BİLİŞİM HUKUKU ULUSLARARASI UYUŞMAZLIKLAR

Ş. Cankat TAŞKIN*

GİRİŞ

Bilişim hukuku, niteliği gereği pek çok hukuk dalıyla bağlantılıdır.[1] Örneğin yazılımların korunması, kullanılması, bunlara ilişkin sözleşmeler ve ihlaller fikri mülkiyet hukukunun konusuna girerken; bilişim aracılığıyla işlenen suçlar, özel hayatın gizliliği, kişisel verilere karşı işlenen suçlar, banka veya kredi kartları aracılığıyla işlenen suçlar gibi konular ceza hukukunun; kamu kurum ve kuruluşlarında bilgisayarların kullanılmasına ilişkin sorunlar idare hukukunun; verilerin uluslararası kullanımından doğan sorunlar devletler hukukunun ve bilişim hukukundaki soruşturma, kovuşturma ve yargılama yöntemleri ise medeni usul hukuku ile ceza muhakemesi hukukunun kapsamına girmektedir.[2]

Bu çalışmamızda, kapsamı bu kadar geniş olan bir dalın yalnızca ceza ve ceza muhakemesi hukuku ile bağlantılı olan bölümünü incelenmiştir. Diğer hukuk dallarına, ise, yeri geldikçe yalnızca fikir vermesi anlamında kısaca değinilmiştir.

Çalışmamızın ilk bölümünde hukukumuzdaki bilişim suçları, karşılaştırmalı hukuka ve bu hukuk sistemlerindeki örnek yargı kararlarına da değinerek incelenmiştir. Son bölümde ise, bilişim suçlarının soruşturma ve kovuşturma yöntemleriyle, alınabilecek önlemler; 5651 Sayılı Kanun'la getirilen düzenlemeler, bunlara ilişkin görüş ve öneriler sunularak ders notları tamamlanmıştır.

---

* Av., Bursa Barosu.

1 Yazıcıoğlu, R. Yılmaz, *Bilgisayar Suçları,* İstanbul, Alfa Yayınevi, Ekim 1997, s. 50.

2 Taşkın, Şaban Cankat, *Bilişim Suçları,* İstanbul, Beta Yayıncılık, Kasım 2008, s. 1.

BİLİŞİM HUKUKU İLE İLGİLİ KAVRAMLAR

Bilişim suçunun ne olduğunun anlaşılabilmesi için, bilişim sisteminin ne olduğuna kısaca değinilmelidir. Öncelikle belirtmemiz gerekir ki bilişim suçu ile ilgili çok farklı tanımlar bulunmaktadır.[3] Bu tanımların ortak bir özelliğinin bulunmayışı, bilişim suçunun tanımlanmasında ciddi güçlüklere yol açmaktadır. Ancak kısaca, bilişim suçlarını iki grupta inceleyebiliriz.

Birinci grupta bilişim sistemlerine karşı işlenen suçlar yer alır. Örneğin, biraz aşağıda inceleyeceğimiz TCK'nın 10. Bölümünde yer alan ve TCK m. 243-TCK 244 ve TCK 245'te düzenlenmiş olan suçlar bu kapsamdadır.

İkinci grupta ise bilişim sistemleri aracılığı ile işlenen suçlar yer almaktadır. Bu suçlarda, suç doğrudan doğruya bilişim sistemine karşı işlenmez ancak bilişim sistemi araç olarak kullanılır. Sözgelimi, TCK m. 142/2.e'de hırsızlık suçunun bilişim sistemleri aracılığı ile işlenmesi ağırlaştırıcı neden olarak düzenlenmiştir. Burada, bilişim sistemi, hırsızlık suçunda bir araç konumundadır.

Peki bilişim sistemi nedir? Bu konuda öğretideki değişik görüşlerden[4] ve yargı kararlarından yola çıkılarak şu temel ölçütlere göre karar verilecektir.

• Bir sistem eğer bilgisayar temelli çalışıyorsa bilişim sistemidir. Bir başka deyişle, bilgisayar olmadan o sistem olamayacaksa, sistemi bilişim sistemi olarak adlandırmak gerekir. Bu durumda, bilgisayar olmadan o sistem çalışamaz. *(Bilgisayar, o sistemin olmazsa olmazı konumundadır. (sine qua non!).* Yargıtay kararlarından da yola çıkılarak, otomatik para çekme makineleri (ATM) bilişim sistemi sayılacaktır.

• İkinci ölçüt ise, 765 Sayılı (eski) TCK dönemindeki yasal terimden yola çıkılarak ortaya atılmıştır. Buna göre, bir sistem eğer bilgileri otomatik olarak işleme koyabiliyor ve işleyebiliyorsa, o sistemi bilişim sistemi olarak kabul etmek gerekir. Bilgileri otomatik işleme koyabilmekten kasıt, sistemin veri gönderip alabilmesi, manyetik olmasıdır

---

3 Geniş bilgi ve tanımlar için bkz Taşkın, *Bilişim Suçları,* s.10 vd.

4 Geniş bilgi, görüşler ve yargı kararları için bkz Taşkın, *Bilişim Suçları,* s. 6 vd ile s.182.

• Sistemin belli bir amaç için özgülenmemesi ve genel amaçlı olarak programlanabilmesi de o sistemi bilişim sistemi olarak kabul etmemize yol açar.

Öyleyse, yukarıdaki ölçütlerden yola çıkılarak, bilişim sistemi olan ve olmayan sistemlere şunlar örnek gösterilebilecektir.

Bilişim sistemi sayılan sistemler: Bilgisayar, ATM'ler,

Bilişim sistemi sayılmayan sistemler: Cep telefonları, takograf cihazları, dekoderler (Dekoderin kaçak kullanımı özel hukuk gereğince tazminat konusudur. -Yargıtay)

Yukarıdaki tüm ölçütlere rağmen, duraksama yaşanırsa, Yargıtay kararları gereğince, sistemin bilişim sistemi olup olmadığı bilirkişi incelemesi ile belirlenecektir.

I. BÖLÜM

HUKUKUMUZDA BİLİŞİM SUÇLARI

Çalışmamızın bu bölümünde, TCK'nın 10. Bölümünde düzenlenen bilişim suçları, TCK'da bilişim suçu kapsamında kabul edilebilecek veya bilişim sistemleri aracılığı ile işlenebilecek diğer suçları inceleyeceğiz.

I. TCK'DAKİ BİLİŞİM SUÇLARI

Bu bölümde, TCK 243-244-245 ve 246. maddeleri incelenmiştir. Yeri geldikçe, TCK'daki diğer bilişim suçlarına ve karşılaştırmalı hukuktaki düzenlemelerle, Yargıtay kararlarına da değinilmiştir.

1. Bilişim Sistemine Girme Suçu

Bu kısımda 243. maddede, bir bilişim sisteminin tümüne veya bir kısmına hukuka aykırı olarak girme ve girdikten sonra hukuka aykırı olarak çıkmama eylemi suç olarak tanımlanmıştır. Burada suçun oluşması bakımından önemli olan bilişim sistemine girmek ve sistemde bir süre kalmaktır. Yalnızca sisteme girmek hukukumuzda suç değildir. Sistemde bir süre kalınmasının aranması, suçun cezalandırılmasını güçleştirmektedir.

Ancak, henüz tarafı olmadığımız Avrupa Konseyi Siber Suçlar Sözleşmesi (AK-SSS) 2. maddesinde ise, sisteme erişim başlı başına suç olarak kabul edilmiştir.[5] Benzeri düzenlemeler Avustralya, Belçika, Şili, Çin Fransa, İsviçre, İngiltere, Singapur, İrlanda,[6] ABD, Yunanistan, İsrail, Malta, Hollanda, Finlandiya, Kanada ve Malezya hukuklarında da mevcuttur. Bizdeki düzenlemenin o düzenlemelerden farkı, sisteme girmenin yanı sıra, sistemde belli süre kalmayı arıyor oluşudur.

Sistemde kalma süresinin ne kadar olduğunu somut olaya göre yargıç takdir edecektir. Sürenin, sistemdeki bilgileri elde etmeye yetecek kadar olması temel koşul olarak aranacaktır.

Bu suçun yasaya konması ile hem bilişim sisteminin güvenilirliği, hem kişilerin özel yaşamı hem de sistemi kullananların kişisel çıkarları korunmuştur.

243. maddedeki suçta herkes fail olabilir. Ancak, takdir edilmelidir ki bu suçun faili olabilmek için, iyi düzeyde (ortalamanın üzerinde) bilgisayar bilgisine sahip olmak aranmalıdır. Bu suçta, sistemine girilmek yoluyla zarara uğrayan herkes mağdur sayılır.

Suçun oluşması için sisteme ne şekilde girildiği önem taşımaz. Örneğin, fail sisteme bizzat girmese ama sisteme girmeye yarayan bir casus programı e-posta yoluyla gönderse de bu suç oluşacaktır. Çünkü casusu program genellikle güvenilir ve tanıdık bir e-posta aracılığı ile sisteme ulaştırılmakta ve e-postayı açan kişi, kötü niyetli casus programın farkına varmamaktadır. Bu suçun oluşması için mutlaka sistemin tümüne girilmesi gerekmez; bir kısmına girmekle de suç oluşacaktır.

Suçun oluşmasına örnek olarak, sistemin şifresinin veya güvenlik duvarının sahibinin rızası dışında kırılması ya da kırma olmasa dahi, sistemin şifresinin bilinmesi durumunda, şifre sahibinin rızası dışında sisteme erişilmesi verilebilir. (MSN şifresini kırmak yoluyla sisteme

---

5 Sözleşme ile ilgili geniş bilgi için bkz Helvacıoğlu, Aslı Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümleri'nin İncelenmesi", *İnternet ve Hukuk,* Derleyen: Yeşim M. Atamer, Bilgi Üniversitesi Yayınları, 1. Baskı İstanbul, Ocak 2004, s. 280 vd.

6 Hedley, Steve, *The Law of Electronic Commerce and The Internet in The UK and Ireland,* Cavendish Publishing, First Edition, London, 2006, s. 20.

girmek ve sistemde kalmak ya da şifresini bildiğiniz bir kişinin MSN adresine, ondan habersiz olarak girmek ve o sayfada kalmak).

Suçun oluşması için mağdurun bir zarara uğramış olması şart değildir. Salt sisteme girmek ve sistemde kalmak dahi suçtur. Failin, sisteme kendi adına ya da bir başkası adına girmesi de suçun oluşmasını önlemeyecektir.

Suçun oluşması için, sisteme erişimin hukuka aykırı olması gerekmektedir. Sözgelimi yalnızca yetkili kişilerin girmesine izin verilen ya da belli bir şifre ile girilebilen sisteme üçüncü kişi tarafından erişilmesi durumunda suç oluşacaktır. Çünkü bu durumda sistem özel bir şifre ile korunmaktadır. Ancak, sisteme erişmeye yetkili olan kimse, üçüncü kişiye şifresini vermiş ve sisteme o şekilde erişilmişse suç oluşmaz. Bunun dışında, bir mahkeme kararına dayanılarak, sözgelimi, Ceza Muhakemesi Kanunu (CMK) m. 134 gereğince, bilgisayarda arama işlemine girişilmişse, yine hukuka uygunluk nedeni var sayılmaktadır ve suç oluşmaz. Aynısını, CMK m. 135'te düzenlenmiş olan *"iletişimin tespiti tedbiri"* bakımından da söylemek mümkündür. Örneğin, CMK m. 135 gereğince, şüphelinin e-postalarının izlenmesi için bilişim sistemine girilmesi durumunda da suç oluşmayacaktır. Ayrıca, kanaatimizce, *"etik hacker"* veya *"beyaz hacker"* olarak adlandırılan ve bir kurumun sistemindeki zafiyetleri ortaya koymakla görevlendirilen kişiler de bu suçun faili olamazlar. Ancak bunun için, adı geçen kişilerin, sistemine girilmesine izin veren kuruluşa karşı bir eylemi söz konusu olmalıdır. Örneğin, Microsoft'un sistemindeki zayıflıkları ortaya çıkarmak için bu şirket tarafından görevlendirilen ve şirketin sistemine giren kişilerin durumu bu kapsamda ele alınabilir.

Bu suçun yasada öngörülen cezası bir yıla kadar hapis veya adli para cezasıdır. Ancak, sistemin içerdiği veriler yok olur veya değişirse ceza altı aydan iki yıla kadar hapis olarak uygulanacaktır.

2. Bilişim Sistemine Müdahale ve Bilişim Sistemi Aracılığıyla Yarar Sağlama Suçu

TCK'daki diğer düzenleme ise TCK'nın 244. maddesindedir. Buna göre, bu suç bakımından aşağıdaki ölçütlere göre değerlendirmeye gidilecektir.

TCK m. 244/4'te *"yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur."* ifadesi yer almaktadır. Öyleyse, öncelikle, yukarıdaki fıkralarda tanımlanan fiillerin *(suçun maddi unsurunun)* neler olduğunun açıklığa kavuşturulması, suçun nitelendirmesi bakımından önem taşımaktadır.

TCK m. 244/1'de bir bilişim sisteminin *işleyişinin engellenmesi veya bozulması* fiili yaptırıma bağlanmıştır. İşleyişin engellenmesinden kasıt, bir tanıma göre, sistemin düzgün işleyişinden ötürü elde edilecek yararın engellenmesi veya sistemin olağan işlevini yerine getiremeyecek hale getirilmesidir.[7] Diğer bir tanım ise, işleyişin engellenmesinden, sisteme yapılan eklerle, sistemin usulüne uygun şekilde değerlendirilmesi olanağının kaldırılması, sistemin amacını yerine getiremeyecek duruma getirilmesinin anlaşılması gerektiği yönündedir.[8]

Belirtmek gerekir ki işleyişin engellenmesi her somut olayda farklı biçimde ortaya çıkabilir. Örneğin sistemi besleyen elektrik kesilebilir, sistemin çalışması için mutlaka gerekli olan bir donanım çıkarılabilir, sistemin kabloları sökülebilir, sisteme virüs veya benzeri bir zararlı yazılım yüklenebilir, sistemde olmayan bir şifre sisteme yerleştirilebilir veya sistemdeki mevcut şifre değiştirilebilir.[9] Sistemin elektronik posta yoluyla kilitlenmesi de işleyişinin engellenmesi olarak tanımlanabilir.[10]

TCK m. 244/1'de tanımlanan diğer bir hareket ise sistemin işleyişini bozmaktır. Bozmak, *Türk Dil Kurumu Sözlüğü*'nde *"bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek"* olarak tanımlanmıştır.[11] Buna göre, sistem bozulduğunda tamamen çalışamaz hale gelmektedir.[12]

---

7 Yazıcıoğlu, *Bilgisayar Suçları,* s. 263; aynı yönde Kurt, Levent, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Seçkin Yayıncılık, Ankara, 2005, s.164.

