BANKA HUKUKU
VE
YARGITAY KARARLARI
SEMPOZYUMU

BİLDİRİLER-TARTIŞMALAR

(8 Haziran 2007)

BANKA ve TİCARET HUKUKU ARAŞTIRMA ENSTİTÜSÜ
(T. İş Bankası A.Ş. Vakfı)

İNTERNET BANKACILIĞININ ÜÇÜNCÜ KİŞİLER TARAFINDAN HUKUKA AYKIRI KULLANIMI NEDENİYLE DOĞAN ZARARI KİM TAŞIR?

Doç. Dr. Yeşim ATAMER

İNTERNET BANKACILIĞININ ÜÇÜNCÜ KİŞİLER TARAFINDAN HUKUKA AYKIRI KULLANIMI NEDENİYLE DOĞAN ZARARI KİM TAŞIR?

Doç. Dr. Yeşim M. ATAMER*

I. Genel Olarak

İnternet bankacılığı, müşterilere, genelde bir müşteri numarası, parola ve şifre ile doğrudan hesaplarına ilişkin kayıtların bulunduğu sisteme giriş yaparak, bunlar üzerinde tasarruf edebilme imkânının sunulduğu bankacılık yöntemidir. Bu yöntem sayesinde müşteriler dünyanın neresinde bulunursa bulunsun her saatte hesaplarına ulaşabilmekte ve bir banka şubesinin varlığına bağımlı olmaktan kurtulmaktadır. Bankalar ise şubelerinde daha çok uzmanlık gerektiren danışmanlık faaliyetleri vererek, fatura, havale gibi gündelik işlemlerin gerçekleştirilmesi için daha az eleman çalıştırabilmekte ve bu sayede ciddi bir kaynak tasarrufunda bulunabilmektedir[1].

Ancak bu avantajlarının yanı sıra sistemin ciddi bir dezavantajı vardır. O da, müşterilerin güvenlik şifrelerini hukuka aykırı yollardan ele geçiren yetkisiz kişilerin, onların hesaplarından para çekmesi ve istenmeyen işlemler yapması rizikosunun mevcut olmasıdır. Bu şekilde, sahte vekaletname, tahrif edilmiş çek, sahte veya çalınmış banka veya kredi kartı kullanılması suretiyle bankada biriken mevduata yönelen saldırı türlerine bir yenisi daha eklenmiştir. Bu hallerin hepsinde üçüncü kişi bankaya, yetkisi olmaksızın bir talimat vermekte ve banka bu sahte talimata uyarak bir ödemede bulunmaktadır. Dolayısıyla hepsi açısından cevaplanması gereken ortak soru, gerçekleştirilen bu haksız fiilin ilk aşamada kimin malvarlığına bir saldırı teşkil ettiğidir. Yani bu "hırsızlık" kimin malvarlığında bir azalma meydana getirmiştir? Cevaplanması gereken ikinci soru ise malvarlığı azalan bu kişinin, haksız fiil faili dışında birisine zararını tazmin ettirme imkânının olup olmadığıdır.

(*) İstanbul Bilgi Üniversitesi Hukuk Fakültesi Öğretim Üyesi (yesima@bilgi.edu.tr.). Bu makalede kullanılan hyperlink'lerin hepsi 08.09.2007 tarihi itibariyle günceldir. Farklı bir atıf verilmeyen kararların tümüne www.kazanci.com.tr adresinden ulaşılmıştır.

(1) *Erfurth*, René: Haftung für Missbrauch von Legitimationsdaten durch Dritte beim Online-Banking, Wertpapiermitteilungen (WM) 2006, s. 2198, 2206.

II. Mevduat hesabının hukukî niteliği nedir ve bu hesaptan üçüncü kişiler tarafından hukuka aykırı şekilde para çekilmesi halinde bu zarar kimin malvarlığında doğar?

