büyük askeri güçlerinde bulunan ve ülke savunmasında kullanılan bilişim sistemlerinin kompleksliği aynı zamanda zarar görebileceği dikkate alınırsa bilişim sistemleri alanında bulunan yazılımın yapımı ve yönetimindeki hata ve ihmallerin toplumsal sonuçlarına ilişkin endişeler artacaktır. Yapma akılın[3] kullanılması halinde bahsettiğimiz bu problemler tamamen, çözülemez gözükmektedir.

1.2.- İkinci konuda ise, insan ve bilgisayar arasındaki komunikasyon teknolojisinin gelişimi, etik, sosyal ve hukuki alanda birçok sonuca yol açacaktır.

Birinci problem, akıllı robotların yapılması ve yönetimine ilişkindir, yani hareket etme, belirli durumlarda tepki verme, belirli uyarılara cevap vermek ve belirli durumları çözmek için yeniden programlanma kapasitesi olan robotlar. Bu alanda hukukun, özellikle ceza hukukunun çözmesi gereken problemler olacaktır.

Kuraldışı, tehlikeli veya zararlı bir durumu gerçekleştiren bu tip bir robotun hareketinden sorumluluk kime yüklenmelidir? Onu yapana mı? Sahibine mi? Ve hangi sınırlar dahilinde? Japonya'da ve Amerika'da sanayi kuruluşları içinde robots-killer halleri gerçekleşmiştir. Uzmanlar yakında robot bekçi köpekleri veya bodyguardları[4] kullanma imkanına sahip olacağımızı söylüyorlar. Hukuki açıdan mülkiyetin korunmasında bu tip robotların kullanımıyla offendicula kullanımını mukayese etmek mümkün müdür?

Başka bir açıdan da robotların varlığı medeni hukukta, anayasa hukukunda, hukuk felsefesinde ve felsefe biliminde çözülmesi çok zor problemler getirebilecektir.

Bu konuda Amerika'da (bkz. Mc Nally ve Inyatullah'ın makaleleri, Law and Tecnologie, 1987; August'ın makalesi, Computer and Law Journal, 1988; Felsefeci Putman'ın eserleri, "Mente, linguaggio e realta", Milano, 1987, vs.) ve İtalya'da (bkz. Prof. Taddei-Elmi'nin "Una tutela degli automi implementati da programmi intelligenti" başlıklı çalışması ve Gozzano'un" I cinque sensi dei robots" başlıklı makalesi, Sapere, Nisan 1990) bir tartışma bulunmaktadır.

---

3 Uzmanlara göre yapma akılın yeni şekilleri hukuksal problemlerden öte büyük etik problemler yaratacaktır. Yapma akıl sistemlerinin en büyük uzmanlarından biri olan ve Massachusetts Teknoloji Enstitüsü profesörü Alain Minsky, 50 yıl içinde "gerçek düşünen makinalar"a sahip olacağımızı, ancak bunların son derece saldırgan ve çılgın olacağını söylüyor. Yine Minsky ilk modellerin birden fazla elle üretildiğinden, öngörülemez hareketler gerçekleştireceklerini ancak sonradan bu makinaların büyük bir olasılıkla düzeltileceğini ve o zaman - bilgi gücü konusunda insanın rakipleri alacaklarını söylüyor.

4 Alvin Toffler'e göre"....gelişmiş askeri laboratuarlarda bugün nöbetçi robotlar, keşifçi robotlar, hatta sanal uçuş eğitimi sırasındaki hatalarından öğrenme kapasitesinde olan pilot robotlar zaten var ve bunlar etten ve kemikten olan meslekdaşlarına göre daha iyiler. (bu konuda bakınız Luca Neri'nin 7 Ocak 1994 tarihli L'Espresso'daki makalesi, s.27).

Robotlara hukuksal şahsiyet açısından da olsa medeni hakların sağlanması aracılığıyla bir hukusal kimlik selfdeterminasyon verilmesinin doğru veya gerekli olup olmadığı sorulmaya başlandı[5].

1.3- Üçüncü konu sanal gerçeğe veya virtuel gerçeğe ilişkindir. Sanal uçuşlara ilişkin bu tip bir teknoloji sivil ve askeri pilotların formasyonu ve eğitimi için zaten kullanılmaktadır[6]. USA Dayton eğitim merkezi askeri pilotlarının sanal kabinden çıkarken sanal hava muharebesi sonucunda hayatta kalmış veya ölmüş oldukları için terden su içinde kaldıkları görülmüştür. Yeni teknoloji Amerika'da Nasa'nın, Fransa'da Cea, Tolosa'nın Laas'ın ve Montpellier'deki 103 Birliği'nin çalışmaları ve denemeleri sonucunda önemli ölçüde gelişmiştir. Yeni dünya özel yön ve durum duyuları olan gözlüklerle, el ve parmak hareketlerini yöneten özel eldivenli, sesleri tanıma sistemine bağlı mikrofonlu bir bilgisayar desteğiyle yaratılmıştır; daha gelişmiş sistemlerde özel bir tulum da kullanılmıştır.

Araştırmacılara göre insan-bilgisayar ilişkisi Cyberspace denen bağlantıyla üç boyutlu görüntü, tat ve anlatım kullanılarak gerçek boyuta ulaştırmak amacıyla insan birden fazla duyuma ulaşmıştır. Bu gelişmiş mekanizmalar sayesinde kişi gerçeğe tıpa tıp benzeyen bir dünyaya kavuşmuştur. Virtuel gerçeğin en büyük uzmanlarından olup, bu yeni tekniğin babası kabul edilebilecek Krueger'e göre bu yüzyılın sonunda interaktif teknoloji olağan olacak ve bu sayede insanlar tecrübelerinin en büyüğünü yaşayacaklardır (Kruger, Realtà artificiale, Addyson-Wesley, Milano, 1992). Bu sebeple de yeni ve çözülmesi zor hukuksal problemler ortaya çıkacaktır. Uzmanların da dediği gibi kişilik ve sorumluluk gibi değerler tartışma konusu olacaktır[7].

Amerika, İngiltere, Fransa, Japonya ve İtalya'da ticareti yapılan bu sistemlerin kullanılması bazı uyuşturucu maddelerin, özellikle LSD'nin kullanılmasıyla karşılaştırıldı.