8 Kardaş, Ümit, "Bilişim Dünyası ve Hukuk", *Karizma Dergisi,* Sayı 13, 01.03.2003, s. 16.

9 Dülger, M. Volkan, *Bilişim Suçları,* Ankara, Seçkin Yayıncılık, Kasım 2004, s. 234.

10 Kurt, *Bilişim Suçları,* s. 164.

11 http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=bozmak (Erişim Tarihi: 26.01.2009)

12 Taşkın, *Bilişim Suçları,* s. 45.

Çalışamaz hale gelmekten kasıt ise, sistemin çökertilmesi, program akışının değiştirilmesi, bozulması, sistemin soyut unsurlarının örneğin virüsler aracılığıyla işleyemez hale getirilmesidir.[13] Buna göre, yazılımın kısmen veya tamamen çalışamaz hale getirilmesi durumunda ya da sistemin çalışmasına yarayan düzeneğe zarar verilmesi durumunda sistem eğer bir daha çalışamayacak hale geliyorsa, sistemin işleyişinin bozulduğu kabul edilmelidir[14]. Buna örnek olarak bilgisayarın hard diskini kırmak ya da fiziki bir etkiyle (örneğin baltayla parçalamak gibi) hard diske zarar vermek gösterilebilir. Çünkü hard diske bu şekilde verilen zarar sonucunda, hard diskteki verilere ulaşabilmek olanaksız olacaktır. Bunun sonucu da sistemin işleyemez hale gelmesidir. Aynısı, CD, DVD, taşınabilir bellek gibi veri taşıma araçları için de geçerlidir.

TCK 244/2'de ise suçun maddi unsuru olarak verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi tanımlanmıştır. Bu fiillerin sonucunda faile altı aydan üç yıla kadar hapis cezası verilecektir.

Veri kavramından neyin kast edildiğini tanımlamak da TCK m. 244'teki suçun anlaşılması bakımından önem taşımaktadır. Bilişim hukuku anlamında veri, "*olgu, kavram veya komutların, iletişim, yorum veya işlem için elverişli biçimde gösterilmesi*" olarak tanımlanmaktadır.[15] Örneğin, perakende satış yapan bir mağazada, bir müşterinin siparişinde yer alan kimliği, sipariş ettiği ürün, satın almak istediği ürün miktarı ve ürün fiyatı o mağaza için ham haldeki veridir.[16]

Somut olayımızdaki suçun tanımlamasının daha sağlıklı ortaya konabilmesi bakımından TCK m. 244/2'deki eylemleri de açıklamak gerekecektir. Verilerin bozulması, biraz yukarıda açıkladığımız sistemin işleyişinin bozulmasından çok da farklı değildir.[17]

---

13 Kurt, *Bilişim Suçları,* s.164.

14 Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Seçkin Yayıncılık, Ankara, 1.Baskı, Mayıs 2005, s. 188

15 http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=veri (Erişim Tarihi: 26.01.2009)

16 Özkul, Davut, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", *Sayıştay Dergisi,* Sayı 44-45, 01.06.2002, s.13

17 Taşkın, *Bilişim Suçları,* s. 46

Burada, fail hakkında TCK m. 244/1'in mi yoksa m. 244/2'nin mi uygulanacağının tespiti bakımından, failin kastı ortaya koymak önem taşımaktadır. Bu konuda, öğretide iki görüş öne sürülmüştür. İlk görüşe göre,[18] birinci fıkra bakımından failin kastı, hangi yolla olursa olsun sistemin işleyişini bozmak veya sisteme zarar vermektir. Oysa ikinci fıkrada fail sistemin bütününe zarar vermek yerine, yalnızca sistemdeki belli verilere ve belli uygulama yazılımlarına zarar vermek kastıyla hareket etmektedir. Bunun sonucu olarak da ikinci fıkranın yaptırımı daha hafif düzenlenmiştir.

İkinci görüşe göre ise,[19] ikinci fıkradaki suçun oluşması için, failin eyleminin bilişim sisteminin işleyişini engelleyecek hale gelmemesi gerekir. Maddede tanımlanan seçimlik hareketlerden biri yoluyla sistemin işleyişi engellenmişse, artık TCK m. 244/1 uygulanacaktır.

TCK m. 244/2'de tanımlanan diğer bir eylem ise "*verileri yok etmek*"tir. Bilişim sistemindeki verilerin yok edilmesinden, verilere ulaşılmasının tamamen engellenmesi anlaşılmalıdır.[20] Bu durumda, bilişim sistemindeki veriler, yukarıda hard diskin kırılması örneğinde olduğunun aksine, somut olarak değil, soyut (mantıksal) olarak ortadan kaldırılmaktadır. Bu tür verilerin yeniden ortaya çıkarılması, bazen uzun uğraşlar sonucunda bazen de kolaylıkla mümkün olabilmektedir. Verilerin yok edilmesine örnek olarak, bilişim sisteminin belleğindeki verilerin geri dönüşümü olanaksız biçimde silinmesi (format edilmesi) verilebilir.

TCK m. 244/2'de tanımlanan diğer bir eylem ise, verilerin değiştirilmesidir. Bundan kasıt, bilişim sistemindeki bir verinin silinerek yerine başka bir verinin konması ya da sistemdeki veriyle başka bir verinin değiştirilmesidir.[21] Bir başka deyişle, verilerin değiştirilmesinde verilerin orijinal halinden başka bir hale dönüştürülmesi söz konusu olmaktadır.[22] Bu dönüştürmenin kısmen veya tamamen oluşu ya da dönüştürme ile çıkar sağlama ya da zarar verme kastı güdülmüş olması arasında, suçun oluşması bakımından fark yoktur. *Ancak, belirt-*

---

18 Dülger, *Bilişim Suçları,* s. 236

19 Karagülmez, *Bilişim Suçları,* s. 190

20 Taşkın, *Bilişim Suçları,* s. 46

21 Dülger, *Bilişim Suçları,* s. 237.

22 Taşkın, *Bilişim Suçları,* s. 47.

memiz gerekir ki fail bu eylem sonucunda bir çıkar sağlamışsa ve eylem başka bir suç oluşturmuyorsa TCK 244/4 hükmü uygulanmalıdır.[23]

Nitekim Yargıtay 4. CD, 28.02.2000 tarih ve 2000/1068 E; 2000/1771 k sayılı ilamında,[24] sanık tarafından bilgisayar kayıtlarındaki sayaç çarpanlarının değiştirilerek eksik fatura düzenlenmesiyle 15 milyar lira eksik tahakkuk ve tahsilata neden olma eylemini 756 sayılı TCK'nın 525/b maddesi kapsamında değerlendirmiştir. *Bu tür bir eylem artık TCK 244/4 kapsamında değerlendirilecektir.*

Madde 244/2'de belirtilen diğer bir hareket ise *"verilere erişilmez kılmak"*tır. Verilere erişilmez kılmak kavramından neyin anlaşılması gerektiği yönünde üç farklı görüş öne sürülmektedir. İlk görüşe göre,[25] bu eylemden verileri kullanan ya da bu verilere malik olan kişinin dilediği zaman verilere ulaşmasının engellenmesi anlaşılmalıdır. Sözgelimi, sisteme giden elektriğin kesilmesi, verilerin bulunduğu sistemin bozulması, verilerin sistemden silinmesi, verilerin veri taşıma aygıtından silinmesi durumunda verilere erişilmez kılmak eylemi oluşacaktır. Verilerin, mutlaka bu verilerin malikine ait olması gerekmez. Suçun oluşması için önemli olan bu verilere erişme olanağının ortadan kaldırılmasıdır.

İkinci görüş ise,[26] verilere erişilmez kılınması eyleminden, bu verilere ulaşmaya yarayan anahtar sözcüğün değiştirilmesi yoluyla veriyi kullanmakla yetkili olan kimsenin bunları kullanamamasının anlaşılması gerektiğini savunmaktadır. Örneğin bir bilim sisteminin açılması için gerekli olan giriş şifresinin değiştirilmesi verilere erişilmez kılınması suçunu oluşturacaktır.

Üçüncü görüş ise,[27] verilere erişilmez kılınması eyleminin, sistemde şifre olmadığı halde sisteme şifre yerleştirmekle de işlenebileceğini savunmaktadır. Bu durumda, sisteme erişme yetkisi olan kimse, konulan şifre nedeniyle verilere ulaşamayacak ve verilere erişilmez kılmak suçu oluşacaktır.

---

23 Taşkın, *Bilişim Suçları,* s. 47.

24 Aktaran: Kurt, *Bilişim Suçları,* s. 169.

25 Dülger, *Bilişim Suçları,* s.237.

26 Kurt, *Bilişim Suçları,* s. 170.

27 Taşkın, *Bilişim Suçları,* s. 48.

TCK m. 244/2'de belirtilen suçun diğer maddi unsuru ise *"sisteme veri yerleştirmek"*tir. Sisteme veri yerleştirmek, bilişim sistemini kullanmakla yetkili olan kimsenin (veya sistemin malikinin) bilgisi ve onayı dışında, dışarıdan herhangi bir verinin bilişim sistemine yerleştirilmesidir. Yerleştirme işlemi, kaydetme, ekleme veya yükleme şeklinde gerçekleştirilebilir. Veri yüklenirken kullanılan yöntem de bu eylemin oluşması bakımından önem taşımaz. Sözgelimi, taşınabilir bellek, CD, disket ya da internet aracılığı ile de verinin yüklenebilmesi mümkündür. Failde, sisteme zarar verme kastı aranmaz. Bu kasıt olmasa da yalnızca sisteme girilerek verilerin değiştirilmesi bile başlıbaşına suçtur.[28]

TCK m. 244/2'de belirtilen suçun diğer maddi unsurlarından biri de *"verilerin başka yere gönderilmesi"*dir. Veri göndermeden anlaşılması gereken, veri göndermeye ya da kopyalamaya yarayan bir araçla verilerin kopyasının çıkarılarak başka bir bilişim sistemine veri aktarılması ya da internet yoluyla (örneğin e-posta) bir sistemdeki verilerin başka bir sisteme aktarılmasıdır.[29] Burada da herhangi bir zarar doğmasa dahi yalnızca veri gönderme eylemi nedeniyle fail cezalandırılacaktır.[30] Ancak, burada veriler tamamen yok olmamıştır. Zira tamamen yok olması durumunda, biraz yukarıda incelemiş olduğumuz verileri yok etme suçu oluşacaktır.[31]

Belirtmemiz gerekir ki TCK m. 244/2'de tanımlanan suç seçimlik hareketli bir suçtur ve maddede sayılan (yukarıda incelenen) sistemin işleyişini engellemek, işleyişini bozmak, sisteme veri yerleştirmek, var olan verileri başka yere göndermek, verileri erişilmez kılmak, verileri değiştirmek veya verileri yok etmek hareketlerinden herhangi birinin gerçekleşmesi ile suç işlenmiş olacaktır.

TCK m. 244'te tanımlanan suçun banka ve kredi kurumları ya da kamu kurum ve kuruluşlarına ait bilişim sistemleri aleyhine işlenmesi suçtaki ağırlaştırıcı nedendir. TCK m. 244/1 ve 2. fıkralarındaki suçun manevi unsuru ise genel suç işleme kastıdır.

Sanıklar hakkında, TCK m. 244/4'teki bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlanması suçunun oluşması ancak yukarıda

---

28 Geniş açıklama için bkz Taşkın, *Bilişim Suçları,* s. 48 vd.

29 Dülger, *Bilişim Suçları,* s. 238.

30 Kurt, *Bilişim Suçları,* s. 170.

31 Dülger, *Bilişim Suçları,* s. 238.

ayrıntılı olarak açıklanan hareketlerden birinin işlenmesi ile oluşacaktır. *Bir başka deyişle, bir sanığın TCK 244/4'ten cezalandırılabilmesi için "bir bilişim sisteminin işleyişinin engellenmesi, sistemdeki verilerin bozulması, sisteme veri yerleştirilmesi, sistemdeki verilerin başka yere gönderilmesi, verilere erişilmez kılınması, verilerin değiştirilmesi veya yok edilmesi yoluyla kişinin kendisinin veya başkasının yararına haksız çıkar sağlaması" gerekmektedir. (Buradaki haksız çıkardan maddi bir çıkar anlamak gerekir kanısındayız). Bu yetmemekte, bu şekilde sağlanan haksız çıkarın da başka bir suç oluşturmaması gerekmektedir. Eğer bu haksız çıkar başka bir suç oluşturuyorsa, TCK 244/4'ten hüküm kurma olanağı da olmayacaktır.* Böyle bir durumda, somut olaya göre, hırsızlık, güveni kötüye kullanma, dolandırıcılık ve zimmet gibi bir başka düzenlemeden hüküm kurulması gerekecektir.[32] Ancak madde gerekçesinde *"fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir"* şeklinde bir ifade yer almaktadır. Gerekçe, ceza hukuku uygulamasında, yargıca yol gösterici olarak kabul edildiğinden, gerekçeye göre hüküm kurmak yanıltıcı olacaktır.

TCK m. 244/4'te tanımlanan suç bakımından, failde *özel kast* aranmalıdır. Bu kasıt, yukarıdaki fıkralarda tanımlanan hareketler yoluyla, kendisine veya bir başkasına maddi bir çıkar sağlama kastı olarak anlaşılmalıdır.[33]

AK-SSS'nin 4. ve 5. maddelerinde, TCK m. 244'teki düzenlemelere koşut düzenlemeler mevcuttur. Sözleşme'nin 4. maddesinde *"verilere müdahale"*; 5. maddesinde ise *"sistem engellemeleri"* eylemleri tanımlanarak yaptırıma bağlanmıştır. Bu bağlamda, TCK m. 244 ile AK-SSS arasında bir koşutluk olduğunu söyleyebiliriz.

Sözleşme'nin 4. maddesindeki suçun oluşması için verilerin silinmesi, bozulması, değiştirilmesi veya ortadan kaldırılması gerekir. Ayrıca, failde kasıtlı olarak sisteme müdahale etme kastı olmalıdır. Suçtaki eylemler, seçimlik hareketlerdir. Taraf devletleri suçu *"tehlike suçu"* olarak belirleme konusunda takdir hakkına sahiptirler.