Müşterinin bankaya para yatırmasını ve bir hesap sahibi olmasını hukuken farklı şekillerde nitelendirmek mümkündür. Müşterinin vadesiz bir mevduat sözleşmesi kurduğu, dolayısıyla istediği an parasını çekebileceği hallerde, Borçlar Kanunu (BK) m. 472'de düzenlenmiş olan usulsüz tevdie ilişkin hükümlerin uygulanması akla gelir. Zira bu hallerde paranın güvenli bir yerde saklanması ön plandadır. Buna karşılık vadeli mevduat sözleşmelerinde müşterinin aynı zamanda faiz alıyor olması, karz akdi (BK m. 306) niteliğinin ağır basması ve bu hükümlerin uygulanması gerektiğini düşündürür. Ancak bankanın bu hesaba ilişkin olarak müşteriye çok farklı hizmetler de sunduğu gerçeği karşısında vekalet sözleşmesinin unsurlarını görmek de pekala mümkündür (BK m. 386)[2]. Nitekim bugün uygulamada ve doktrinde ağır basan görüş, banka mevduat sözleşmesinin bütün bu unsurları içinde barındırması nedeniyle karma veya kendine özgü (*sui generis*) bir sözleşme olarak nitelendirilmesi icap ettiği ve bu sözleşmeye, niteliğine uygun düştüğü ölçüde karz, usulsüz tevdi ve vekalete ilişkin Borçlar Kanunu hükümlerinin kıyasen uygulanması gerektiği yönündedir[3].

(2) *BernKomm/Fellmann*, Walter: OR Art 398 N. 430 vd., in: Berner Kommentar zum Schweizerischen Privatrecht, Obligationenrecht Bd. VI, 2. Abteilung, 4. Teilband, Der einfache Auftrag, Bern 1992.

(3) Ayrıntılı bilgi için örn. bkz. *Çeker*, Mustafa: Hukuki Yönüyle Banka Mevzuatı, Adana 2004, s. 25 vd.; *Reisoğlu*, Seza: Bankalar Kanunu Şerhi, C. I, Ankara 2007, s. 117 vd.; *Tandoğan*, Haluk: Borçlar Hukuku, Özel Borç İlişkileri, C. I/2, Ankara 1985, s. 329 vd.; *Tekinalp*, Ünal: Banka Hukukunun Esasları, İstanbul 1988, s. 310 vd.; 12. HD, 29.04.2004, 6537/10591: "Mevduat yatırma, ağırlıklı olarak esas itibariyle belli oranda faiz elde etme amacına yöneldiği için karz akdine daha çok yaklaşan, ancak güvenilir bir kurumda parayı muhafaza etme fikri ile vedia akdini hatırlatan kendine özgü bir akit tipidir. Mevduata uygulanacak hükümler, ancak kıyas yolu ile ve niteliğine uygun düştüğü ölçüde karz akdi hükümleri ve istisnai hallerde vedia akdi hükümleri olacaktır". HGK, 15.06.1994, 11-178/398: "Bankalar kendilerine yatırılan paraları mudilere istendiğinde veya belli bir vadede aynı veya misli olarak iade etmekle yükümlüdürler. Bu tanımlamaya göre mevduat ödünç (karz) ile usulsüz tevdi sözleşmelerinin niteliklerini taşıyan kendine özgü bir sözleşmedir. Bunun sonucu olarak mevduatın niteliğine uygun düştüğü oranda karz (ödünç) veya usulsüz tevdi hükümlerinin kıyasen uygulanması gerekir. BK'nun 306 ve 307. maddeleri uyarınca ödünç alan, akdin sonunda ödünç verilen parayı iade ve eğer kararlaştırılmışsa faizi ile iadeye mecburdur. Aynı Yasanın 372/1. madde uyarınca usulsüz tevdide paranın nef'i ve hasarı mutlak şekilde müstevdaa (saklayana) geçtiği için ayrıca açıklamaya gerek kalmadan saklayan bu parayı kendi yararına kullanabilir. Ancak mudi'nin istediği zamanda iade ile yükümlüdür. Bankalar türlü bahanelerle yararlandıkları bu mevduatı mudilere iadeden kaçınamazlar".