---

5 Robotların, en azından kuramsal bir açıdan, sırf modern bilimsel düşüncenin bir oluşumu olmadığını hatırlatmak isterim. Zaten İlyada da robotlardan söz edilmekteydi. Homeros XVIII. bölümde Ateş Tanrısı'nın (Vulcanus) hoş "bodyguardlar" olarak tanımlayabileceklerimizin eşliğinde görkemle yürüdüğünü söylüyordu ..."sağda ve solda korkunç efendilerinin adımını takip eden belirsiz şekil ve görünümlü hizmetçiler, hepsi altından ve canlı genç kadınlara benzer, büyük yaratan yüreklerine ses ve hayat ve akıl ve zanaat gücü vermişti, Gök Tanrıları'ndan sağduyu öğrenmişlerdi. Efendilerinin yanında çevik bir şekilde yürüyorlardı...".
Eski yahudi geleneğinde insana benzer kil makinası -Tevratın yorumlanmasına göre- Yahudi halkını korumakla görevli fantastik oluşum Golem'le robot fikri yeniden ele alınmıştır.

6 Bilimsel polis uzmanları, ENEA ile işbirliği yaparak bir suikast olayının canlandırılması için yeni bir teknik üzerinde çalışmaktadırlar. Olayı özel bir fotograf makinesi çekmemekte; stereo kamera, bir kompütür sayesinde mekanları üç boyutlu olarak canlandırmaktadır. Yollar, köprüler, geçitler, binalar bir virtuel gerçek oyununda olduğu gibi geometrik şekillerle canlandırılmışlardır. Bu konuda bakınız Polizia moderna, n. 2, Aralık 1993.

7 H. Rheingold İngiliz medyasının seçkin dergisi Lancet'in Ağustos 1991 sayısındaki " *Essere o credere:etica per la realta virtuale"* başlıklı makaleden söz ediyor. Bu makalede virtuel gerçeğin kullanılması psikolojik bir araç olarak gözler önüne seriliyor ve vituel gerçeğin kullanılması en azından önemli üç etik sorusunu getirdiği ileri sürülüyor ve bunlar 1) gerçek hava hücumlarıyla videoyunlar arasındaki farkı anlaşılmaz hale getiren virtuel çetenin etiği hangisidir?; 2) gerçeğe kim sahip olacaktır, onu kim kontrol edecektir, oraya kim girebilecektir?; 3) toplumun görüşlerini ve idealarını değiştirmek için virtuel gerçek teknolojisinin kullanılmasında var olan etik problemler hangileridir? (*La realta virtuale*, Bologna, 1993, 6-7).

Araştırmacılar (Kruger, op. cit., 258) suistimallerin ve hataların olacağını öngörüyorlar ve totaliter bir toplumda bireyin düşünsel bir dünyada hapsolabileceği ve önlenemez yani mecburi deneyler aracılığıyla beyni yıkanabileceğini ileri sürüyorlar. Biz de katiller tarikatının başkanı, esrarengiz dağ yaşlısının[8] sistemlerini teknolojik açıdan geliştirerek mecburi cehennem ve cennetler yaratılabileceğini ekleyelim. Son olarak Japonya, Tokyo'da Ask Kodamsha Company gibi bazı şirketler Video-Uyuşturucuyu piyasaya sürdüler, son ürünlerden birinin adı Video-Tanrı, insanüstü olayları ve gökyüzü görüntüleri sağlamaktadır. Yasal video-uyuşturucuya sahip olacak mıyız? Bu tip bir teknolojinin kullanılması uyuşturucuları ve buna ilişkin suçları azaltabilecek midir?

Sanal pornonun kullanılması cinsel suçları azaltacak mıdır? Virtuel gerçeklerin yapımı ve/veya ticareti için özel hükümler öngörülmeli midir? Bu sanal gerçeklerin kullanılmasına karşı küçüklerin korunması için tedbirler öngörülmeli midir?

Virtuel gerçeklerin kullanılması genel ve siyasi suç organizasyonları tarafından gerek katillerin formasyonu ve eğitiminde gerek suikastçıların hazırlanmasında kullanılabilir[9].

Sanal gerçeklerin sonucunda hukuki boşlukları engellemek için yeni olaylar hakkında multidisipliner bir yaklaşımla araştırmalar ve çalışmalar yapmak gerekir.

2- CEZA KANUNU VE CEZA USUL KANUNUN TAMAMLANMASI VE YAPILAN DEĞİŞİKLİKLER: 547/93 SAYILI KANUNUN ANALİZİ VE YORUMU

2.1- Öncelikle bugüne kadar bilişim suçlarıyla mücadele konusunda özel kanun yapan hiç bir ülkede ve uluslararası boyutta bile bilişim suçlarının tanımı yapılamadığını söylemek gerekir.

Yapılan hareketlerin heterojenliği nedeniyle daha çok kriminolojik açıdan yaklaşıldı ve hareketleri sayma yoluna gidildi; bu konuya önceki yazılarımda değinmiştim. Özellikle Kara Avrupası hukuku devletleri cezacıları, özel hayatın gizliliğini tehdit eden davranışlardan yola çıkarak bilişim suçlarının değişik tiplerine geleneksel hukuk normlarının uygulanabileceğini göstermek için bilişim suçlarını incelemeye başladılar.

Bu yeni fenomenlere eldeki normların uyarlanması kolay gözükmediğinden kanunkoyucular, kişisel bilgilerin korunmasıyla birlikte yavaş yavaş, diğer alanlar için de

8 Bilindiği gibi (bakınız Enciclopedia Treccani, voce Assassini) Dağın yaşlısı, seçtiği gençleri uyuşturduktan sonra cennette olduklarını inanmalarını sağlayarak Tanrı'nın bütün güzellikleriyle ve çok güzel kadınlarla dolu zevk bahçesine kapatıyor. Onları yeniden uyuşturduktan sonra cennetin dışına çıkarıyor ve cennete yeniden erişmek için onun buyurduğu her işte hayatlarını feda etmek zorunda olduklarını söylüyor.

9 Basın haberlerine göre Körfez savaşı operasyonlarında bazı Amerikalı pilotlar diğer meslekdaşlarına göre daha kontrollü ve onları geride bırakan hareketler sergilediler. Pilotlar görevlerini önceden virtuel gerçek tekniğinden yararlanılan eğitim programlarında gerçekleştirmişlerdi (bakınız Focus dergisi, Nisan 1994, 62). Böylece söz konusu teknikle eğitilmiş katiller normal suçlulara göre daha tehlikeli olacaktır.