Sözleşme'nin 5. maddesindeki suçun oluşması içinse sistemin çalışmasını zorlaştıracak şekilde sisteme veri yüklenmesi, verilerin silinmesi, bozulması, değiştirilmesi, sistemden dışarıya veri aktarılması gerekir. Suçun oluşması için, failde genel kastın varlığı yeterlidir. Söz-

---

32 Geniş açıklama için bkz Taşkın, *Bilişim Suçları,* s. 57 vd.

33 Taşkın, *Bilişim Suçları,* s. 59.

leşmedeki hareketlerin sınırlı sayıda olmadığını da belirtmemiz gerekmektedir.

Karşılaştırmalı hukukta ise, bilişim sistemin de yer alan verilerin veya programların kısmen veya tamamen tahrip edilmesi, değiştirilmesi, işlevleriyle oynanması, olağan işleyişlerinin engellenmesi, erişiminin kısıtlanması eylemleri genel olarak bilişim sistemlerine karşı mala zarar verme suçu biçiminde tanımlanmıştır. Fransa, Almanya, Danimarka, Finlandiya, Avusturya, İtalya, İsveç Ceza Kanunları buna örnektir. Bu eylemleri ayrı kanun şeklinde düzenleyen ülkeler de mevcuttur. İngiltere ve İrlanda bunlara örnek gösterilebilir.

Son olarak belirtilmelidir ki TCK m. 244, 765 sayılı TCK'nın 525/b.1 maddesinin karşılığını oluşturmaktadır.

BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU

TCK 245. maddesinde düzenlenen *"Banka ve Kredi Kartlarının Kötüye Kullanılması"* suçu bakımından da bir değerlendirmeye gitmek gerekecektir.

Öncelikle belirtmemiz gerekir ki TCK'nın 245. maddesi, 765 sayılı TCK'nın 525/b.2 maddesinin karşılığını oluşturmaktadır ve o dönemde verilen Yargıtay kararları da bu bağlamda yol gösterici olarak kabul edilebilecektir. Ancak o dönemdeki çelişkili Yargıtay kararları ve bunun sonucunda ortaya çıkan tartışmaların sonlandırılması için TCK 245 yeniden kaleme alınmış ve Yargıtay CGK'nın o dönemdeki tartışmaları sonlandırmak için verdiği 10.04.2001 tarih ve 2001/76-30 E; 2001/757 K sayılı kararı da göz önünde bulundurulmuştur.[34] Yargıtay'ın adı geçen kararında özetle, *"sanığın haksız olarak ele geçirdiği başkasına ait kart ve şifre ile bankanın ATM makinelerinden para çekilmesi eylemi TCK'nın 525/b.2'deki "bilgileri otomatik işleme tabi tutan sistemi kullanarak kendisine hukuka aykırı yarar sağlama suçu"nu (bilişim suçu) oluşturur."* denmiştir.

Ayrıca, TCK 245. maddenin gerekçesinde de *"Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis'lerinin tümünü de içeren bu füllerin, duraksamaları ve içtihat farklılıklarını önlemek*

[34] *Yargıtay Kararları Dergisi,* Haziran 2001, s. 913-915.

amacıyla, bağımsız suç haline getirilmesi uygun görülmüştür." şeklindeki ifadeden de banka veya kredi kartı yoluyla elde edilen her türlü çıkarın TCK m. 245 anlamında değerlendirileceği anlatılmak istenmiştir.

TCK'nın 245. maddesinde üç ayrı suç düzenlenmiştir. Maddenin ilk fıkrasında, başkasına ait bir banka veya kredi kartını, bu kartı ne şekilde ele geçirmiş olursa olsun, elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanarak veya kullandırtarak kendisinin ya da bir başkasının adına çıkar sağlaması suç olarak düzenlenmiştir.

İkinci fıkrada ise, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satın alınması, satılması, devredilmesi, kabul edilmesi suç olarak düzenlenmiştir.

Üçüncü fıkrada, sahte olarak üretilmiş olan ya da üzerinde sahtecilik yapılan bir kredi kartını kullanmak yoluyla kendisine veya bir başkasına yarar sağlama fiili suç olarak düzenlenmiştir.

TCK m. 245/1'deki suçu kısaca *"başkasının kartıyla yarar sağlama suçu"* olarak tanımlayabiliriz.[35] Bu suçun oluşması için, failin kartı ne şekilde elde ettiği önem taşımaz. Buluntu, çalıntı (ya da hatta belki de rızaen teslim) yoluyla kart elde edilmiş olsa da suç oluşacaktır. Kartın ne şekilde elde edildiğinin önem taşımaması, maddedeki *"her ne suretle olursa olsun"* deyiminden yola çıkılarak söylenebilir.

Suçun oluşumu için önemli olan en temel nokta, kartı kullanan kimsenin, *bir başkasına ait kredi kartını kullanarak* kendisinin veya bir başkasının adına bir çıkar elde etmesidir. Bu çıkar, kartın bizatihi kullanılması yoluyla ya da kart bilgilerinin veri iletim ağlarında (internet) kullanılması yoluyla ya da karttan alışveriş yapılması yoluyla olabilir.

Suçun oluşması için gereken ikinci koşul, maddedeki deyişle, *"kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın"* kartın üçüncü kişi tarafından kullanılmış olmasıdır.

Suçta korunan hukuki yarar konusunda değişik görüşler öne sürülmüş olmakla birlikte, maddenin gerekçesinden de yola çıkılarak, kanımızca korunan hukuki yararın karma bir nitelik taşıdığı belirtilebilir.[36] Ancak, yine de en baskın olan hukuki yarar kişinin malvarlığıdır. Zira

---

35 Taşkın, *Bilişim Suçları,* s. 66.

36 Geniş bilgi ve açıklamalar için Taşkın, *Bilişim Suçları,* s. 63.

söz konusu suçun işlenmesi ile kişinin malvarlığında ciddi kayıplar oluşmaktadır.

Suçta herkes fail ve mağdur olabilir. Ancak, suçun işlenmesi için gerekli olan banka ve kredi kartlarının kopyalanmasında gereken teknik donanıma sahip olunması ve bu donanımın nasıl kullanıldığının bilinmesi fail bakımından bir özellik olarak düşünülebilir. Suçun mağduru, malvarlığında azalma olan kimsedir. Banka veya kredi kurumu ise ancak suçtan zarar gören sıfatını taşıyabilir.[37]

Suçun oluşumu için failde genel kastın mı özel kastın mı aranması gerektiği tartışmalı olmakla birlikte, kanımızca madde metninde yer alan "yarar sağlamak" ifadesi de gözetildiğinde, bu yararın *"hukuka aykırı yarar"* olduğu belirtilmeli ve bu durumda failde özel kastın varlığı aranmalıdır.[38]

TCK m. 245/4'te özel bir cezasızlık sebebi düzenlenmiştir. Buna göre, bu maddenin ilk fıkrasındaki suçun haklarında ayrılık kararı verilmemiş eşlerden birine, üstsoy veya altsoya veya bu derecedeki kayın hısımlarından birine ya da evlat edinene veya evlatlığa; aynı konutta yaşayan kardeşlerden birine karşı işlenmesi durumunda ilgili akraba hakkında cezaya hükmolunmayacaktır. Burada, ceza vermeme konusunda yargıcın bir takdir hakkı yoktur. Yargıç, cezayı vermeyecektir.

245. madde benzeri düzenlemelere karşılaştırmalı hukukta da rastlanmaktadır. Örneğin ABD'de[39] 1986 tarihli *"Elektronik Haberleşme Gizliliği Kanunu" (Electronic Communication Privacy Act)* ve *"Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanunu" (Computer Fraud and Abuse Act)* ile *"Kredi Kartlarının Kötüye Kullanılmasının Önlenmesi Kanunu" (Credit Card Fraud Act);* Hollanda'da 1 Mart 1993 tarihli Ceza Kanunu değişikliği,[40] İsviçre'de 01.01.1995 tarihli Ceza Kanunu değişikliği, Almanya'da[41] Ceza Kanunu'nun 226.b maddesi bu tür suçları düzenleyen değişik kanunlara örnektir.

---

37 Taşkın, *Bilişim Suçları,* s. 64.

38 Aynı yönde Karagülmez, *Bilişim Suçları,* s. 216.

39 Yazıcıoğlu, *Bilgisayar Suçları,* s. 191; *Karagülmez*, *Bilişim Suçları,* s.197.

40 *Yazıcıoğlu*, Bilgisayar Suçları, s. 174.

41 Nuhoğlu, Ayşe, *Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması,* Analiz Basım Yayın, İstanbul, 2002, s. 254.

TCK'nın 246. maddesinde ise, tüzel kişilerin sorumluluğu düzenlenmiştir. Buna göre, bilişim suçu faili tüzel kişilikse, tüzel kişiliğe ceza verilmeyecek ancak TCK m. 20/2 anlamında, tüzel kişilik hakkında bunlara özgü güvenlik tedbirlerine hükmolunacaktır.

5237 SAYILI TCK'DAKİ DİĞER BİLİŞİM SUÇLARI

Yukarıda incelediğimiz suçların yanı sıra, diğer bazı suçlar da bilişim alanında suçlar başlığında düzenlenmemiş olmasına rağmen, bilişim sistemleri aracılığıyla işlenebilecektir.

Bu suçları da iki başlık altında incelemek mümkündür. İlk başlıkta, kişilerin özel hayatına karşı işlenen suçlar olan ve TCK m. 132'deki *"Haberleşmenin Gizliliğini İhlal Suçu"*, TCK m. 135'teki *"Kişisel Verilerin Kaydedilmesi Suçu"*; TCK m. 136'da düzenlenmiş olan *"Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme"* suçu ile TCK m. 138'de düzenlenen *"Verilerin Yok Edilmemesi"* suçları ile TCK m. 226. maddesinde düzenlenen *"Müstehcenlik"* suçlarıdır.

İkinci başlıktaki suçlar ise, kişilerin özel yaşamının korunması ile doğrudan doğruya bağlantılı olmamakla birlikte, bilişim sistemleri aracılığı ile de işlenebilen TCK m. 106'daki tehdit, TCK m. 124'teki *"Haberleşmenin Engellenmesi"*; TCK m. 125'teki *"Hakaret"*; TCK m. 142/2.e'deki *"Bilişim Sistemlerinin Kullanılması Yoluyla Hırsızlık"* ile TCK m. 158/1.f'deki *"Bilişim Sistemlerinin Kullanılması Yoluyla Dolandırıcılık"* suçlarıdır.

Bunlardan en yaygın olarak görülenleri hakaret, tehdit ve hırsızlıktır. Dolayısıyla, bu suçlara kısaca değinilecektir.

Hakaret suçu, TCK m. 125'te düzenlenmiştir ve bilişim suçu bakımından maddenin ikinci fıkrası önem taşımaktadır. Buna göre, mağduru hedef alan sesli, yazılı veya görüntülü bir ileti suçun oluşması için yeterli olacaktır. Örneğin, mağdura yönelik hakaret ya da sövme içeren bir e-posta gönderilmesi sonucunda suç oluşacaktır. TCK m. 106'daki tehdit suçu bakımından da aynısını söylemek mümkündür.

TCK 142.2'e'de hırsızlık suçunun bilişim sistemleri aracılığı ile işlenmesi nitelikli hırsızlık olarak kabul edilmiş ve bu fiil basit hırsızlığa göre daha ağır bir yaptırıma bağlanmıştır. Bu suça örnek olarak, uygulamada sıklıkla karşılaşılan ve *"internet hırsızlığı"* olarak da adlandırı-

lan suç verilebilir. Bu durumda, bir başkasının hesabına girilerek o hesaptaki paraları kendi hesabına aktaran fail, aslında mağdur olan kimsenin parasını çalmaktadır. Bir başka şekilde belirtilecek olursa, bu eylem nedeniyle, fail bir başkasının malvarlığına zarar vermektedir. Ortada, somut banknot /madeni para şeklinde bir para olmasa da bir başkasına ait malvarlığının hukuka aykırı olarak elde edilmesi söz konusu olduğundan, hırsızlık suçunun TCK m. 141'de tanımlanan maddi unsurunun da oluştuğu kabul edilmelidir.

Öğretide Tezcan-Erdem-Önok tarafından,[42] TCK 141. maddesinde, hırsızlığın basit halinin tanımlandığı, bu maddede somut nesnelerin çalınmasının yaptırıma bağlandığı, bunun istisnası olarak ise elektrik enerjisinin belirtildiğini, ancak bilişim sistemlerinin kullanılması yoluyla hırsızlık suçunun ne somut nesnelere yönelik ne de elektrik enerjisine yönelik olduğunu, bu nedenle de maddenin tartışmalara yol açacak uygulamaların önünü açacağı, hatta m. 142/2.e'deki düzenlemenin uygulanmasının çok zor olduğu yönünde bir görüş öne sürülmüştür.

Ancak bu görüş, kanaatimizce doğru değildir.[43] Zira her şeyden önce, yasa koyucu TCK m. 142/2.e düzenlemesini ihdas etmişse, bunun bir anlamı olmalıdır. Çünkü *"yasa koyucu abesle iştigal etmez!"*. Şu halde, TCK m. 142/2.e'nin uygulaması nasıl olmalıdır?

Bir başkasının hesabına girilerek o hesaptaki paraları kendi hesabına aktaran fail, aslında mağdur olan kimsenin parasını çalmaktadır. Bir başka şekilde belirtilecek olursa, bu eylem nedeniyle, fail bir başkasının malvarlığına zarar vermektedir. Ortada, somut banknot /madeni para şeklinde bir para olmasa da bir başkasına ait malvarlığının hukuka aykırı olarak elde edilmesi söz konusu olduğundan, hırsızlık suçunun TCK m. 141'de tanımlanan maddi unsurunun da oluştuğu kabul edilmelidir.

Kanaatimizce, bankadan para çekip çantasına koyan mağdurun çantasından bu parayı almakla, kişinin banka hesabına bilişim korsanlığı yoluyla girilerek failin kendi hesabına para aktarması arasında hiç-

---

42 Tezcan, Durmuş/ Erdem, Mustafa Ruhan/ Önok, Murat, *Teorik ve Pratik Ceza Özel Hukuku,* 5560 sayılı Kanuna Göre Güncellenmiş 5. Baskı, Seçkin Yayıncılık, Ankara, 2007, s. 506.