Bankaya yatırılmış olan paranın, üçüncü bir kişi tarafından, müşterinin hiçbir talimatı olmaksızın "çalınması", acaba bu farklı sözleşme türlerinin hükümlerine göre nasıl bir hukukî sonuç doğurur? Gerek *karz*, gerekse *usulsüz tevdi* sözleşmesini belirleyen unsur, ikisinin de konusunu aynen iade yerine misleri iade borcu doğuran para, misli eşya veya kıymetli evrakın oluşturmasıdır[4]. Dolayısıyla bu iki sözleşmede de para veya şeyin mülkiyeti karz alana veya müstevdiye geçmektedir. Bunun doğal bir sonucu ise, sözleşme süresi boyunca hasar rizikosunu karz alan veya müstevdiinin (yani olayımızda bankanın) taşımasıdır. Nitekim usulsüz tevdiyi düzenleyen BK m. 472'de bu durum açıkça ifade de edilmektedir:

"Müstevdiin tevdi olunan meblağı aynen iadeye mecbur olmaksızın misleri iade etmesi sarahaten veya zımnen mukarrer ise, *o meblağın nefi ve hasarı kendisine ait olur*".

Karz akdinde ise bu, mülkiyetin karz alana geçmesinin doğal sonucudur. Dolayısıyla olay tamamıyla bankanın malvarlığına yönelik bir haksız fiil olarak nitelendirilecektir[5]. Bankanın bu olayın meydana gelmesinde kusurlu veya kusursuz olması kural olarak önem taşımaz[6]; bankanın durumu adeta, kendi evine hırsız giren kişiye benzetilebilir. 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 bu meblağı borç

(4) *Tandoğan* (dn. 3), s. 326; *BaslerKomm/Koller*, Alfred: OR Art 481 N. 8 ve Art 312 N. 8-9, in: Basler Kommentar zum Obligationenrecht I, Art 1-529 OR, 4. Auflage, 2007.

(5) Hesaptan yetkisi olmaksızın para çeken kişiyi bankanın tespit etmesi ve doğrudan ona karşı dava açması üzerine, karşı tarafın, bankanın henüz asıl müşteriye ikinci kez ödemede bulunmaması nedeniyle zararının doğmadığına ilişkin savunmasını Yargıtay haklı olarak reddetmiştir. Yargıtay'a göre: "... mevduat, ödünç (karz) ile usulsüz vedia akitlerinin karışımı, kendine özgü niteliği bulunan bir sözleşme türü olmaktadır. Bankalar kabul ettikleri mevduatları sadece saklamak yükümlülüğü altında bulunmamakta ayrıca, bu parayı ticari hayatta kredi olarak kullandırarak kendi gelirlerini sağlamak yetkisine de sahip bulunmaktadırlar. Bu nedenle, yani bankaların hesap sahibince bankaya yatırılan paranın bu mevduat hesabında kaldığı sürece bu parayı kullanma yetkisi bulunduğundan, bu paranın haklı bir nedene dayanılmadan üçüncü kişiler tarafından hesaptan çekilmesi halinde onlardan istirdatını talep etmekte hukuki yararı bulunduğunun kabulü gerekir." (11. HD, 17.6.1988, YKD 1988, 1242, 1243).

(6) *Reisoğlu*, (dn.3), s. 852: "Yukarıda değinildiği gibi, banka kusurlu olsa da olmasa da sahtekarlıkla bir kişinin hesabından para çekilmesi halinde sadece banka zarara uğramıştır. Mevduat sahibinin bankaya karşı alacağı aynen devam etmektedir. Mevduat sahibi, burada olduğu gibi, bankanın zararının doğmasına kendisi de ortak kusuru ile sebep olduğu takdirde, banka ortak kusur oranında mevduat sahibine başvurabilecek ve bu zararını mevduat sahibine olan mevduat borcundan takas edebilecektir."

kaydetme imkânı, aşağıda açıklanacak olan istisnalar dışında, yoktur[7]. Kendisine ödünç verilen meblağın tamamen veya kısmen çalınmış olması, banka kusursuz da olsa, onu sorumluluktan kurtarmaz[8]. Bu parayı müşterisine geri ödemekten kaçınma imkânı olmaz[9].