(mülkiyetin, kamu güveninin vs...korunması) özel ceza normları düzenlediler. Birçok ülkede bilişim cihazlarının gelişiminin kriminojen bir alan yarattığı gözlendi ve geleneksel hukuk normlarının bu yeni suç fenomenini karşılamaya yetersiz olduğu biliniyordu ve bu kanunkoyucuları özel kanun reformları yapmaya zorladı. Bazı hukukçular ise hukuk sisteminin eksizsiz olduğunu düşündüklerinden reformu önlemeye çalıştılar. Onlara göre eldeki normlar, özellikle mülkiyetin, kamu güveninin korunmasına ilişkin normlar, teknolojinin getirdiği yeni suçları önlemek için yeterliydi. İtalya'da bu doktrinel eğilim kimi zaman bir içtihatla da kabul edilmiştir: hırsızlık, nası ızrar, ihkakı hak konusundaki ceza normları, yeni hukuka aykırılıklara uygulamaya çalışılırken, kanunilik ve ceza hukukunda kıyas yasağı prensibine aykırı olarak plastik hukuk cerrahlığı yapılmıştır.

Dönemin Adalet Bakanı Giuliano Vassalli,1989 yılında başkanlığını Ceza İşleri Genel Müdürü Dr. Piero Calla'nın yaptığı bir Bakanlık Komisyonu kurdu. Hakimler, bilişim uzmanları, akademisyenlerden oluşan bu komisyon bilişim suçlarıyla mücadele etmek amacıyla ceza kanunlarını değiştirmek veya tamamlamak için kanun tasarısının bir taslağını hazırlamakla görevliydi.

Kanun tasarısının taslağı 1991 yılının ilk aylarında metni yeniden incelemekle görevli dönemin Bakanlığına teslim edildi. Ancak bürokratların özensizliği nedeniyle testin incelenmesi 1992 Kasıma kadar uzayarak dönemin Bakanına kesin metin sunuldu ancak çekmece bekledi. Sonraki Adalet Bakanı Prof. Giovanni Conso'nun taslağı alarak önce Bakanlar Kuruluna sonra Parlamentoya sunması gerekti.

Kanun tasarısı önce Senatoya sunuldu ve sonra özel hayatın korunmasıyla birarayа getirilmesi için Meclise sunuldu. Meclis 1993 Temmuzda söz konusu tasarıyı kabul etti ve onu Ağustos ayının başında Senatoya sundu. 14 Aralık 1993'teki oturumda test, kabul edildi ve 23 Aralık 1993 tarihli 547 sayılı yasa haline geldi.

2.2- Bilişim suçlarını engellemek için geleneksel ceza kanunlarını incelemek gerekmektedir. Bilişim sistemine hukuka aykırı olarak girilmesi, verilerin, bilgilerin ve programların çalınması, değiştirilmesi, tahrip edilmesi, bilişim sistemlerinin işlemesinin engellenmesi, bilişim iletişimine hukuka aykırı olarak girme, bilişim casusluğu, bilişim dolandırıcılığı, bilişim araçlarının hukuka aykırı kullanılması vs... öngörmek ve engellemek söz konusudur. Sonuç olarak, sanayileşmiş ülkelerde büyük ölçüde yeni hukuk normları getirildi. Böylece bilişim sahteciliği Fransa, Almanya, Portekiz, Finlandiya, Lüksemburg, Avustralyanın güneyindeki ülkelerde ve dolaylı olarak Kanada, Yunanistan ve Japonya'da düzenlenmiştir. Bilişim tahribatı Avusturya, Kanada, Fransa, Almanya, İsveç, Finlandiya, Portekiz, Belçika, Lüksemburg, Güney Ülkelerinde ve İrlanda'da cezalandırılmıştır. Bilişim sabotajı, engellemesi Kanada, Danimarka, Fransa, Almanya, Norveç, Yunanistan, İngiltere, Portekiz, Lüksemburg ve Avustralya'da düzenlenmiştir. Bilişim dolandırıcılığı altı ülkede öngörülmüştür: Avusturya, Danimarka, Norveç, Almanya, İsveç ve Finlandiya. Bilişim casusluğu Yunanistan, Almanya, Finlandiya ve Fransa'da cezalandırılmıştır.

Suç politikası açısından en büyük problem sisteme hukuka aykırı girmenin cezalandırılmasıdır: bilişim suçlarına karşı özel normları olan ülkelerin büyük çoğunluğu bu tip bir yol izledi. Hukuka aykırı girme Danimarka, Fransa, Yunanistan, İngiltere, Portekiz. Norveç, İsveç, Güney Ülkeler, Lüksemburg, İrlanda, Avustralya'da tam olarak engellendi. Bunlara değişik özellikte olan Amerika'yı da eklemek gerekir.

Bir bilgisayarın fonksiyonlarına yetkisiz girme Kanada, Amerika, Portekiz ve Güney Ülkelerinde öngörülmüştür; bilgisayar kullanma hırsızlığı Kanada, Norveç, Finlandiya'da cezalandırılmıştır.

Bilişim ceza hukukunun en büyük problemlerinden biri, verilerin, bilgilerin ve programların çalınmasını özel normlarla engellemektir.

Özellikle İtalya, Fransa ve Almanya'da hakim olan görüşe göre bilişim şeyleri kuramsal açıdan bile ne cismi şeylerle ne de enerjiyle özdeşleştirilebilirler.

Bu kuramsal imkansızlık, sözü edilen bilişim şeylerinin taşınabilir şeyler gibi çalınmaya, elden alınmaya, yani bir mülkiyetten başka birine geçirilmeye uygun olmamasından ileri gelir; bu sebepten, mülkiyeti korumaya yönelik ceza normları bunlara uygulanamaz. Bir bilgiye sahip olma o bilgiyi bilme ile gerçekleşir: şu halde sahiplenme sırf bilme ile gerçekleşir. Yürürlükteki ceza kanunun hazırlık çalışmaları hırsızlık için, başkasının taşınabilir şeyinin elde edilmesi gerektiğini, enerjiye gelince, bunların yalnızca kendi yararına veya başkasının zararına kullanılabilecek durumda olduğunda, taşınabilir şeyler sayılabileceğini belirtmektedir. Sonuç olarak doktrinin çoğunluğuna göre istisnai olarak, bilgiler, veriler ve programlar sui generis de olsa mülkiyet hakkının konusu olabilirler. Bu halde koruma, mülkiyeti yani fikir ve sanat mülkiyetini, endüstiyel veya bilimsel veya ticari sırları korumaya yönelik olanlardan başka normlar tarafından sağlanır.