43 Taşkın, *Bilişim Suçları,* s. 116, 117.

bir fark yoktur.[44] Her iki durumda da mağdurun hesabında, failin yararına bir artış (mağdurun zararına azalma) söz konusu olmakta ve her iki eylem de mağdurun rızasına aykırı olarak gerçekleşmektedir. Burada, bilişim sisteminin varlığı yanıltıcı olmamalıdır. Bilişim sistemi, hırsızlık suçunda yalnızca bir araç konumundadır. Dolayısıyla, bilişim sistemi aracılığı ile hırsızlık suçunun varlığı kabul edilmelidir.

Nitekim Yargıtay 11. CD 24.10.2002 tarih ve 2002-5711 E. 2000/8416 K. sayılı kararında[45] şu ifadelerle konuya ışık tutmuştur:

"E... Bankası İzmir Otomasyon Bölge Merkezi'nde şef olarak görev yapan sanığın, yakınlık kurduğu banka personelinin bilgisayarının başında bulunmadığı bir sırada personelin şifresiyle H.Ö adıan sıfır bakiyeli vadeli hesap açarak aynı gün şube mudilerinden İ.A'nın hesabını 8 milyar lira düşürüp H.Ö adına açtığı hesabı, aynı miktarda yükseltmek suretiyle gerçekleştirdiği eylemi_765 sayılı TCK m. 525/b.2'de (TCK m. 244/4) belirtilen eylem kapsamında değerlendirilmesi gerekirken...."

Buna göre, eğer yalnızca hesaplar arasında para aktarma söz konusu ise fail TCK m. 142/2.e'deki nitelikli hırsızlıktan; ancak para aktarmanın yanı sıra, hesapları dengeleyici bir tarzda, bir hesabın bakiyesinin (verilerinin) arttırılarak diğer hesabın bakiyesinin (verilerinin) düşürülmesi söz konusu ise failin TCK m. 244/4'ten cezalandırılması söz konusu olacaktır.

Diğer yandan, TCK m. 244/4'ün mü yoksa 142/2.e'nin mi uygulanacağının tespitinde, failin sisteme şifre kırma yoluyla mı yoksa mağdurun şifresini öğrenmek suretiyle mi girdiği de önem taşımaktadır. Zira fail eğer şifre kırma yoluyla bilişim sistemine erişmiş ve bu şekilde verileri göndermek suretiyle kendisi yararına bir çıkar elde etmişse TCK m. 244/4, şifreyi gizlice öğrenmek suretiyle verileri elde etmişse TCK m. 142/2.e'nin uygulanması söz konusu olacaktır.

TCK 158/1.f'de dolandırıcılığın nitelikli hali düzenlenmiştir. Dolandırıcılık suçunun maddi unsuru, failin hileli hareketlerle bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına yarar sağlamasıdır. (TCK m. 157)

Kanaatimizce, dolandırıcılığın nitelikli hali olan ve TCK m. 158/1.f'de tanımlanan bilişim sistemlerinin kullanılması suretiyle ger-

---

44 Taşkın, *Bilişim Suçları,* s. 117.

45 Aktaran, Kurt, *Bilişim Suçları,* s.169.

çekleştirilen dolandırıcılık eylemi şu anda bilinen bilişim suçlarının hiçbirinde uygulama alanına sahip değildir.[46] Zira bir eylemin dolandırıcılık olarak değerlendirilmesinin en temel koşulu, hileli hareketlerin bireye karşı yapılması gerekmektedir.[47] Oysa TCK m. 158/1.f'de bireye karşı olan bir hileli hareket söz konusu değildir. Bu nedenle, somut olayda dolandırıcılık suçunun varlığı kabul edilemez.

MÜSTEHCENLİK SUÇU

TCK m. 226/3'te müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişinin cezalandırılacağı belirtilmektedir. Bu noktadan hareketle, öncelikle bu tür ürünlerin üretiminin ne anlamda yorumlanması gerektiği, suçun oluşumu bakımından önem taşıyacaktır.

Üretim, bir hammaddeyi veya yan ürünü işleyerek, bir sanayi ürünü veya bir mal üretme işlemi olarak tanımlanabilir.[48] Buna göre, müstehcen görüntülerin oluşturulmasında çocukların kullanılması da üretim sayılacak ve TCK 226/3'teki suç oluşacaktır.

TCK m. 226/3.c.2'de müstehcen görüntülerin ülkeye sokulması, çoğaltılması, satışa arz edilmesi, satılması, nakledilmesi, *depolanması*, ihraç edilmesi, *bulundurulması,* ya da başkalarının kullanımına sunulması suç olarak kabul edilmiştir. Bir başka deyişle, müstehcenlik suçunun maddi unsuru bu sayılan eylemlerden herhangi biridir.

Görüldüğü gibi, bulundurma eylemi de maddeye göre suç sayılmaktadır. *Ancak, salt lafzi yorumla yola çıkılarak, kanundaki "bulundurma" eyleminin başlı başına suç sayılması birtakım ciddi hukuki sorunlara yol açabilecektir.* Öncelikle belirtmemiz gerekmektedir ki TCK m. 226 yorumlanırken, tüm internet kullanıcılarının neredeyse yarısının internetteki pornografinin "*tüketicisi*" olduğu da düşünülmeli ve *müstehcenlik kavramının olabildiğince dar yorumlanması* doğabilecek olası mağduriyetleri baştan önleyebilecektir.[49]

---

46 Taşkın, *Bilişim Suçları,* s. 81.

47 Aynı yönde bkz Tezcan/Erdem/Önok, Ceza Özel, s. 556; Dönmezer, Sulh, *Kişilere ve Mala Karşı Cürümler,* Beta Yayıncılık, 16. Baskıdan Tıpkı 17. Baskı, İstanbul, Ekim 2004, s. 449.

48 http://tr.wikipedia.org/wiki/Üretim (Erişim Tarihi: 19.01.2009)

49 Taşkın, *Bilişim Suçları,* , s. 123.

TCK'nın 226. maddesi açık ve net biçimde kaleme alınmamıştır. Bu yönden de yoruma açıktır. Oysa ceza hukukunda temel kural, normların yoruma açık olmaması ve kafalarda herhangi bir kuşku uyandırmamasıdır. Ancak, maddedeki anlatımın kötü olması nedeniyle, TCK m. 226/3.c.2'de kanaatimizce yalnızca çocuklara ilişkin müstehcenlik değil; tüm müstehcen görüntüler yaptırıma bağlanmıştır.

Bu durumda, kanımızca, herhangi bir müstehcen görüntünün ülkeye sokulması, dağıtılması, satışa arz edilmesi, satılması, nakledilmesi, *depolanması*, ihraç edilmesi, *bulundurulması* veya başkalarının kullanımına sunulması fiilleri TCK m. 226/3.c.2'deki suçu oluşturacaktır. Bulundurma, sanığın bilgisayarında veya veri taşıma aygıtında yer almasıdır. Depolamaktan kasıt ise, müstehcen içerikli görüntülerin, bilgisayarda, veri taşıma aygıtında yer alması ancak, bu verilerin sayısının bulundurmaya göre daha fazla olmasıdır. Sözgelimi, tek bir görüntünün yer alması bulundurmak olarak tanımlanırken, birden çok görüntünün bir veri taşıma aygıtında ya da bilgisayara da yer alması depolama olarak tanımlanmaktadır. Ayrıca, bulundurmada amaç "*tüketmek*" olarak yorumlanabilir. Zira sanığın veri taşıma aygıtında bir veya birkaç görüntü yer almakta ve sanık bu görüntülerden kendisi yararlanmaktadır. Ancak depolamada ise, görüntü sayısı çok olduğundan, sanığın bu görüntüleri satma, dağıtma gibi bir amacı olabilir.

Tam bu noktada, *TCK m. 226. maddenin müstehcen içerikli herhangi bir görüntüyü bulundurmanın ya da depolamanın suç sayılmasının laik devlette kabul edilebilir bir uygulama olmadığını da belirtmemiz gerekmektedir.*[50] Zira bir laik devlette ve hukuk devletinde, devlet vatandaşının "*kişisel bilgisayarında*" hangi görüntüleri bulundurduğu ile veya depoladığı ile ilgilenmemelidir. Aksi halde, tabiri yerindeyse, devlet "*namus bekçiliği*"ne soyunmuş olacaktır ki bu tür bir yaklaşımın kişilerin özel yaşamına aykırı olduğu da açıktır.[51]

Bu açıklamalardan yola çıkılarak denilebilir ki *TCK m. 226/3.c.2 dar yorumlanmalı*[52] *ve yetişkinlere ilişkin müstehcen görüntülerin bulundurul-*

---

50 Taşkın, *Bilişim Şuçları,* s. 126.

51 Soyaslan, Doğan, *Ceza Hukuku Özel Hükümler,* Gözden Geçirilmiş 6.Baskı, Yetkin Yayınevi, Ankara, 2006, s. 464.

52 Nebil Sarp, Füsun, "İnternet Sitelerinin Filtrelendirilmesi" konulu sunum, *Ankara Barosu Uluslararası Hukuk Kurultayı,* 8 Ocak-11 Ocak 2008, Bilişim ve Hukuk, Cilt 2, Ankara Barosu Yayınları, 2009, s. 41.

ması veya depolanması suç olarak kabul edilmemelidir. Ancak, çocuklara ilişkin müstehcen görüntülerin ise bulundurulması ya da depolanması ise suç sayılmalıdır.

Nitekim *Yargıtay 5. CD.27.03.1995* tarih ve 1991-749 E; 1670 K sayılı ilamında[53] "*Sanıkların müstehcenlik içeren bir kaseti yalnızca izlemek amacıyla birbirlerine vermeleri şeklindeki eylemde, sanıklarda ticaret ve teşhir kastı olmadığı için fiilin alenen müstehcen hareket sayılabilmesinin olanaksız olduğu gözetilmeden mahkumiyet hükmü verilmesi BOZMAYI gerektirmiştir.*" diyerek, müstehcenlik suçunun oluşması için failde ticaret ve teşhir kastının varlığını aramıştır.

Yine Yargıtay 5. CD, 28.03.1991 tarih ve 1991-685 E; 1991-1719 K sayılı bir başka kararında[54] yetişkinlere ilişkin müstehcenlikle ilgili şu kararı vermiştir: "*Kahvehanede yalnızca video kaset bulundurmaktan ibaret olan sanığın fiilinin umuma teşhir edilmiş müstehcen hareket sayılamayacağı yönünde hüküm kurulması gerekirken, mahkumiyet kararı verilmesi Bozmayı gerektirmiştir.*"

Ancak, *çocuklara ilişkin müstehcenlik* bakımından Yargıtay 5.CD, 01.10.2007 tarih ve 2007-9856 E; 2007-6957 K. sayılı son kararlarından birinde[55] özetle "*...Çocuk pornografisi ve hayvanlarla yapılan cinsel davranışlara ilişkin çok sayıda resim ve video kaydını bilgisayar sistemi vasıtasıyla temin edip bilgisayarda sistematik bir şekilde depolama ve bulundurma fiili kişisel amaçlı dahi olsa 5237 sayılı TCK'nın 44. maddesi yollamasıyla 226/3. maddesindeki suçu oluşturur.*" demiştir. Karara konu olan olayda, sanığın bilgisayarında çocuk pornosu içerikli 23.000 den fazla fotoğrafa ve 550'nin üzerinde video kaydına rastlanmış, ayrıca, çocuk ve yetişkin birinin hayvanlarla cinsel ilişkisini gösterir fotoğraflar da bulunmuştur.

Yargıtay'ın bu yaklaşımının yanı sıra, biraz aşağıda, konunun daha iyi anlaşılması için müstehcenlik suçunun karşılaştırmalı hukuktaki ve uluslararası sözleşmelerdeki düzenlemelerini de kısaca incelemekte yarar görmekteyiz.

Henüz tarafı olmadığımız Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (AK-SSS) 9. Maddesinde,[56] *çocuk pornografisine ilişkin mater-*

---

53 Aktaran: Soyaslan, *Özel Hükümler,* s. 465.

54 Aktaran: Soyaslan; *Özel Hükümler,* s. 465.

55 *Yargıtay Kararları Dergisi,* Şubat 2008, s. 337.

56 Geniş bilgi için bkz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi"; *İnternet*

yalin elektronik olarak üretimi, dağıtımı ve bu materyale sahip olunması eylemlerinin cezalandırıldığı görülmektedir. Ancak, burada ilk dikkatimizi çeken konu, AK-SSS'nin yalnızca çocuklara ilişkin müstehcen görüntülere sahip olunmasını (veya bu görüntülerin ticaretinin yapılmasının; depolanmasının ya da yayılmasının) suç sayıyor oluşudur. Yetişkinlere ilişkin müstehcen görüntülerin bulundurulması veya depolanması bu Sözleşme'ye göre suç değildir.

Yine AK-SSS'nin 9. maddesinin 2. fıkrasında, çocuk pornografisi tanımlanmış ve bu eylemlerin kapsamında cinsel anlamda müstehcen bir eyleme reşit olmayan kişinin katılımını; cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımını; cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımını gösteren görüntüler çocuk pornografisi kapsamında ele alınmıştır.

Yine AK-SSS m. 9/3 gereğince, "*reşit olmayan kişi" terimi 18 yaşından küçük olan kişileri* ifade etmektedir. Ancak, Sözleşme'ye taraf olan devletlerden herhangi biri, 18 yaş olan bu sınırı daha küçük bir yaş olarak da belirleyebilecektir. Bu yaş sınırı hiçbir şekilde 16 yaşından aşağı belirlenemeyecektir.

ABD'de *Çocukların Online Yayınlardan Korunması Yasası (Child Online Prevention Act); Çocuk Pornografisinin Önlenmesi Yasası, (Child Pornography Prevention Act)* ile çocuklara ilişkin zarar verici içeriğin yayınlanması durumunda ticari kazanç sağlanmışsa, fail 6 aya kadar hapis ve 50.000 USD'ye kadar para cezasına çarptırılacaktır. Hatta bilimsel amaçla bile olsa, çocuk pornosuna ilişkin araştırma yapılması suç sayılmaktadır.[57] Fransa'da[58] küçüklere yönelik olmadığı sürece pornografi suç sayılmamıştır. Ancak, pornografik ve şiddet içerikli yayınlara (internet de dahil), küçükler tarafından erişilebilir kılınması suç olarak

---

ve Hukuk, s. 287; ayrıca bkz Dülger, M. Volkan; "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", *İstanbul Barosu Dergisi,* Cilt 78, Sayı 2004/4, s.1488-1493; Erbaşı, Aslıhan Ayşe; "Çocuk Pornografisi", *İstanbul Barosu Dergisi,* Cilt 81, Sayı 2007/4,s.1609-1647.

