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 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 hiçbir fark yoktur. 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.

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 157)

Kanaatimizce, dolandırıcılığın nitelikli hali olan ve TCK 158/1.f'de tanımlanan bilişim sistemlerinin kullanılması suretiyle gerçekleştirilen dolandırıcılık eylemi şu anda bilinen bilişim suçlarının hiçbirinde uygulama alanına sahip değildir. Zira, bir eylemin dolandırıcılık olarak değerlendirilmesinin en temel koşulu, hileli hareketlerin bireye karşı yapılması gerekmektedir. Oysa, TCK 158/1.f'de bireye karşı olan bir hileli hareket söz konusu değildir.

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.

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 (interpol) ile de Türk Polis Teşkilatının işbirliği içerisinde olması önem taşımaktadır.

Uluslar arası 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 tarafından belirlenen şifreye de ulaşmaları gerekmektedir ki bu da bilişim korsanlarının işini oldukç agüçleştirmektedir.

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. 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 kullancı belirlediğinden, kart numarasının bir başkası tarafından öğrenilmesi durumunda dahi, sistem alışveriş yapmaya ve limit aşımına olanak taşımaz. Bu da internet dolandırıcıklarının önüne geçmekte ve doğabilecek zararı azaltmaktadır.

Bilişim korsanlığına maruz kalan (sözgelimi bilgisyarına 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. Dolayısıyla, bilişim korsanlığına maruz kalan birey, bilgisyarı açıksa açık, kapalıysa kapalı konumda bırakmalı ve verilerin yok olmasını önlemek için o bilgisayarda hiçbir işlem yapmadan derhal teknik bilirkişiden destek alarak, bilgisyara 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 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.

Av. Ş.Cankat TAŞKIN
26.02.2009-BURSA

KAYNAKÇA

İnternet Kaynakları

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

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

www.garanti.com.tr/kredi_kartlari/sanal_kredi_kartlari/guvenlik.html (03.01.2009)

http://tr.wikipedia.org/wiki/IP_adresi (Erişim Tarihi: 03.01.2009)

Basılı Kaynaklar

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 A.Ş Vakfı), Sözkesen Matbaacılık, Ankara, 2007, s.49

ÇEKER, Mustafa; " İnternet Bankacılığı ve Bankaların Sorumluluğu" , Prof. Dr Hüseyin ÜLGEN'e Armağan, Vedat Kitapçılık Basım Yayım Dağıtım, İstanbul 2007, Cilt 2, s.1343

DÜLGER, M. Volkan; Bilişim Suçları, Ankara, Seçkin Yayıncılık, Kasım 2004

EKİNCİ, Mustafa ; 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu, Adalet Yayınevi, 3. Baskı, Ankara,2006

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

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

ÖZKUL, Davut; "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", Sayıştay Dergisi, Sayı 44-45, 01.06.2002, s.13

SMITH, Russel/GRABOSKY, Peter/URBAS, Gregor; Cyber Criminals On Trial, First Published by Cambridge University Press, Cambridge, 2004

TAŞKIN, Şaban Cankat; Bilişim Suçları, İstanbul, Beta Yayıncılık, 1.Baskı, 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

YAZICIOĞLU, R.Yılmaz; Bilgisayar Suçları, İstanbul, Alfa Yayınevi, Ekim 1997