Fikri buluşlarla enerji, özellikle elektrik enerjisi arasında yapılmaya çalışılmış da olsa ciddi bir karşılaştırma yapılamaz. Enerji, ölçülebilir ve sahip olunmaya uygundur, fizikseldir. Amerikalılar bu tartışıldığında "Elektrik enerjisinin fiziksel olup olmadığını araştırmak istiyorsanız parmaklarınızı elektrik prizine sokun" derler.

Bu sebepten bilişim suçlarını engellemeye yönelik kanunu olan ülkelerde bilişim şeyleri hırsızlığını öngören ve cezalandıran bir norm yoktur.

Verilerin veya bilgilerin veya programların hukuka aykırı olarak bilinmesini önlemenin dolaylı yolu, yetkisiz girmeyi cezalandıran bir normun düzenlenmesidir. Bu, birçok ülke tarafından tercih edilen bir yoldur.

3- HÜKÜMLERİN İNCELENMESİ

547/93 sayılı kanun hükümlerini kısaca yorumlayalım.

3.1- Ceza Kanunu'nun 392. maddesi

Kanun taslağındaki rapora göre 392. maddeye ikinci bir fıkra eklendi ve böylece şeyler üzerinde cebir şiddet hukuksal kavramı, bilişim veya telematik programlarına veya bir sistemin çalışmasına ilişkin bir takım hareketlere cebir şiddet olarak genişletilerek, teknolojik cebir şiddet kavramı getirildi.

Bu genişletmenin mantığı, kuşkusuz toplumsal sonuçları olan hareketleri yaptırımdan yoksun bırakmamakta aranmalıdır ve bu hareketler en azından kuramsal açıdan tahrip veya amacını değiştirme hallerine benzer görünmektedirler.

Söz konusu raporda görüldüğü gibi hakim önünde geçerli olabilecek haklar kullanmak amacıyla bilişim programlarını değiştirme veya kısmen de olsa işe yaramaz hale getirme, ve bu sayede failce başkasının yararlanabileceği programda hak ileri sürme veya bilişim veya telematik sistemlerinin işlemesini engelleme veya değiştirme (yanlış biçimde işlemesini sağlama) söz konusu ve bunlar nedeniyle bir çeşit kendini korumaya yani c.p. 392. maddedeki normun önlemek istediği kendini haklı göstermeye başvurulmaktadır[10].

Şeyler üzerinde cebir şiddetin yeni tanımı programlara ve bilişim sistemlerine ilişkindir: hüküm, sözleşmedeki sürelere karşılık gelen ödemeyi dolaylı olarak sağlamak için programın sahibi-kiralayanı tarafından gizlice virüs veya mantık bombası bağlanmasını engellemeyi amaçlamaktadır.

Söz konusu suç sulh ceza mahkemesinin yetkisindedir.

3.2- Ceza Kanununun 420. maddesi

Kanunkoyucu 420. maddenin korumasını (gerek suçun basit halinde gerek ağırlaşmış halinde) bilişim veya telematik sistemlerine, verilere, bilgilere veya bunlarda bulunan programlara genişletmek istemiştir.

Söz konusu suç, kalkışma suçu veya peşinen tamamlanmış suç olarak oluşturulmuştur. Suç, zarar vermeye veya tahrip etmeye yönelen hareketin yapılmasıyla tamamlanır.

Yürürlükteki 420. maddenin birinci fıkrasındaki kamu yararı tesislerine göre verilerin araştırılması veya hazırlanması tesislerinin alternatif belirtilmesi nedeniyle -bilindiği gibi- kararsızlık oluştuğundan normun yeni şekliyle suçun maddi konusunun kesin tespiti amaçlanmıştır.

Hakim doktrine göre verilerin işlenmesi ve araştırılması tesisatını tehlikeye sokma 420. maddedeki suçun oluşabilmesi için önemli olabilir. Bu tesisat özel şahıslara ait

---

10 Bilişim sistemleri sağlanan bir şirketin görevlisi ve aynı şirket tarafından kullanılan programların yapımcısı çalışma şartlarından memnun olmayarak ve programlara ilişkin haklarını arttırarak 392. maddenin 2. fıkrasındaki fiili işlerse ne olacak?

olsa da ve özel amaçlara tahsis edilmiş olsa da onları tahrip etmeye yönelik bir hareket toplum için önemsiz olamayacağından sosyal önemi vardır. Bu komisyon tarafından izlenilen yoldur oysaki komisyon bütün yanlışlıkları kökten kaldıracak şekilde, birinci fıkradan verilerin araştırılması ve hazırlanması tesislerine ilişkin kısmın çıkarılması gerektiği görüşündeydi: birinci halde suç, yalnızca kamu ihtiyacını karşılama amacına yönelen tesislere yani yapı, cihaz, aygıt vb. komplekslerine saldırmakla sınırlanmış oluyordu.

İkinci fıkraya geçersek, özel bir suç eklendi: birinci fıkradaki fiilin aynısı yani bilişim veya telematik sistemini veya verileri, bilgileri veya onlarda bulunan programları zarar vermeye veya tahrip etmeye yönelik hareket birinci fıkradaki cezayla cezalandırılmakta; ikinci halde de tasarı kamuya veya özel şahıslara ait sistemler, veriler, vs..söz konusu olması gerektiğini saptamaktadır. Kamu düzeni veya toplumun sosyo-ekonomik menfaatleri için doğrudan tehlike kaynağı olarak önemlidirler.

Üçüncü fıkrada (kalkışma hareketinden) gerek tesisata zarar verilmesi veya tahrip edilmesi veya işlemesine kısmen de olsa engel olunması, gerekse bilişim veya telematik sistemlerine veya verilere, bilgilere veya onlarda bulunan programlara karşı aynı sonuçların yapılması suçun ağırlaşmış halini öngörmektedir.

Suçun basit şekli sulh ceza mahkemesinin, ağırlaşmış hali ise asliye ceza mahkemesinin yetkisine girmektedir.

3.3- 491bis maddesi

Ceza Kanununun 2. kitabının, 2. babının, 3. fasılına bilişim sahteciliği yani bilişim belgelerinde sahtecilik eklenmiştir. Norm bilişim belgesinin hukuksal kavramını da kapsamaktadır.

Rapor bunun kanuna göre bilgisayarın eseri sayılmaması gerektiğini ve c.p. 476 ve devamı maddelerinde düzenlenen kağıt belgelere girdiğini ileri sürmektedir. Artık içtihatta da mekanik imzanın elle atılan imzayla bir tutulması gerektiği kabul edilmektedir.