57 Geniş bilgi için bkz Akdeniz, Yaman, "Controlling illegal and harmful content on the internet", *Crime and The Internet,* Edited by David S.Wall, First Published 2001, by Routledge, London, s.117; Smıth, Russel/ Grabosky, Peter/ Urbas, Gregor, *Cyber Criminals on Trial,* First Published by Cambirdge University Press, Cambridge, 2004, s. 75-76).

58 Sınar, Hasan, *İnternet ve Ceza Hukuku,* İstanbul, Beta Yayıncılık, 1.Baskı, Temmuz 2001, s. 98.

kabul edilmiştir. (Fransız Ceza Kanunu m. 227-24). Keza İngiltere'de çocuklara karşı internet üzerinden işlenen suçlar *"tehlike suçu"* olarak kabul edilmektedir.[59] Çocuk pornografisinin suç olduğu ülkelere örnek olarak Rusya Federasyonu, İsveç, Danimarka, Polonya, İrlanda, Japonya ve Malezya da gösterilebilir.[60] Ayrıca, belirtmemiz gerekir ki Avusturalya'nın Victoria Eyaleti Ceza Yasası'nda (*Crimes Act* 1958, m. 67/A) 16 yaşından küçüklerle (ya da 16 yaşından küçük görünenlerle) ilgili her türlü film, fotoğraf, bilgisayar oyunu, animasyon ya da yayınlarda çocukla cinsel ilişkiye girildiğini gösteren sahneler, cinsel içerikli tavırlar ve bu her türlü hareket suç sayılmaktadır.[61]

Yine ülkemizin de taraf olduğu Birleşmiş Milletler Çocuk Hakları Sözleşmesi'nin (BM-ÇHS) 1. maddesinde *"Bu sözleşme uyarınca çocuğa uygulanabilecek olan kanuna göre daha erken yaşta reşit olma durumu hariç, on sekiz yaşına kadar her insan çocuk sayılır."* tanımı yer almaktadır. Buna göre, 18 yaşını doldurmamış olan herkes çocuktur. Aynı Sözleşme'nin 34. maddesine göre çocukların cinsel istismardan ve pornografiden korunması için taraf devletlerin her türlü önlemi alma yükümlülüğü bulunmaktadır. 34. madde şöyledir:

"Taraf Devletler, çocuğu her türlü cinsel sömürüye ve cinsel suiistimale karşı koruma güvencesi verirler. Bu amaçla taraf devletler özellikle:

a. Çocuğun yasadışı bir cinsel faaliyete girişmek üzere kandırılması veya zorlanmasını;

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

c. Çocukların, pornografik nitelikli gösterilerde ve malzemede kullanılarak sömürülmesini; önlemek amacıyla ulusal düzeyde ve ikili ile çok taraflı ilişkilerde gerekli her türlü önlemi alırlar."

Çocuk tanımı bakımından, iç hukukumuzdaki duruma kısaca göz atacak olursak, *TCK'ya göre çocuk deyiminden henüz 18 yaşını doldurmamış olan kişi anlaşılır (TCK m. 6/1.b). Keza, 5395 Sayılı Çocuk Koruma Kanunu'na göre de çocuk daha erken yaşta olsa bile; 18 yaşını doldurmamış*

---

59 Hedley, *Electronic Commerce,* s. 151.

60 Kurt, Levent, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Seçkin Yayıncılık, Ankara, 2005,s. 99-113.

61 Smıth/Grabosky/Urbas, *Cyber Criminals,* s. 69.

olan kişiyi ifade eder. (ÇKK m. 3/1-a). *Buna göre, TCK m. 226/3'teki suçun oluşması için müstehcen görüntüleri içeren ürünlerin üretiminde 18 yaşından küçüklerin kullanılması gerekecektir.* Aynı şekilde, üretiminde 18 yaşından küçüklerin yer aldığı müstehcen içerikli ürünleri ülkeye sokmak, çoğaltmak, satışa arz etmek, satmak, nakletmek, depolamak, ihraç etmek, bulundurmak ya da başkalarının kullanımına sunmak suç sayılacaktır.

Sonuç olarak ve kısaca denilebilecektir ki müstehcenlik suçunun yorumlanmasında çok dikkatli olmak, doğabilecek ciddi sakıncaların önlenmesi bakımından önem taşımaktadır.

5651 Sayılı Kanunla Getirilen Düzenleme

1.1. Genel Olarak

23.05.2007 gün ve 26530 sayılı *Resmi Gazete*'de yayımlanarak yürürlüğe giren 14 maddeden ve bir geçici maddeden oluşan 5651 sayılı Kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun) ile Türk Hukuku'nda ilk kez internete erişim yasağı getirilmiş; internet öznelerinin (süjeler) cezai sorumluluğu düzenlenmiştir.

Aşağıda, 5651 sayılı Kanun'un ve bu kanuna dayanılarak çıkarılan 30.11.2007 tarih, 26716 sayılı *Resmi Gazete*'de yayımlanan *"İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik"*in (kısaca Yönetmelik olarak adlandıracağız) çalışmamızla ilgili olan düzenlemeleri incelenecektir. İncelememizde internet öznelerinin cezai[62] ve hukuki[63] sorumluluğuna, çalışmamızın kapsamını genişletmemek için girilmeyecektir. Bu bölümde yalnızca, erişimin engellenmesi kararı ile internet üzerinden cevap ve düzeltme hakkı da incelenecektir.

---

62 Cezai sorumluluk hakkında geniş bilgi için Taşkın, *Bilişim Suçları,* s. 149.

63 Hukuki sorumluluk hakkında geniş bilgi için Soysal, Tamer, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", *Türkiye Barolar Birliği Dergisi,* Sayı 61, Kasım-Aralık 2005, s. 304-309.

2.2. Erişimin Engellenmesi Kararı

5651 sayılı Kanun'un 8. maddesinde, erişimin engellenmesi kararının verilmesine yönelik usul düzenlenmiştir. Buna göre, erişimin engellenmesi kararı ancak birinci fıkrada sınırlı sayıda sayılmış olan (katalog) suçlar hakkında verilebilecektir. Bu suçlar, intihara yönlendirme (TCK m. 84), çocukların cinsel istismarı (TCK m. 103/1); uyuşturucu veya uyarıcı madde kullanımını kolaylaştırma (TCK m. 190); sağlık için tehlikeli madde temini (TCK m. 194); müstehcenlik (TCK m. 226); fuhuş (TCK m. 227); kumar oynanması için yer ve imkan sağlama (TCK m. 228) suçlarıyla 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlardır.

5651 sayılı Kanun'un 8. maddesi gereğince, erişimin engellenmesine karar verilebilmesi için, katalog halinde belirtilmiş olan suçların yanı sıra, bu suçların işlendiğine ilişkin *"yeterli şüphe"* sebebinin oluşmuş olması da aranacaktır.

Erişimin engellenmesi kararı ancak soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından verilecektir. Soruşturma evresinde, gecikmede sakınca varsa, Cumhuriyet Savcısı tarafından da erişimin engellenmesine karar verilebilir. Ancak bu durumda, savcı, bu yöndeki kararını yirmi dört saat içerisinde yargıcın onayına sunar. Yargıç da kararın kendisine sunulmasından itibaren yirmi dört saat içerisinde savcının kararının hukuka uygun olup olmadığına ilişkin kararını verir. Yargıcın bu kararı onaylamaması durumunda, Cumhuriyet Savcısının tedbire derhal son vermesi gerekecektir. Karara karşı 5271 sayılı CMK m. 267 vd. hükümlerine göre itiraz edilebilecektir.

Kararın bir örneği, gereğinin ifası için Telekomünikasyon İletişim Başkanlığı'na (Başkanlık) gönderilir. İlgililerin, kararın kendilerine ulaşmasından itibaren 24 saat içerisinde gereğini yerine getirmesi ve erişimi engellemesi gerekmektedir. Kararın gereğinin yerine getirmeyen sorumlular hakkında, fiil başka bir suç oluşturmuyorsa, altı aydan iki yıla kadar hapis cezası verilecektir.

İdari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi durumunda, Telekomünikasyon İletişim Başkanlığı tarafından, erişim sağlayıcıya on bin YTL'den yüz bin YTL'ye kadar para cezası verilebilecek; bu karardan itibaren 24 saat içerisinde de tedbirin yerine getirilmemesi durumunda ise, Başkanlığın istemi üze-

rine, erişim sağlayıcının yetkilendirmesi iptal edilebilecektir. Bu karara karşı da 2577 sayılı İdari Yargılama Usul Kanunu hükümlerine göre itiraz edilebilecektir.

Erişimin engellenmesi tedbirine hükmedilmesine rağmen, şüpheli hakkında kovuşturmaya yer olmadığına veya kovuşturma aşamasında beraat kararı verilirse tedbir kendiliğinden kalkacaktır. Bu durumda, kovuşturmaya yer olmadığına ya da beraate ilişkin kararın bir örneği Başkanlık'a gönderilecektir.

Ayrıca, hakkında erişimin engellenmesine karar verilen şüpheli, internet sayfasından, hakkındaki soruşturmaya ya da kovuşturmaya neden olan içeriği kaldırınca erişimin engellenmesi kararı da soruşturma evresinde Cumhuriyet Savcısı, kovuşturma evresinde mahkeme tarafından kaldırılacaktır.

Maddede katalog şeklinde belirtilen suçların içerik veya yer sağlayıcısı yurt dışında bulunuyorsa ya da içerik veya yer sağlayıcı yurt içinde bulunmasına rağmen, içeriği çocukların cinsel istismarı (TCK m. 103) veya müstehcenlik (TCK m. 226) suçlarına ilişkin verilerden oluşan web sitesine erişim Başkanlık tarafından re'sen verilecek ve erişim sağlayıcıya bildirilerek gereğinin yapılması istenecektir.

Erişimin engellenmesine ilişkin düzenleme ciddi eksiklikler içermektedir. Bunlardan en önemlisi, katalog halinde suç sayımıdır. Bu demektir ki ancak sayılan suçlarla ilgili olarak erişim engellenebilecektir. Oysa çok tartışmalı olan kumar oynamak için yer sağlama suçu ile müstehcenlik suçu yasanın kapsamındayken terör suçları ya da ırkçılık propagandası bu kapsamda değildir. Örneğin TCK m. 314/1, 316/1 veya 318'deki suçların işlenmesi yönünde propaganda amaçlı kurulan bir internet sitesine erişim yasağı konabilmesi bu kanuna göre mümkün olmayacaktır. Şu halde çözüm ya katalog suçları yöntemine son vermek ya da katalog suçlarının kapsamını genişletmektir.

Diğer önemli bir eksiklik ise, erişimin engellenmesi kararının ne kadar süreyle uygulanacağı yönündedir. Bir başka deyişle, yasaklanan site 1 ay mı 3 ay mı 1 yıl mı ne kadar süreyle kapalı kalacaktır? Bu durum ciddi bir eksikliktir ve *Youtube* sitesinin yaklaşık 1 yıldır kapalı olması da bu sakıncayı çarpıcı biçimde ortaya koymaktadır. Bunun çözümü, CMK m. 135'te olduğu gibi, iletişimin denetlenmesi tedbirinde öngörülen 3 aylık sürenin uygulanmasıdır. Kanımızca, buradaki süre-

nin erişimin engellenmesi tedbiri bakımından uygulanmasına da bir engel yoktur. Zira Ceza Muhakemesi Kanunu uyarınca, sanığın/şüphelinin lehine olmak kaydıyla kıyas mümkündür.

Diğer önemli eksiklik ise, bir veri nedeniyle tüm siteye erişimin engellenmesidir. Bu durum, aynı zamanda kişinin haberleşme özgürlüğüne de engel oluşturmaktadır. Dolayısıyla, teknik olarak mümkün olması durumunda, verilecek olan erişimin engellenmesi kararında sitenin tümüne erişimin engellenmesi yerine yalnızca suç oluşturan içeriğe erişimin engellenmesi ve bu tedbirin de yasada belirtilmesi doğru bir yaklaşım olacaktır.[64]

Bu karara, CMK m. 267 vd hükümlerine göre itiraz edilebilecektir. Erişimin engellenmesi kararından, erişim engellendiği için bundan zarar gördüğünü kanıtlayan herkesin itiraz olanağı bulunmalıdır. Bu durumda, sitenin erişime kapatılması nedeniyle, bu siteye ulaşamayan herkesin mağdur sayılması ve bu nedenle de herkese itiraz olanağının tanınması uygun olacaktır.[65] Ancak CMK m. 260 ve 237 vd. düzenlemeleri, bu yoruma ne yazık ki engeldir.

Düzenlemedeki diğer bir sakınca, 8. maddenin 5. fıkrasında, içeriği yurt dışında olan veya yurt içinde olmakla birlikte, çocukların cinsel istismarı (TCK m. 103) veya müstehcenlik (TCK m. 226) içerikli veriler içeren sitelere erişimin Başkanlık tarafından re'sen engellenmesidir. Bu kararın Başkanlık tarafından verilmesi yürütmeye bağlı olan bir kurumun yargı yetkisini kullanması anlamına gelmektedir ki bu durum erkler ayrılığı ilkesini kabul etmiş bir hukuk devleti olan Türkiye'de kabul edilebilir bir yaklaşım değildir. Kaldı ki Başkanlık "*Başkanlık, Adalet Bakanlığı, İçişleri Bakanlığı; Çocuk, Kadın ve Aileden Sorumlu Devlet Bakanlığı ile Kurum ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile internet servis sağlayıcıları ve ilgili sivil toplum kuruluşları arasından seçilecek bir temsilcinin katılımı suretiyle teşkil edilecek*" bir kurum olması sebebiyle de siyasi bir kurumdur. Dolayısıyla, Başkanlık'ın görevi m. 8/5'e ilişkin bir durumla karşılaştığında bu durumu Cumhuriyet Savcılığı'na ihbar etmekle sınırlı olmalıdır.

---

64 Kayral, Kürşat; "İnternet Sitelerinin Filtrelendirilmesi" konulu sunum, Ankara Barosu Uluslararası Hukuk Kurultayı, 8 Ocak-11 Ocak 2008, *Bilişim ve Hukuk,* Cilt 2, Ankara Barosu Yayınları, 2009, s. 49.