Kanunkoyucu hangi tür olursa olsun veri, bilgi veya program içeren bütün desteklere bilişim belgesi niteliği verme fikrindeydi. Raporda belirtildiği gibi bu belgelerin menşeini saptama problemi olacaktır, bilindiği gibi sahtecilik için suç konusu belgenin onu yapan kişiye veya kuruluşa dayandırılabilmesi vazgeçilemez bir şarttır: "failin teşhisi". Bu açıdan Bakanlık Komisyonu problemin çözümünü, kamusal veya özel alanda belgenin niteliğine veya etkili olması gerekeceği konuya göre kabul ettirilebilineceği disiplinine koymayı tercih etti. Raporda görüldüğü üzere bilişim desteğinin suçun konusunu oluşturabileceği mutlak koşulu onda bulunan verilerin kullanılması ve ispata etkisi veya aynı desteğe kaydedilen programların bilgisayarda kullanılmasına karşıdır. Tasarıya göre bu koşul kamu güveni için zarar veya tehlike yaratmaya uygun belgelerde sahtecilik ile korunan menfaate göre tamamen zararsız olan ve ceza yaptırımı uygulanmasını

haklı göstermeyen, ispat değeri de olmayan belgelerde sahtecilik arasındaki değişken unsuru oluşturur.

Kanunkoyucu sonuç olarak bilişim belgesiyle ilgili hallere belgelerde sahtecilik hakkındaki hükümlerin uygulanmasını hükmederek bu hükümlere atıf yapmayı tercih etti. Böylece iki amaca birden ulaşıldı: yalnızca maddi konunun farklı olması nedeniyle suç tipinin yapısını değiştirmemek ve hukuksal konu veya ihlal edilen menfaatin niteliği açısından farkı olmayan suçların aynı yaptırım rejimine tabi olması.

Yetki konusunda c.p. 477, 478, 482, 485, 489, 490.maddeleri gözönünde tutmak gerekir.

3.4- 615ter maddesi

Madde bilişim veya telematik sistemine hukuka aykırı girme veya hak sahibinin açık veya rızası hilafına sisteme devam etmeyi cezalandırmaktadır.

Raporda görüldüğü üzere, norm konut dokunulmazlığına karşı suçlar arasında yer almaktadır; çünkü bilişim veya telematik sistemleri Anayasa'nın 14. maddesince güvence altına alınan ve daha önemli hallerde ceza kanununun 614. ve 615. maddelerince korunan ilgili kişiye ait saygı alanını düşünsel olarak genişletmiştir.

Koruma, güvenlik tedbirleriyle korunan bilişim veya telematik sistemleriyle sınırlıdır; özel bir sujenin hakkını korumak gerektiğinden, raporda ileri sürdüğü gibi, sujenin bilimsel ve fiziksel koruma araçlarının hazırlanmasıyla sisteme girme ve sistemde kalmayı yalnızca kendisi tarafından yetkilendirilen kişilere bırakmak istediğini göstermesi gerekir.

Söz konusu madde gerçekte bilişim ceza hukukunun en büyük problemlerinden biriyle karşılaşmaktadır. Geçmişte kanunkoyucular kötü niyet olmaksızın yani yalnızca bilgi edinmek amacıyla hukuka aykırı araçlara başvurarak (hacking) bir sisteme girmenin ceza hukukunda dikkate değer bir fiil oluşturmadığı görüşünden etkilenmişlerdir. Kamuoyunun şu ana kadar hacker'lara karşı oldukça hoşgörülü olduğunu, onları canlı hayatı seven, eğlence amacıyla hareket eden kişiler, suçlu gençler yerine uyanık gençler olarak kabul ettiğini söylemek gerekir. Öte yandan hackers "bilgi güçtür" sloganıyla bilgi kaynaklarına herhangi bir sınırlama olmaksızın girme hakları olduğunu ileri sürerek her şekilde hareketlerini rasyonelleştirmeye çalıştılar.

Sonuç olarak kamuoyunun bu eğilimi söz konusu hareketin cezalandırılmasını geciktirdi ya da zorlaştırdı. İlahi intikamdan mı dır bu normun getirilmesini reddeden ülkelerden biri olan Almanya kendi içinde, gerçekten çok tehlikeli olan "Caos Computer Club" denen hackers birliğinin oluştuğunu gördü. İşe bakın ki, hackerlar tarafından bilişim sistemlerine virüs sokulmasıyla yapılan bilişim ağlarına en büyük sızmalar ve en büyük tahripler Almanya'nın ta kendisinden başladı.

Yetkisiz girme Avrupa Konseyince hazırlanan en son tavsiye kararına eklenen "Guidelinees"da (s. 89 (R) 9) da öngörülmüştür. Bununla Konsey hükümetlere bilişim sistemine yetkisiz girmeyi öngörme ve cezalandırmayı tavsiye etmiştir.

Kanunun metnine dönecek olursak, üç özel ağırlaştırıcı sebep (420 madde de) öngörülmüştür, bunlardan ikincisi netice sebebiyle ağırlaşmış suçtur.

Suçun basit hali, sulh ceza mahkemesinin, ağırlaşmış haller ise asliye ceza mahkemesinin yetkisindedir.

3.5- 615quater maddesi

615quater maddesi, güvenlik sistemleriyle (615ter maddesinde kullanılan anlamda) korunan bilişim veya telematik sistemlerine girme kodlarını herhangi bir şekilde (bağımsız bilgisayar aracılığıyla da) hukuka aykırı olarak elde etme ve yaymayı cezalandırmaktadır.

Söz konusu suç için özel kast aranmıştır ki, bu da, kendisine veya başkalarına yarar sağlamak veya başkalarına zarar vermek amacıdır.

Bilişim veya telematik sistemine hileyle veya her ne olursa olsun hukuka aykırı olarak girme kodlarının, anahtar kelimelerinin veya diğer uygun araçların yapılması, bildirilmesi, verilmesi veya aynı amaca uygun işaret veya bilgilerin sağlanması önceki hallerle bir tutulmuştur. Bu öngörme, birinci fıkrada belirtilen cihazların veya araçların lisans olmadan üretimi, ihracı, satın alınması, satılması, taşınması kiralanmasına ilişkin 8.4.1974 tarihli 98 sayılı kanunun 9. maddesinin üçüncü fıkrasındakiyle bir anlamda benzerdir.

Söz konusu suç sulh ceza mahkemesinin yetkisindedir.

3.6- 615quinques maddesi[11]

Norm kendisi veya başkası tarafından yazılarak bir bilişim veya telematik sistemine, bunda bulunan veya buna ilişkin verilere veya programlara zarar verme veya sistemin işlemesini tamamen veya kısmen engelleme veya bozma amaçlanarak veya bunları sonuç olarak gerçekleştirerek bilişim programını bildiren veya veren kişinin hareketini cezalandırmaktadır.

Ulusal veya uluslararası düzeyde çok ağır bir şekilde bir bilişim sistemine zarar verebilecek yollardan biri, virüslerin yani sistemi bloke eden hatta verileri, tahrip eden

---

11 Bu konuda iki ayrı durum düşünülür. Birincisi, üçüncü kişilere verilecek programda belirli koşullarda sistemin işlemesini bozabilecek büyük hataların bulunduğunu bilmesine rağmen ürünü bu şekilde veren software üreticisinin hareketine ilişkindir. Zararlı neticenin gerçekleşmesinin hukuki sonucu nedir? Muhtemel kast hali söz konusu olur mu? İkincisi, çalışma veya önleme amacıyla yani antivirüs programları yapmak için virüs programlarını başkalarına verenin hareketine ilişkindir. Suçun varlığı için kast arandığı için bu halde fiilin suç oluşturmaması gerekir. Bu halde c.p. 51. maddedeki hukuka uygunluk sebebine başvurulabilir. Hiç kuşkusuz yalnızca "virüs programları" elde etme veya kopyalama halinde kastın varlığını" ispatlamak çok zor olacaktır. Çalışma veya önleme araçlarının hazırlanması nedeniyle "virüs programları elde eden ve/veya saklayan kişinin yukarıdaki suçu işleyeceğini düşünmüyorum.

veya hard-diske zarar veren programların sokulmasıdır. "Virüs" hakkında söylenecek çok şey vardır; ancak burada bunu yapmak için zaman yoktur. Bilişim alanında hukuka aykırı hareketlere ilişkin olarak İtalya'da da "kötü örnekler" oldu, terörizm zamanında dendiği gibi belki bunlar üzerine dikkat çekmek gerekir. Torino'da ünlü bir politeknik profesörü bir gazetedeki (Stampa Sera) röportajında kurumun bigisayarlarına da bulaşan "virüsler" hakkında "korsanlar"a hayran olduğunu açıkladı, öğrencilerinden bazılarının "sebatlı çalışmayla" yaklaşık 100 milyon değerindeki programa uygun korumaları atlayarak bunları ele geçirdiğine değindi ve söz konusu "korsanlar"a ilişkin olarak "... bunlar saptansa da cezalandırılmaları çok zor olacaktır; hocalarından daha başarılı olduklarını gösteren öğrenciler cezalandırılamazlar" sonucuna vardı. Hocaların suçu övmemeleri gerektiğini hatırlamak kolay olabilir...

Tanınmış yazar ve gazeteci Nantas Salvalaggio 1989'da bir magazin dergisinde (Oggi) "Li voglio tutti malati da virus questi computer tanto invadenti" "Bütün bilgisayarlara virüs bulaşmasını istiyorum" başlıklı bir makalesinde "itiraf ediyorum: bilgisayarların belleklerine çok tehlikeli elektronik basillerle bulaşan gizemli bilişim bozguncularına hayranım. Hayatımın bir diskete dönüşmemesi için özgürlüğün romantik şövalyelerine güveniyorum" dedi.

Bu davranışlar karşısında, adli polis başkanı Dr. W. Paul 1989'un 5/6 sayılı RDU'da yayınlanan bir makalede "Bullettin Boards"da (elektronik gazeteler) gerçekleşen "virüs" programlarının açıkça reklamının yapılmasına değindi: "Bu durum, bütün oyuncak ve eğlence dükkanlarında avlanmamak güvencesiyle patlayıcı silahların yapımı bilgilerini serbestçe elde edebilme imkanı olmasıyla bir tutulabilir" dedi. Ve ekledi: "Sabotaj programları suç aracı olarak çok gürültülü değiller, ama bu yüzden patlayıcı silahtan daha az tehlikeli değiller"...

Şimdi söz konusu maddeye dönersek, Callà komisyonunun hazırladığı metinde bulunmayan madde Kanunlaştırma Bürosu tarafından eklendi. Kesin metni hazırlayanlara göre pratikte çok tehlikeli olan virüs programlarından birini kasten yayan kişinin harekatini de engellemek gerektiği ortaya çıktı.

Bilişim sistemlerine "virüs programları"nın girmesi sonucu oluşan zararlardan kesin olarak koruma zorunluluğu taksirli hareketi engellemeyi gerektirdi ama bu değişiklik hakkında Kanunlaştırma Bürosu'nda karasızlıklar saptandı.

Söz konusu suç için genel kast aranır ve sulh ceza mahkemesi yetkilidir.

3.7- 616. madde

Haberleşmenin ihlali, çalınması ve ortadan kaldırılmasına ilişkin 616. madde de kanunkoyucunun dikkatini çekmiştir. Söz konusu maddenin dördüncü fıkrası bilişim ve telematik haberleşme kavramını genişletmek amacıyla değiştirilmiştir.

Bu öngörme telefax, telex, videokonferans sistemlerini vb. de kapsamaktadır.

Suç sulh ceza mahkemesinin yetkisindedir.

3.8- 617quater - quinques - sexies

Yürürlükteki ceza kanununa 617quater, 617quinques ve 617sexies maddeleri eklenmiştir.

617 quater bilişim ve telematik haberleşmelerinin hukuka aykırı olarak dinleme, engelleme veya araya girmeye ilişkindir. Söz konusu haberleşmelerin içeriğini herhangi bir kitle iletişim aracıyla ifşa edenin fiili de gözönünde tutulmuştur. Suç şikayet üzerine koğuşturulabilir, ancak özel ağırlaştırıcı sebepler varsa re'sen koğuşturulabilir.

Söz konusu ağırlaştırıcı sebepler şunlardır:

1) Devlet veya kamu kurumu veya kamu hizmetini veya kamu yararını gerçekleştiren şirket tarafından kullanılan bilişim veya telematik sistemi zararına;

2) Bir memur veya kamu hizmeti gören kimse tarafından görevine veya hizmetine ilişkin yetkilerini kötüye kullanarak yahut görevine veya hizmetine ilişkin yükümlülüklerine aykırı davranarak veya sistem operatörlüğü sıfatını kötüye kullanarak ;

3) Özel dedektiflik mesleğini kötüye kullananarak işlenmişse.