65 Taşkın, *Bilişim Suçları,* s. 159.

Belirttiğimiz sakınca Yönetmelik'in 14. maddesiyle, biraz olsun giderilmiştir. Buna göre, Başkanlık'ın verdiği karar, TCK m. 103/1 veya TCK 226.madde kapsamındaysa ve bunlara ilişkin içerik veya yer sağlayıcı yurt içindeyse, 24 saat içerinde yargıcın onayına sunulacak; yargıç da kararını 24 saat içerisinde verecektir. Bu süre içerisinde tedbirin onaylanmaması halinde tedbir Başkanlık tarafından derhal kaldırılacaktır. Ancak bu düzenleme de konuyla ilgili eleştirilerimiz ve kaygılarımızı tam olarak gidermemiştir. Her şeyden önce kararı Başkanlık'ın vermesi, bir siyasi oluşum olması nedeniyle, yukarıda belirttiğimiz gerekçelerle Anayasa'ya aykırıdır. Yine de önemle belirtmek gerekir ki Başkanlık tarafından verilecek olan kararın, içerik veya yer sağlayıcının yurt içinde bulunması durumunda yargıç denetimine tabi tutulması olumlu bir gelişmedir. Ancak aynı düzenlemenin içerik veya yer sağlayıcının yurt dışında olması durumunda Başkanlık tarafından verilecek kararlar bakımından da uygulanması gerektiği kanısındayız.

Başkanlığın re'sen vereceği karara karşı nereye itiraz edileceğinin düzenlenmemiş olması da ayrı bir eksikliktir. CMK m. 267 vd. hükümlerinin Başkanlık'ın verdiği kararlar için uygulanabilmesi olanaksızdır. Başkanlık kararıyla erişimin engellenmesi durumunda, bu karar nedeniyle menfaati ihlal olan kişi ancak 2577 sayılı İdari Yargılama Usul Kanunu hükümlerine göre Başkanlık kararının iptali ve yürütmesinin durdurulmasını isteyebilecektir.

3.3. İçeriğin Yayından Çıkarılması ve Cevap Hakkı

5651 sayılı Kanun'un 9. maddesinde internet sayfasındaki içerik nedeniyle haklarının ihlal edildiğini düşünen kimseye, içeriğin kaldırılmasını ve düzeltme metninin yayınlanmasını isteme hakkı tanınmaktadır. Buna göre, hakkının ihlal edildiğini düşünen kimse önce içerik sağlayıcısına (web sitesinin içeriğini oluşturan kişiye) veya buna ulaşamıyorsa yer sağlayıcısına (Süperonline, Telekom gibi) başvurarak kendisiyle ilgili içeriğin yayından kaldırılmasını ve yayının kapsamından fazla olmamak ve en çok bir hafta ile sınırlı olmak kaydıyla, hazırladığı içeriğin internette yayınlanmasını isteyebilir. Bu istemin, içerik ya da yer sağlayıcı tarafından, kendilerine ulaştığı andan itibaren iki gün içerisinde yerine getirilmesi gerekmektedir. Bu süre içerisinde istem yerine getirilmezse reddolunmuş sayılır.

İstemi reddolunan kimse, ret tarihinden itibaren on beş gün içerisinde, isteminin yerine getirilmesi için sulh ceza yargıcından bu konuda bir karar vermesini isteyebilecektir. İstemin kapsamı, içerik veya yer sağlayıcıdan istenen istemle aynı olacaktır. İstemi alan sulh ceza yargıcı, üç gün içerisinde dosya üzerinden karar verir; bu karara karşı CMK hükümlerine göre hem kişi, hem de içerik veya yer sağlayıcı tarafından itiraz edilebilir.

Sulh ceza yargıcı istemi yerinde bulur ve karar da kesinleşirse, içerik veya yer sağlayıcı, kararın kendilerine tebliğinden itibaren iki gün içerisinde içeriği yayından çıkarıp gerekli yanıtı yayınlarlar. Mahkemenin kararına uymayan sorumlu hakkında, altı aydan iki yıla dek hapis cezası verilir. Sorumlu, eğer tüzel kişilikse, tüzel kişinin yayın sorumlusu hakkında aynı cezai yaptırım uygulanacaktır.

Düzenleme benzeri bir düzenleme Basın Kanunu md 14'te de mevcuttur; ancak Basın Kanunu ile konan düzenlemeye yöneltilen eleştiriler bertaraf edilmek istendiği için bu konu 5651 sayılı Kanun'la düzenlenmiştir. Bu yönüyle düzenlemenin doğru olduğunu ve basın kanunu hükümlerinin internet hakkında uygulanıp uygulanamayacağı yönündeki öğreti tartışmalarına son verdiğini düşünüyoruz.[66]

Son olarak, internet haberleşmesinin kısıtlanmasına ya da denetim altına alınmasına yönelik benzeri tedbirlere, bazı devletlerin gerek politik gerekse güvenlik kaygılarıyla başvurduğunu da belirtmeliyiz.[67] Örneğin Çin Halk Cumhuriyeti'ndeki *"sanal polis"*[68] uygulaması buna benzer bir önlemdir. 5651 sayılı Kanun uygulanırken bu tür aşırı kısıtlamalara yol açmayacak şekilde uygulanmalıdır; yorumlar özgürlükler ekseninde yapılmalıdır.

---

66 Konuyla ilgili geniş bilgi, eleştiri ve görüşler için bkz. sınar, Hasan, İnternet ve Ceza Hukuku, Beta Yayıncılık, 1. Baskı, İstanbul, Temmuz 2001, s. 145-149.

67 Benzeri kısıtlamaların Çin Halk Cumhuriyeti, Vietnam, İran, Özbekistan, Tunus, Vietnam hukuk sistemlerinde de var olduğu bilinmektedir. Ancak bu kısıtlamaların önemli bir bölümü, bizdekinin aksine, internet erişimine yasak koymak; bazı siyasi içerikli sayfalara erişimin engellenmesi amacıyla yapılmaktadır. (http://www.ntvmsnbc.com/news/402066.asp (22.10.2007). Beyaz Rusya, Burma, Kuzey Kore, Küba, Libya, Azerbaycan ve Orta Asya Cumhuriyetleri, Sierra Leone, Suriye, Sudan, Suudi Arabistan da internete yasak koyan ülkeler arasında gösterilebilir (Sınar, *İnternet ve Ceza Hukuku,* s. 105-110).

68 Buna göre, kullanıcıların ekranlarında beliren bir motosikletli sanal polis, kullanıcıları yasak sitelere girmemeleri yönünde uyarmaktadır .http://www.ntv.com.tr/news/418268.asp-03.09.2007 tarihli haber)-22.10.2007

Bilişim Özel Hukuku ve İnternet Bankacılığından Doğan Hukuki Sorumluluk

Bankalar güven ilişkisine dayanan kurumlardır. Bireyler, mevduatlarını bankalarına duydukları güven nedeniyle bankalarına emanet etmektedirler. Bu nedenle bankaların, müşterinin kendilerine olan güvenini korumaları ve bu güvene yakışır biçimde müşterilerinin zarar görmelerini önlemek yönünde çalışmaları, sistemlerini buna göre uyarlamaları gerekmektedir.

Nitekim Yargıtay 11. HD'nin 22.06.2006 tarih ve 2005-4748 E; 2006/7341 K. sayılı ilamında da özetle ''*Bir güven kurumu olarak faaliyet gösteren bankaların objektif özen yükümlüğünün yerine getirilmemesinden kaynaklanan hafif kusurlarından dahi sorumlu oldukları*'' dile getirilmiş ve ''*müşterisinin hesabında bulunan paranın, müşterinin haberi olmadan bilgisayar korsanlığı yoluyla başka bir hesaba aktarılmasının önlenmesi konusunda ek güvenlik tedbirleri almayan bankanın hafif kusurundan dahi sorumlu olduğu dikkate alınarak, müşterisinin zararını önlemek zorunda olduğu sonucuna varılmalıdır.*'' denilmekte ve yerel mahkemenin tamamen bankayı kusurlu bulan, davacıya müterafik kusur yüklemeyen kararı onanmaktadır. Bu karara karşı davalı vekilince yapılan karar düzeltme itirazı da 24.11.2006 tarihinde aynı daire tarafından 2006/11943E; 2006/12226 K. sayılı kararla reddedilmiştir.

Aynı yöndeki bir kararın Antalya Asliye Ticaret Mahkemesi tarafından verildiği görülmüştür.[69] Bu karara konu olan olayda, bir iş adamının bilgisayarına virüs gönderilerek şifreleri kırılmış ve hesaptan değişik hesaplara 30.000 YTL havale/ EFT yoluyla para aktarılmış; aktarılan hesaplardan şebeke olarak çalışan üçüncü kişiler tarafından para çekilmiş, bunun üzerine zarara uğrayan davacı banka aleyhine dava açmış ve mahkeme davalı bankayı kusurlu bularak, davalıyı tazminata mahkum etmiştir.

Bu kararların da ışığında belirtmek gerekir ki bir ticari işletme olan bankaların Türk Ticaret Kanunu'na (TTK m. 20/2) ''*basiretli tacir*'' gibi davranması da ticaret hukukunun temel ilkelerindendir.

Basiretli tacir ilkesinden anlaşılması gereken, geniş anlamda bir edimin yerine getirilmesindeki bütün önlemleri almak ve herhangi bir

[69] www.bilisimsuclari.com/2007707/13/internet-bankaciligi-zararini-banka-oduyor/ (Erişim Tarihi: 29.02.2008).

akdi yükümlülük altında bulunulmuyor olunsa dahi basiretli tacir olmanın gerekliliklerindir. Basiretli tacir ölçütü değerlendirilirken, tacirin kişisel durum ve yeteneğine göre (öznel=subjektif ölçüt) değil, nesnel (objektif) ölçüte göre yoruma başvurmak ve kendisiyle aynı sınıfa dahil, tedbirli ve muktedir bir tacirin aynı durumda göstereceği özen ölçütünden hareket etmek gerekir.[70]

Bu belirlemeler ışığında, internet bankacılığında, bireylere ve bankalara düşen ödevlerle, tarafların hukuki sorumluluğuna değinmek gerekmektedir.

a. Bir Bankanın, kısa aralıklarla ve yüksek meblağlı havale işlemlerini fark etmesine rağmen (hizmeti banka verdiği ve sistemi banka yönettiği için sistemdeki hareketten haberdar olmaması düşünülemez) müşterisinin hesabından bir başka hesaba havale/EFT yapıldığı anda SMS/ mail (ya da her ikisi birden) ile müşterisine uyarı iletisi gönderdiğine yönelik bir uygulaması ya da bankanın müşterisini telefonla arayarak hesap hareketleri konusunda müşterisini uyardığı, hesap hareketleri hakkında müşterisinin haberinin olup olmadığının onayını aldığı yönünde bir uygulaması yoksa, tazminat hukuku ilkeleri gereğince sorumluluğuna gitmek gerekir kanısındayız.

Ancak bu noktada şunu da belirtmekte yarar vardır ki kendisine internet bankacılığı hesabı açılan bir kişinin günlük EFT/havale işlem limiti ne kadardır? Bu limit konusunda banka hesap açarken müşterisinden günlük EFT/havale limitini sormuş mudur? Müşterisinin bu yöndeki beyanını almış mıdır? Ayrıca her ne kadar bankanın tüm müşterilerinin günlük hesap hareketlerinin sıklığını düzenli olarak denetlemesi, günlük internet bankacılığı işlem hacmi bakımından pek olası görünmese de, belli bir müşterisinin genellikle yaptığı işlem sayı ve EFT/havale gönderdiği rakamların değerine göre, eğer hesabında olağanın üzerinde bir hareketlilik yaşanmakta ise, o müşterisini bu olağanüstü hesap herketi konusunda uyarması hatta gerekirse hesaba bloke koyması gerekir.[71] Bu konuya dikkat etmeyen bir banka da basiretli davranmış sayılamayacaktır.

---

[70] İmregün, Oğuz, *Kara Ticareti Hukuku Dersleri,* 8. Bası, Evrim Dağıtım, İstanbul, 1987, s. 36.

[71] Atamer, M. Yeşim, ''İnternet Bankacılığının Üçüncü Kişiler Tarafından Kullanımı Nedeniyle Doğan Zararı Kim Taşır?'', *Banka Hukuku ve Yargıtay Kararları Sempozyumu,* 8 Haziran 2007, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayın-

Banka bu konuda şöyle basit bir önleme başvurabilir: Sözgelimi, bankanın 500 TL veya üzeri olan havale/EFT emirlerinde/ işlemlerinde kullanıcısının cep telefonuna kısa mesajla ve mail hesabına iletiyle ''*...numaralı hesabınızdan 500 YTL havale/EFT emri verilmiştir. Bilgi için 444 ... numarayı arayınız.*'' (Bu tür bir uygulamaya bazı bankalar başvurmaktadır. Kaldı ki bu uygulama bankaya çok fazla ek maliyet getirmez ve bankada zaten müşterisinin bilgileri mevcuttur.)

Bankanın, öncelikle bu türden bir hizmeti kullanıcıya sunmuş olması ve kullanıcıya bu yönde bir uyarı mesajı için limit belirleme olanağı tanıması (bu, günlük EFT/havale limiti belirleme işleminden farklıdır; ek bir güvenlik önlemidir) hatta kanaatimizce, kullanıcının takdirine bağlı olmaksızın, sözgelimi 1000 TL ve üzeri emirler için bu yönde bir uyarı iletisi veya mesajını kullanıcıya, kullanıcının istemi olmaksızın göndermesi gerekmektedir. Bankanın bu yönde bir güvenlik önlemi alması gerekirken, almaması özensiz davrandığını ve bankanın ağır ihmalini ortaya koyacaktır.

Bankaların pek çoğu tarafından havale veya EFT işlemlerini internet üzerinden ayrı bir parola ile yaptırabilme olanağı sunması önemli bir güvenlik önlemi olmakla birlikte, yeterli güvenliği sağlamaktan uzaktır. Zira bilişim sistemine giren bir fail, eğer bu işlemi şifre kırma *(cracking)* yoluyla yapmışsa, şifre kırma bakımından yetenekli olduğu kabul edilir ve eft veya havale için öngörülen şifreyi de kırabilmesi olanak dahilindedir. Zira şifre kırma konusunda yeteneği olan bir failin, bilişim konusunda ortalamanın üzerinde bilgisi olduğunu kabul etmemek için bir neden yoktur. Dolayısıyla, bankanın EFT/havale işlemleri için müşterisinden ayrıca bir şifre istemesi, bilişim korsanlarını önlemek bakımından yeterli bir güvenlik önlemi sayılamaz. Sisteme girebilen üçüncü kişiler bu şifreyi de rahatlıkla değiştirebileceklerdir. Aynı belirlemeler internet şubesi üzerinden EFT/havale limitinin arttırılması için de geçerlidir. O halde, limit belirleme işi müşteriye bırakılmamalı, bunu banka kendiliğinden yapmalıdır.

Öte yandan, bir bankanın ayrı bir şifre istiyor olsa da EFT/havale limitini arttırma işlemini internet şubesinden gerçekleştirmesine izin vermesi de özensiz davrandığını göstermektedir. İnternet üzerinden limit azaltılabilmeli ancak, arttırılamamalıdır. Arttırılması için, banka-

ları (T. İş Bankası AŞ Vakfı), Sözkesen Matbaacılık, Ankara, 2007, s. 49.

nın müşterisinden, limit artırımı yönünde ''*yazılı muvaffakat*'' alması gerekir.

b. Bir banka, internet üzerinden verilecek olan bir emirle vadeli döviz hesabının TL'ye çevrilmesine izin vermişse ve bu işlemin yapılması için müşterisinin de yazılı onayını almamışsa ağır ihmalinden söz edilmelidir. Zira uygulamada pek çok bankanın internet üzerinden vadeli döviz hesabını TL hesabına çevirtmek veya vadeyi bozdurmak için müşterisinin yazılı beyanını aldıkları bilinmektedir. Bu beyan olmadığı takdirde, bankalar, kullanıcısı internet üzerinden bu yönde bir talimat vermiş olsa dahi istenen işlemi güvenlik gerekçesiyle yapmamaktadır. Bu yaklaşım, doğru bir yaklaşımdır.

c. Bir banka internet bankacılığı hesabı açarken, hesap açılışı sırasında kendiliğinden bir limit koymayıp, limit belirlemeyi kullanıcının takdirine bırakmıyorsa, kullanıcı dilerse uygun gördüğü limiti (sıfır bakiyeli olarak da) belirleyebilecektir. Bundan çıkan sonuç, kullanıcının ayrıca ve aksi yönde bir talimatı olmadıkça internet bankacılığında bankanın kendi günlük işlem üst limitlerinin uygulanabildiğidir.

Başka bir deyişle, sözgelimi, kullanıcıya internet bankacılığı hesabı açarken, bankanın kendiliğinden 1000 TL'lik EFT ve havale limiti koyması, bu limiti ancak kullanıcısının ayrıca ve açıkça yazılı talimatı olursa, onun belirlediği rakama çıkarması, internet üzerinden kullanıcılara EFT/havale limitlerini arttırma seçeneği sunmaması (ancak azaltma olanağı sunması mümkün olabilir) güvenlik açısından alınabilecek diğer basit önlemlerdendir ve uygulamada pek çok bankanın bu yöntemi izlediği bilinmektedir. Bu şekildeki basit bir önleme başvurmayan bankanın da ağır ihmalinin olduğu söylenebilecektir.

d. Bankaların, internet şubesi kullanıcılarına, ''*akıllı SMS, akıllı anahtar, şifrematik*''[72] güvenlik sisteminden yararlanma olanağı tanımasına rağmen kullanıcının bu olanaktan yararlanmaması durumunun da değerlendirilmesi gerekir. Böyle bir durumda, bankanın, kullanıcılarına bu olanağı tanıması özenlice davrandığını göstermektedir ancak bu olanağı kullanıcılarının ''*takdirine*'' bırakması bankanın yeterli özeni göstermediği yönünde bir karinedir.

---

[72] Geniş bilgi için bkz www.garanti.com.tr/subesiz/internet_bankaciligi/guvenlik/sifrematik/ (Erişim Tarihi: 02.01.2009)

Her cep telefonunun *"java"* uyumlu bir program olan kullan-at ve benzeri bir programla uyumlu olması ya da kullanıcının bu programı telefonuna yüklemesi (ya da buna uyumlu bir telefon satın alması) kullanıcıdan beklenemeyeceği için, bu programla uyumlu olmayan ya da uyumlu olmasına rağmen bu programı kullanmayan veya kullanmak istemeyen müşterilere hitaben bankaların, müşteriler bakımından ortalama 20 TL civarında maliyeti olan ve bir anahtarlık gibi de kullanılabilen *''şifrematik''* tarzı küçük anahtarlık boyutunda ve her seferde ayrı bir şifre üreten cihazlardan yararlanma olanağını müşterisine sunması gerekir.

Hatta kanaatimizce, internet bankacılığından yararlanmak isteyen kullanıcılarına *''akıllı SMS, akıllı anahtar, şifrematik,''* gibi uygulamalardan birini, diğer güvenlik önlemlerinin yanı sıra, güvenlik açısından zorunlu tutması banka açısından basiretli bir tacirden beklenen bir yaklaşım olmalıdır.

Bankanın bu olanağı vermiş olmasına rağmen davacının bu olanaktan yararlanmamış olması durumunda bile, kanımızca kullanıcıya atfedilecek bir kusur yoktur.Bankanın ağır ihmali söz konusudur. Zira kullanıcısına internet bankacılığı hizmetinden yararlanma olanağı veren bankanın hafif ihmalinden dahi sorumlu olduğu[73] düşünüldüğünde, müşterisinin zarar görmemesi için gerekli olan önlemleri almak ve bunları gerektiğinde zorunlu tutmak bankanın ödevidir. Başka bir deyişle, müşterilerin şifrelerinin üçüncü kişilerin eline geçmemesi konusunda koruma önlemleri geliştirmek bankaların görevidir.[74]

Türkiye'deki bankacılık uygulamasında, şifrenin çalınmasını güçleştirecek PIN-TAN gibi güvenlik uygulamaları bulunmamaktadır. Bu önlem, Alman Bankacılık uygulamasında oldukça yaygındır. Buna göre, banka tarafından kullanıcıya bir internet bankacılığı şifresi (PIN) atanır (veya kullanıcı bunu belirler) ve ayrıca banka müşterisinin bildirdiği adresine TAN (tek kullanımlık şifre) gönderir. Sistem ancak bu iki şifrenin bir araya getirilmesiyle açılabilir. Bir başka deyişle, bilişim hırsızlarının sisteme girebilmeleri için hem bu PIN kodunu öğrenme-

---

73 Reisoğlu, Seza, ''Tartışmalar''; Sempozyum, s.45; Atamer, "İnternet Bankacılığı", Sempozyum, s. 46; aynı yönde Özdamar, Naci, "İnternet Bankacılığı ve Banka Kartları" konulu sunum, *Ankara Barosu Uluslararası Hukuk Kurultayı*, 8 Ocak-11 Ocak 2008, Bilişim ve Hukuk, Cilt 2, Ankara Barosu Yayınları, 2009, s. 70.

74 Atamer, "İnternet Bankacılığı", Sempozyum, s. 24.

leri hem de kullanıcının adresine giderek TAN numaralarını içeren bu belgeyi çalmaları gerekir ki bu da oldukça küçük bir olasılıktır. Ancak, bu (veya benzeri) önlemi almak banka açısından oldukça kolaydır.[75]

e. Çoğu müşteri veya internet kullanıcısı, internetteki tehlikelerin farkında değildir. Bu türden bir uyarıya ulaşmak da müşterinin aktif bir davranışını (o linke tıklamasını) gerektirdiğinden, çoğu müşterinin bu linke tıklamadan işlem yaptığı görülmektedir.[76] Dolayısıyla, bir bankanın internet sitesinde kullanıcının aktif davranışı ile internet bankacılığından doğan tehlikeler hakkında ekran açılıyorsa, bankanın kusurunun varlığı kabul edilmelidir. Zira, böyle bir durumda banka, aydınlatma yükümlülüğünü yeterince yerine getirmemiş sayılır. Olması gereken, tehlikelere ilişkin uyarının internet bankacılığı ekranı açıldığında, kendiliğinden kullanıcının ekranında belirmesi ve kullanıcı kapatmadığı sürece de açık kalmasıdır.

Eğer kullanıcı bu uyarıya rağmen umuma açık bir bilgisayardan internet şubesine girmişse ve bunun sonucunda hesabına girilmesine neden olmuşsa, hükmedilecek tazminatta indirime gidilmesi Yargıtay'ın da kararlarının gereğidir. Nitekim Yargıtay 11. HD 12.09.2003 tarih ve 2003-8280 Es/ 2003-7705 K. sayılı ilamında, ''*Banka tarafından verilen internet şifresinin özenle saklanma yükümlülüğünün, internet hizmet sözleşmesi gereğince, kullanıcıya ait olduğu, şifrenin başkası tarafından kullanılarak hesaptan para havale edilmesi durumunda bankanın hukuki sorumluluğuna gidilemeyeceği*'' belirtilmiştir.[77]

Ancak kullanıcı umuma açık bir yerden internet şubesini kullanmış dahi olsa, bankanın yukarıda açıkladığımız ''*akıllı anahtar, akıllı SMS, akıllı cep, şifrematik..*'' gibi güvenli bir yolu müşterisinin *zorunlu* kullanımına sunmuş olması durumunda zararın oluşmasının büyük ölçüde önüne geçilebilecektir. Zira bu tür bir sistem kullanıldığında, müşterinin internet bankacılığı şifrelerine ulaşmak (sisteme korsan giriş) olanaksız olmasa da oldukça güçtür. Fakat buna rağmen, bir müşterinin umuma açık bir bilgisayardan internet bankacılığı hesabına girmesi başlı başına kendisine kusur atfedilmesi için yeterli bir gerekçe olmamalıdır. Zira hiçbir internet bankacılığı kullanıcısına ''*mut-*

---

75 Atamer, "İnternet Bankacılığı", Sempozyum, s. 25.

76 Atamer, "İnternet Bankacılığı", Sempozyum, s. 26.

77 www.kazanci.com.tr (Erişim Tarihi: 16.04.2008).

laka kendi bilgisayarından hesabına eriş'' diye bir yaklaşım günümüz yaşamının gerçekleriyle de bağdaşmamaktadır.

İkinci olasılık ise kullanıcının umuma açık olmayan bir bilgisayardan internet şubesine erişim sağlamasıdır. Eğer davacı, sürekli olarak kendi bilgisayarından internet şubesine erişim sağlamışsa ve sisteminde de Truva atı[78] gibi casus programları ortaya çıkaran güvenlik duvarları yüklü değilse, davacının bilişim sistemine girilmiş ve bu yolla şifreleri ele geçirilmiş demektir. Casus programları ortaya çıkaran güvenlik yazılımları sistemde yüklü olsa dahi bilişim korsanlarının şifreleri kırması mümkün olabilmektedir. Bu durumda da *''akıllı SMS''* gibi yazılımların önemi ortaya çıkmaktadır. Bu tür programlar, bilişim suçu faillerinin sisteme sızmalarını büyük ölçüde önlemektedir. Böyle bir durumda, bankanın bu programdan yararlanmayı *''tercihe''* bırakması onun ağır ihmalini göstermektedir.

Bu başlıkta (biraz yukarıda) belirttiğimiz Yargıtay kararının geçerli olduğu olaylara örnek olarak, *internet bankacılığı kullanıcısının şifresini herkesin rahatlıkla ulaşabileceği şekilde, uluorta bir yerde özensizce saklaması (sözgelimi bir kağıda yazıp kağıdı ortalıkta bırakması ya da çok kişinin kullandığı bilgisayara kaydetmesi, ya da şahsi bilgisayarında ve şifre koymadan bir klasöre şifresini kaydetmesi gibi) gibi* bir durumun varlığı gerekir. Böyle bir durumda da hiç kimsenin kendi kusuruna dayanarak hak iddia edemeyeceği yönündeki temel hukuk ilkesi yürürlüğe girer ve tazminata hükmedilecekse de bundan indirime gidilebilir veya tazminat verilmeyebilir.

Olayın daha sağlıklı değerlendirilmesi bakımından, şöyle bir örnek vermek uygun olacaktır: *''Nasıl ki kişinin kendi evinden parasının çalınması durumunda, kusurlu olup olmadığı tartışması-sigortalı olduğu haller dışında –yapılmazsa, bankanın malvarlığına dahil olan paranın çalınması halinde de bu tartışma yapılmaz. Dolayısıyla bankanın, müşterinin hesabına*

---

78 Truva atı gibi programlar, güvenilir kişiden gelmiş gibi görünen bir elektronik iletinin arkasına saklanır ve sisteme o şekilde sızarlar. Kullanıcı, gelen iletiyi, ileti tanıdığı kişiden geldiği için kuşkulanmadan açar ve sistemine kurar. Ancak, sisteme kurulan ve masum gibi görünen yazılım sinsice kendisini bilgisayara saklar ve kullanıcının şifrelerini ele geçirip, casus programı gönderen kişinin bilgisayarına bu şifreleri gönderir. (Truva atı ve diğer korsanlık yöntemleri için bkz Dülger, M. Volkan, *Bilişim Suçları,* Seçkin Yayınları, Birinci Baskı, Ankara, Kasım 2004, s. 69; *Yazıcıoğlu*, *Bilgisayar Suçları,* s. 153; Kurt, *Bilişim Suçları,* s. 63).

bu meblağı borç kaydetme imkanı, kural olarak, yoktur…[79] *Hırsız gerçi bankanın ''evine'' girmiştir. Ama hırsızın bunu yapabilmesi için ''anahtarı'' ona müşteri sağlamış veya ihmalin sonucunda ''pencereyi açık bırakmışsa''' bankanın ona karşı bir tazminat istemi olacağı açıktır. Doğaldır ki müşteri sadece kusuru ile orantılı bir tazminat yükümlülüğü altında olabilir. Yani, bankanın evine hırsız girmesinin rizikosunu tümden müşteriye aktarması imkanı yoktur."*[80]

Bu bilimsel görüşün ışığında denilebilecektir ki bir korsanlık olayında sisteme girenler *''bankanın evine''* girmişlerdir. Sonuçta girilmiş olan bir ev söz konusudur; evde bir hırsızlık olmuştur. Konunun temel noktası budur. Eve nasıl girildiği ise, ikincil noktadır. Ayrıca, kanımızca, bir olayda, sisteme girmede davacının kusurlu olduğunun ispatı da davalı bankaya düşer. Bunun için, bankanın öncelikle, davacının internet hizmet sözleşmesine aykırı davrandığını kanıtlaması gerekecektir. Sözleşmeye aykırı davranışın banka tarafından ispatlanması yetmez; bu davranış nedeniyle bir zarar doğduğu ve bu zararla, zarar doğuran davranış arasında da nedensellik bulunduğunu da banka ispatlamak durumundadır.[81]

Ayrıca belirtmek gerekir ki Yargıtay, bankalar tarafından sunulan *"sanal klavye"* gibi hizmetlerin internet bankacılığından doğan zararları ve internet korsanlıklarını önlemek için yeterli olmadığına karar vermiştir. (11. HD 22.06.2006 tarih ve 2005/4748 E; 2006/7341 K sayılı kararı)[82] Ayrıca, adı geçen kararda, internet üzerinden yapılan usulsüzlüklerde öncelikle bankanın sorumluluğunun benimsenmesi de dikkati çekmektedir.