Suç sulh ceza mahkemesinin yetkisindedir.

617quinques maddesi bilişim veya telematik sistemine veya birden fazla sistem arasında geçişlere ilişkin haberleşmeleri dinlemeye, engellemeye veya araya girmeye elverişli cihazları yerleştirmeyi cezalandırmaktadır. Hareketin tehlikeliliğinden dolayı re'sen koğuşturulması öngörülmüştür.

617quater maddesinde belirtilenlerle aynı ağırlaştırıcı sebepler öngörülmüştür.

Suçun basit hali sulh ceza mahkemesinin, ağırlaşmış hali asliye ceza mahkemesinin yetkisindedir.

617sexies maddesi bilişim veya telematik haberleşmelerinin içeriğini değiştirme, bozma veya yok etmeyi öngörmüştür. Ancak kendisine veya başkasına bir yarar sağlamak veya başkalarına zarar vermek amacı gerektiğinden, özel kast aranır. Suç, bir bilişim veya telematik sistemine veya birden fazla sistem arasında geçişlere ilişkin haberleşmelerden birinin içeriği tesadüfen dinlenilmiş de olsa tamamen veya kısmen değiştirerek veya bozarak veya yok ederek onu kullandığında veya başkasının kullanmasına izin verildiğinde oluşmaktadır

Bu suç için de 617quater maddesindeki ağırlaştırıcı sebepler öngörülmüştür.

Suçun basit hali sulh ceza mahkemesinin, ağırlaşmış hali asliye ceza mahkemesinin yetkisindedir.

3.9- 620 - 621 - 623 maddeleri

620. maddenin gizli belgelerin ifşasına ilişkin birinci fıkrasıyla ikinci fıkrası arasına, birinci fıkradaki hali veriler, bilgiler ve programlar içeren herhangi bir bilişim desteğine genişleten yeni bir fıkra eklendi. Ticari ve endüstriyel sır oluşturan verilerin, bilgilerin veya programların hukuka aykırı olarak elde edilmesinin suç olması gerektiğini düşünerek, bilimsel sırların ifşasına ilişkin 623. maddeye, ticari sır kavramının eklenmesini komisyon üyesi sıfatıyla teklif etmiştim. Ancak komisyonun çoğunluğu aynı fikirde olmadığından madde değiştirilmedi.

Telgraf veya telefon haberleşme ve konuşmalarına ilişkin, "Diğer haberleşme ve konuşmalar" başlıklı 623bis maddesi değiştirildi:maddeye "bilişim veya telematik haberleşmeleri" ara tümcesi eklendi ve tel veya dalgalar üzerinden yayınlara ilişkin kısım çıkarıldı. Maddeyi hazırlayan kişi 622. maddenin zinciri olarak ve bilişim casusuluğunu[12] engellemek için bilişim alanında meslek sırrının ifşasına ilişkin 622bis maddesi eklenmesini de teklif etmişti. Ancak bu teklif de komisyon tarafından kabul edilmediğinden Bakanlığın Kanunlaştırma Bürosuna verilen metne eklenmedi.

3.10- 635bis maddesi

Bilişim ve telematik sistemlerine ilişkin özel tahrip halinin ceza kanununa eklenmesi çok önemlidir. 635bis maddesi başkasına ait bilişim veya telematik sistemlerini veya başkalarına ait programları, bilgileri veya verileri tahrip eden veya bozan yahut tamamen veya kısmen kullanılamaz hale getiren kimsenin halini öngörmektedir.

Raporda söylediğim gibi, 635. maddedeki genel tahrip suçuna göre özel bir hükümdür. Söz konusu hal ile 420. maddedeki hal arasındaki özellikle peşinen tamamlanmış suçlardaki ilişki değişmemektedir. Tahrip suçunun netice suçu olduğu da bilinmektedir.

Hareketin tehlikeliliği ve neticenin etkenliğinin artması nedeniyle suçun basit halinde bile söz konusu suç re'sen koğuşturulabilir. 635. maddenin ikinci fıkrasındaki

---

12 Maddenin taslağı şu şekildeydi: 622bis-Bilişim meslek sırrının elde edilmesi ve ifşası:
a) Endüstriyel, bilimsel veya ticari sır oluşturan bir bilişim programını durumu veya görevi veya mesleği veya sanatı nedeniyle bilen kişi onu ifşa eder veya kendisinin veya başkasının yararına kullanırsa iki yıla kadar hapis cezası ile cezalandırılır.
b) Suça iştirak hali dışında önceki fıkradaki programlara ilişkin bilgileri elde eden kişi kendisine veya başkalarına bir yarar sağlamak amacıyla yukardaki programlardan birini kabul eden satın alan veya saklayan veya her ne suretle olursa olsun bunları kabul etmek veya satın almak veya saklamak hususlarında aracılık eden kişi bir yıla kadar hapis ve on milyona kadar para cezası ile cezalandırılır.
c) n. 1 ve 2'deki cürümler zarar gören kişinin şikayeti üzerine cezalandırılabilir.

şekilde veya fiil bir sistem operatörünün sıfatını kötüye kullanmasıyla işlenmişse ağırlaşacağı öngörülmüştür.

Söz konusu suç için sulh ceza mahkemesi yetkilidir[13].

381. maddenin 2. fıkrası değiştirilmediğinden bu halde suçüstü halinde (ihtiyari) yakalama imkanı kabul edilmemiştir.

3.11- 640bis

Dolandırıcılığın özel bir hali olan bilişim dolandırcılığının (640ter maddesi) getirilmiş olması da önemlidir.

Bilişim veya telematik sisteminin veya onunla ilgili bir sistemin (örneğin bir kütüphanede toplanmış olanları, ele geçirmek amacıyla olanları da) işlemesini bozma hareketi cezalandırılmıştır. Başkasının zararına haksız yarar elde edilmiş olması aranmıştır.

. 640. maddenin ikinci fıkrasının 1. numarasındaki veya bir sistem operatörü sıfatının kötüye kullanılmasına ilişkin ağırlaştırıcı sebepler öngörülmüştür.

Suçun basit hali zarar gören kişinin şikayeti üzerine koğuşturulur ve sulh ceza mahkemesinin yetkisindedir.

Ceza Usul Kanunu'nun 7. maddesinin 2. fıkrası değiştirilmediğinden ağırlaşmış hal yetki asliye ceza mahkemesinin yetkisindedir.