Bilişim Suçlarının Önlenmesi ve Alınacak Önlemler

Bilişim suçlarının önlenmesi ve faile ulaşılması, bu suçların dinamik yapısı nedeniyle ciddi anlamda sorun oluşturabilmektedir. Zira bu suçlar çok hızlı bir gelişim içerisindedir.

---

79 Atamer, "İnternet Bankacılığı", Sempozyum , s. 18.

80 Atamer, "İnternet Bankacılığı", Sempozyum, s. 21.

81 Aynı yönde, Atamer, "İnternet Bankacılığı", Sempozyum, s. 27.

82 Aktaran Çeker, Mustafa, "İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden Bankaların Sorumluluğu", *Prof. Dr. Hüseyin Ülgen'e Armağan,* İkinci Cilt, Vedat Kitapçılık Basım Yayım, İstanbul, 2007, s. 1350.

Bilişim suçlarının aydınlatılmasında, gerek bireylere gerekse devlete önemli görevler düşmektedir. Devlete düşen görevlerden ilki, faile ulaşmanın çabuklaştırılması için öncelikle uluslar arası işbirliğine önem verilmektir. Bunu sağlamak için de ülkemizin, Avrupa Konseyi Siber Suçlar Sözleşmesi'ne bir an önce taraf olması sağlanmalıdır. Bu bağlamda, uluslar arası polis teşkilatı (İnterpol) ile de Türk polis teşkilatının işbirliği içerisinde olması önem taşımaktadır.

Uluslararası işbirliğinin diğer boyutu ise, uluslar arası bilgi paylaşımıdır. Bu bağlamda, bir suça karışan IP adresinin nerede olduğunun ve bu IP'nin servis sağlayıcısının kim olduğu ile bu IP'nin kime ait olduğu; gerekirse bu IP'ye ait web-log kayıtları da soruşturma makamları ve mahkemelerle paylaşılmalıdır.

Bireylere ve tüzel kişilere düşen önemli görevlerden en başta geleni ise, kullandıkları bilişim sisteminin güvenliğini sağlamaktır. Güvenlik arttırıcı yazılımların yüklenmesi, sisteme yönelik korsan saldırıları önemli ölçüde engelleyecektir. Diğer yandan, özellikle bankalar veya büyük çaplı şirketler, bilişim suçuna maruz kalmanın kendi saygınlıklarını önemli oranda zedeleyeceğini düşünerek yetkili mercilere başvurmakta duraksama yaşamaktadırlar. Bu şekilde, çoğu suç soruşturmaya uğramamaktadır. Unutmamak gerekir ki faile ulaşmadaki en küçük bir kuşku ya da duraksama (veya devlet açısından gecikme) bilişim suçu faillerine yeni eylemler için zaman ve olanak kazandıracaktır. Durum böyle olunca, mağdur olan bireylerin veya şirketlerin soruşturma makamlarına başvurusu teşvik edilmeli, hatta devlet tarafından bilişim suçlarının ihbarı için Avrupa'da olduğu gibi *"Alo İhbar Hattı"* kurulmalıdır.

Bireylere veya tüzel kişilere düşen diğer önemli bir görev ise, özellikle internet bankacılığından doğan riskleri azaltmak için, hemen hemen her banka tarafından ücretsiz veya cüz'i ücretle sağlanan ve her işlem için, kullanıcının belirlediği sabit şifrenin yanı sıra, tek kullanımlık şifre atayan *"KULLAN-AT"*; *"ŞİFREMATİK"* gibi yazılımların kullanılmasıdır. Bu yazılımların kullanılması sonucunda, bir şekilde bilişim sistemine erişim sağlanarak korsanlar tarafından sabit şifreler elde edilmiş olsa da kullanıcının kendisinin belirlediği kodla açılan ve cihaza ulaşamayan korsanlar sistemdeki verilere de ulaşamayacaklardır. Korsanların internet bankacılığına girebilmesi için, bu cihaza ulaşmaları ve ayrıca bu cihazın şifre atamsı için gerekli olan ve kullanıcı tara-

fından belirlenen şifreye de ulaşmaları gerekmektedir ki bu da bilişim korsanlarının işini oldukça güçleştirmektedir.

Zararların önlenmesi için, kanaatimizce, internet bankacılığı için başvuran kullanıcılara bankaların bu tür uygulamaları zorunlu kılması, doğabilecek zararlı sonuçları en baştan önleyecektir.

Yine bireylere düşen önemli görevlerden birisi de internet üzerinden yapılan alışverişlerde her alışveriş için ayrı limit oluşturma olanağı tanıyan ve başlangıçta 0 (sıfır) limitle oluşturulan; bireyler için hiçbir ek maliyet getirmeyen "*sanal kart*" kullanmaktır.[83] Burada, müşteri sözgelimi 20 TL'lik bir alışveriş yapacaksa, yalnızca o alışveriş için 20 TL'lik bir limit belirler ve alışverişini yapar, Bu alışveriş, asıl kartın ekstresine eklenir ve bu borçla birlikte tahsil edilir. Sanal kartın ayrı bir güvenlik kodu, ayrı bir son kullanma tarihi ve ayrı bir kart numarası bulunur ancak limiti asıl kartın limiti ile sınırlıdır. Bir başka deyişle, sanal kart somut varlığı olmayan bir tür ek karttır. Her alışverişte limiti kullanıcı belirlediğinden, kart numarasının bir başkası tarafından öğrenilmesi durumunda dahi, sistem alışveriş yapmaya ve limit aşımına olanak taşımaz. Bu da internet dolandırıcılıklarının önüne geçmekte ve doğabilecek zararı azaltmaktadır.

Bilişim korsanlığına maruz kalan (sözgelimi bilgisayarına erişilerek MSN şifresi çalınan ya da internet bankacılığı şifresi ele geçirilen) kişinin, bilgisayarını ne durumdaysa o durumda bırakması önem taşımaktadır. Bunu daha açık biçimde şöyle ifade edebiliriz. Bir bilgisayarda, Windows'un sadece çalıştırılması bile bilgisayardaki dijital verilerin ve delillerin milyonlarcasının kaybolmasına yol açabilmektedir.[84] Dolayısıyla, bilişim korsanlığına maruz kalan birey, bilgisayarı açıksa açık, kapalıysa kapalı konumda bırakmalı ve verilerin yok olmasını önlemek için o bilgisayarda hiçbir işlem yapmadan derhal teknik bilirkişiden destek alarak, bilgisayara yüklenen zararlı yazılımlar ve mümkünse IP adresi hakkında rapor almalıdır. Gerektiğinde bu rapor, soruşturma makamlarına ışık tutacak ve belki de faile ulaşılmasını da sağlayacaktır. Uygulamada, en çok hata bu noktada yapılmakta ve veriler kaybolmadan sıcağı sıcağına bilgi alınmamaktadır. Oysa bilişim

---

83 Geniş bilgi için bkz www. garanti. com.tr / kredi_ kartlari / sanal_ kredi_ kartlari /sanal_ kredi_ kartlari_ hakkinda.html (Erişim Tarihi: 02.01.2009).

84 Smıth/ Grabosky/Urbas, *Cyber Criminals,* s. 81 (Aktaran ve çeviren : Taşkın, *Bilişim Suçları,* s.179, dipnot 720).

korsanlığının aydınlatılmasında bu yöndeki bir teknik çaba da oldukça önemlidir.

Sonuç ve Değerlendirme

İnternet, sınırsız özgürlük içeren bir yapıdır. Bu yapı üzerinde denetim kurmak oldukça güçtür. Ancak, yukarıda değindiğimiz önlemlere benzeyen basit, ucuz ve etkili önlemlerle doğacak zararlar daha en baştan engellenebilecektir. Unutulmamalıdır ki internetten yararlanırken zarar görmemek öncelikle kullanıcıların bilinçli hareket etmesiyle mümkündür.

KAYNAKLAR

Basılı Kaynaklar

Akdeniz, Yaman, "Controlling İllegal And Harmful Content On The İnternet", Crime and The Internet, Edited by David S. Wall, First Published 2001, by Routledge, London, s. 117.

Atamer, M. Yeşim, ''İnternet Bankacılığının Üçüncü Kişiler Tarafından Kullanımı Nedeniyle Doğan Zararı Kim Taşır?'', *Banka Hukuku ve Yargıtay Kararları Sempozyumu,* 8 Haziran 2007, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları (T. İş Bankası AŞ Vakfı), Sözkesen Matbaacılık, Ankara, 2007, s. 15-s. 50.

Çeker, Mustafa, "İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden BankalarınSorumluluğu", *Prof. Dr. Hüseyin Ülgen'e Armağan,* İkinci Cilt, Vedat Kitapçılık Basım Yayım, İstanbul, 2007, s. 1335-1350.

Dönmezer, Sulhi, *Kişilere ve Mala Karşı Cürümler,* Beta Yayıncılık, 16. Baskıdan Tıpkı

17. Baskı, İstanbul, Ekim 2004.

Dülger, M. Volkan, "Avrupa Konseyi Ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", *İstanbul Barosu Dergisi,* Cilt 78, Sayı 2004/4, S.1488-1493.

Dülger, M. Volkan, *Bilişim Suçları,* Seçkin Yayınları, Birinci Baskı, Ankara, Kasım 2004.

Erbaşı, Aslıhan Ayşe, "Çocuk Pornografisi", *İstanbul Barosu Dergisi,* Cilt 81, Sayı 2007/4, s.1609-1647.

Hedley, Steve, *The Law Of Electronic Commerce And The Internet İn The Uk And Ireland,* Cavendish Publishing, First Edition, London, 2006.

Helvacıoğlu, Aslı Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümleri'nin İncelenmesi", *İnternet ve Hukuk,* Derleyen: Yeşim M. Atamer, Bilgi Üniversitesi Yayınları, 1. Baskı İstanbul, Ocak 2004, S. 280 vd.

İmregün,Oğuz, *Kara Ticareti Hukuku Dersleri,* 8. Bası, Evrim Dağıtım, İstanbul, 1987.

Karagülmez, Ali, *Bilişim Suçları Ve Soruşturma-Kovuşturma Evreleri,* Seçkin Yayıncılık, Ankara, 1.Baskı, Mayıs 2005.

Kardaş, Ümit, "Bilişim Dünyası ve Hukuk", *Karizma Dergisi,* Sayı 13, 01.03.2003, s. 16

Kayral, Kürşat, "İnternet Sitelerinin Filtrelendirilmesi" konulu sunum, *Ankara Barosu Uluslararası Hukuk Kurultayı,* 8 Ocak-11 Ocak 2008, Bilişim ve Hukuk, Cilt 2, Ankara Barosu Yayınları, 2009, s. 49.

Kurt, Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayıncılık, Ankara, 2005.

Nebil Sarp, Füsun, "İnternet Sitelerinin Filtrelendirilmesi" konulu sunum, *Ankara Barosu Uluslararası Hukuk Kurultayı,* 8 Ocak-11 Ocak 2008, Bilişim ve Hukuk, Cilt 2, Ankara Barosu Yayınları, 2009, s. 41.

Nuhoğlu, Ayşe, *Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması,* Analiz Basım Yayın, İstanbul, 2002.

Özdamar, Naci, "İnternet Bankacılığı Ve Banka Kartları" Konulu Sunum, *Ankara Barosu Uluslararası Hukuk Kurultayı,* 8 Ocak-11 Ocak 2008, Bilişim ve Hukuk, Cilt 2, Ankara Barosu Yayınları, 2009, s. 70.

Özkul, Davut, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", *Sayıştay Dergisi,* Sayı 44-45, 01.06.2002

Reisoğlu, Seza, ''Tartışmalar''; 'İnternet Bankacılığının Üçüncü Kişiler Tarafından Kullanımı Nedeniyle Doğan Zararı Kim Taşır?'', *Banka Hukuku ve Yargıtay Kararları Sempozyumu,* 8 Haziran 2007, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları (T. İş Bankası AŞ Vakfı), Sözkesen Matbaacılık, Ankara, 2007, s. 45.

Sınar, Hasan, *İnternet ve Ceza Hukuku,* Beta Yayıncılık, 1. Baskı, İstanbul, Temmuz 2001.

Smıth Russel/Grabosky, Peter/Urbas, Gregor, *Cyber Criminals On Trail,* First Published By Cambridge University Press, Cambridge, 2004.

Soyaslan, Doğan, *Ceza Hukuku Özel Hükümler,* Gözden Geçirilmiş 6. Baskı, Yetkin Yayınevi, Ankara, 2006.

Soysal, Tamer, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", *Türkiye Barolar Birliği Dergisi,* Sayı 61, Kasım-Aralık 2005, s. 304-309.

Taşkın, Şaban Cankat, *Bilişim Suçları,* İstanbul, Beta Yayıncılık, Kasım 2008.

Tezcan, Durmuş/ Erdem, Mustafa Ruhan/Önok, Murat, *Teorik Ve Pratik Ceza Özel Hukuku,* 5560 sayılı Kanuna Göre Güncellenmiş 5. Baskı, Seçkin Yayıncılık, Ankara, 2007.

Yargıtay Kararları Dergisi

Yazıcıoğlu, R. Yılmaz, *Bilgisayar Suçları,* İstanbul, Alfa Yayınevi, Ekim 1997.

İnternet Kaynakları

www.kazanci.com.tr (Erişim Tarihi: 16.04.2008)

www.garanti.com.tr/subesiz/internet_bankaciligi/guvenlik/sifrematik/ (Erişim Tarihi : 02.01.2009)

www. garanti. com.tr/kredi_kartlari/sanal_kredi_kartlari/sanal_kredi_kartlari_hakkinda.html (Erişim Tarihi: 02.01.2009).

www.bilisimsuclari.com/2007707/13/internet-bankaciligi-zararini-banka-oduyor/
(Erişim Tarihi: 29.02.2008)

http://www.ntv.com.tr/news/418268.asp-03.09.2007 tarihli haber)-Erişim Tarihi: 22.10.2007
(http://www.ntvmsnbc.com/news/402066.asp-
(Erişim Tarihi: 22.10.2007)

http://tr.wikipedia.org/wiki/Üretim (Erişim Tarihi: 19.01.2009)

http://www.tdk.gov.tr/TR/SozBul.aspxF6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=veri (Erişim Tarihi: 26.01.2009)