4 - CEZA USUL KANUNUNDAKİ DEĞİŞİKLİKLER

Ceza Kanunu için öngörülen değişikliklerle uyum sağlamak ve Yargı Otoritesinin bilişim veya telematik sistemlerine veya birçok sistem arasında geçişlere ilişkin haberleşme akımının meşru olarak dinlenmesini kabul etmek gerektiği dikkate alındığında, dinleme konusundaki usul normlarının da tamamlanması veya değiştirilmesi gerekliydi. Ceza Usul Kanunu'nun 266. maddesinden sonra aşağıdaki metnin eklenmesi öngörülmüştür:

266bis maddesi - Bilişim veya telematik sistemlerinin dinlenmesi

266. maddede belirtilen suçlarla bilişim veya telematik teknolojisinin kullanılması yoluyla işlenilen suçlara ilişkin yargılamalarda bilişim veya telematik sistemlerini veya birçok sistem arasında geçişlere ilişkin haberleşme akımının dinlenmesi kabul edilmiştir.

---

13 Ağırlaştırmanın mantığı sistem operatörlüğü yapan kişinin suçun işlenmesinde "özel elverişlilik"e sahip olmasında ve bir yabancıya göre kolaylaşmasında aranmalıdır. Özel ağırlaştırıcı sebep c.p. 61 maddenin 11. numarasında öngörülenin zincirini oluşturur.

Ceza Usul Kanunu'nun 268. maddesi şu şekilde değiştirilmiştir:

İçüncü fıkradan sonra "bilişim veya telematik haberleşmeleri dinlendiğinde savcı operasyonların hususi şahıslara ait cihazlarla yapılmasına karar verebilir" diyen 3bis eklenmiştir.

6., 7. ve 8. fıkralar şu şekilde değiştirilmiştir:

6- Tarafların müdafilerine 4. ve 5. fıkralarda belirlenen süre içinde işlemleri inceleme ve kayıtları dinleme veya bilişim veya telematik haberleşme akımlarından bilgi alma hakları olduğu hemen bildirilir. Süre geçince hakim, taraflarca belirtilen bilişim veya telematik haberleşme akımlarının veya konuşmaların açıkça önemsiz oldukları ortaya çıkmayanların elde edilmesine hükmeder, kullanılması yasaklanan tutanakları ve kayıtları re'sen çıkarır. Savcının ve müdafiilerin çıkarmaya katılma hakları vardır ve en az 24 saat öncesinden haberdar edilirler.

7- Hakim bilirkişilik için öngörülen şekil ve garantilere uyularak kayıtların tamamen yazıya geçirilmesini veya bilişim veya telematik haberleşme akımlarında bulunan bilgilerin anlaşılabilir şekilde basımına hükmeder. Kayıtlar ve basımlar tartışma için dosyaya eklenir.

8- Müdafiler kayıtların fotokopisini çekebilirler ve kayıtları manyetik şerit üzerine geçirebilirler. Bilişim veya telematik haberleşme akımlarının dinlenmesinde müdafiler dinlenilen akımların uygun destek üzerine kopyesini veya 7. fıkrada öngörülen basımın kopyasını talep edebilirler.

266bis maddesini, değiştirilerek 7.8.1992 tarihli 356 sayılı kanuna dönüştürülen 8.6.1992 tarihli 306 sayılı kanun hükmünde kararnamenin 25ter maddesiyle birleştirmek gereklidir. Kanun tasarısının 13. maddesi, belirtilen kanun hükmünde kararnamenin 25ter maddesinin 1. fıkrasında "ve diğer telekomunikasyon şekilleri" sözcüklerinden sonra "veya bilişim veya telematik sistemlerine ilişkin komunikasyon akımı[14]" eklenmesini öngörmektedir.

DİĞER GİRİŞİMLER

1988'de zamanın Adalet Bakanı prof. Giuliano Vassalli, Bakanlığın Kanunlaştırma Bürosu nezdinde, başkanlığını prof. Antonio Pagliaro'nun yaptığı yalnızca akademisyenlerden (prof. Bricola, Mantovani, Padovani ve Fiorella) oluşan bir komisyon kurdu. Komisyona gerek genel kısım gerek özel kısım açısından yeni bir ceza kanunu çıkarılması için kanun tasarısını yönlendiren prensipleri ve kriterleri hazırlama görevi verildi.

---

14 C.P.P. 284. maddenin 2. fırkasında düzenlenen evde hapis halindeki emirler çerçevesinde hakim diğer kişilerle haberleşmeyi sağlayan telefon ağlarına bağlanan bilgisayar kullanma yasağına hükmedebilir. Bu halde aynı madenen 4. fıkrasındaki kontrolü gerçekleştirmek son derece zor olabileceğini söylemek gerekir.

1992'nin başında komisyon açıklamalı ve tek tek belirtilmiş bir tasarıyı dönemin Adalet Bakanı'na verdi. Daha sonra bu Documenti delle Giustizia dergisinin 1992 Mayıs tarihli 3. sayısında yayınlandı.

Daha önce açıklanan bilişim suçlarını engellemek için ceza kanununu tamamlama kanun tasarısını düzenlemekle görevli olan Calla' Komisyonu ile Pagliaro Komisyonu arasında resmi bir birleşme maalesef şu ana kadar olmadı.

Pagliaro Komisyonu haberleşme gizliliğine karşı suçlarda, çıkartma hakkına sahip bir kimsenin açık veya örtülü rızası hilafına bilişim sistemlerine hukuka aykırı olarak girme suçlarıyla ilgilendi. Örtülü rıza hilafına hali özellikle telematik haberleşmesine girme (76. madde n.6), hileyle elde etme, içeriğini ifşa, telematik haberleşmesini yok etme ve belirtilen haberleşmelerin kesilmesi ve dinlenmesine ilişkindir (76. madde n.2, 3, 4 ve 5) .

Bundan başka, bilişim veya otomatik araçlarından hileyle yararlanarak veya bunları kötüye kullanarak başkasının zararına olarak kendisine veya başkasına haksız bir yarar sağlama olan bilişim veya otomatik araçlarının kötüye kullanılması (83. madde n.4) ve belgelerde sahtecilik amacıyla bilişim verilerinin resmi veya özel evraklarla bir tutulması öngörülmüştür (93. madde n.3) .

Başkasının fikir eserinin hukuka aykırı olarak kopya edilmesi suçu bilişim programını da kapsayacak şekilde öngörülmüştür (83. madde n.10).

Taslak kanun tasarısı haline getirilmiş ancak hiçbir zaman Parlamentoya sunulmamıştır.