Bankanın müşterisine sunduğu bilumum bankacılık hizmetleri nedeniyle *vekalet sözleşmesi* özelliklerinin ağır bastığı düşünülecek olursa, soruna yine farklı şekilde yaklaşmak mümkün olmayacaktır. Her ne kadar vekil BK m. 394 uyarınca vekaletin icrası nedeniyle yapmış olduğu masrafları ve uğramış olduğu zararların tazminini istemeye yetkiliyse de, örneğin, sahte veya tahrif edilmiş bir havale talimatı vesilesiyle bankanın bir üçüncü kişiye ödemede bulunması halinde kabul edildiği gibi[10], internet üzerinden verilen "sahte" talimatlarda da aslında müşterinin bir irade beyanı mevcut olmadığı için, vekaletin icrası nedeniyle ortaya çıkmış olan bir zararın varlığı kabul edilemez. Dolayısıyla BK m. 394, f. 2'ye dayanarak bankanın bu zararı tazmin ettirmesi mümkün değildir. Bu maddenin uygulanması ancak vekaletin gereği gibi icra edilmiş olması halinde mümkündür. Eğer "var olmayan" bir talimat sonucu banka yanlış kişiye ödemede bulunuyorsa, kendi malvarlığından ödemede bulunmaktadır ve bu meblağı müşterisine karşı borçlu kalmaya devam eder[11]. Dolayısıyla müşterinin bankaya yönelteceği talep, bankanın para

(7) *Gautschi*, Georg: Berner Kommentar zum Schweizerischen Privatrecht, Das Obligationenrecht, Bd. VI, 3. Auflage, Bern 1971, Art.398 N.36b.

(8) Bu açıdan Yargıtay 11. Hukuk Dairesinin 21.12.2006 tarihinde vermiş olduğu 12186/13739 sayılı kararına katılmak olanağı bulamıyorum. Karara konu olayda sahte bir vekaletname ile bankadan para çekilmiş; yapılan incelemelerde imzanın taklit olduğunun çıplak gözle tespit edilmesinin mümkün olmadığı anlaşılmıştır. Yargıtay bu gerekçeyle "... davalı bankanın BK'nın 96. maddesinde öngörülen kusursuzluğu kanıtlanmış bulunmasına rağmen, davalı banka hakkındaki davanın kabulüne karar verilmesi doğru görülmediğinden kararın bu nedenle de davalı banka yararına bozulması gerekmiştir" ifadesine yer vermiştir. Oysa metinde de ifade edilmiş olduğu gibi, sahte vekaletname ile bankadan para çekilmesi halinde zarar bankanın malvarlığında meydana gelir. Dolayısıyla bankanın imzanın taklit vs. olduğunu anlayıp anlamaması önem taşımaz. Asla taklit olduğu anlaşılamayacak olan bir imza söz konusu olsa da ilk aşamada banka zarara katlanır.

(9) Bkz. *Tandoğan*, Haluk: Borçlar Hukuku, Özel Borç İlişkileri, C. II, 3. bası, Ankara 1987, s. 427 vd.

(10) *Kilgus*, Sabine: Haftung für Unterschriftenfälschung im Bankverkehr und die Zulässigkeit ihrer Wegbedingung durch AGB, Zürich 1988, s. 138; *Guggenheim*, Daniel: Die Verträge der schweizerischen Bankpraxis, Zürich 1986, s. 247; *Hardegger*, Ida: Über die allgemeinen Geschäftsbedingungen der Banken, Bern 1991, s. 120; *Tandoğan* (dn. 9), s. 582 ve 600; Ayrıca bkz. BGE 108 II 314.

(11) *Brückner*, Dirk: Online Banking - Sphärenhaftung, Rechtsscheinhaftung, Verschuldenshaftung, Berlin 2002, s. 52; *Janisch*, Sonja/*Schartner*, Peter: Internetbanking - Sicherheitsaspekte und Haftungsfragen, DuD 2002, s. 162, 165; *Wiesgickl*, Margareta: Rechtliche Aspekte des Online-Banking, WM 2000, s. 1039, 1049; *Kunst*, Diana: Rechtliche Risiken des Internet-Banking, Multimedia und Recht (MMR) Beilage 9/2001, s. 23, 24; Avusturya Yüksek Mahkemesi (OGH), 19.11.2002 tarihli kararı, ÖBA 2003, s. 141.

borcuna (çeşit borcuna) ilişkin bir ifa davası olacak (yoksa tazminat davası değil) ve borçlu bankanın kusurlu olup olmaması bu noktada yine hiçbir önem taşımayacaktır[12].

Nitekim TTK m. 724 (İBK m. 1132), sahte bir çekin ödenmesinden dolayı doğan zararın muhataba ait olacağını açıkça beyan etmektedir:

"Sahte ve tahrif edilmiş bir çeki ödemiş olmasından doğan zarar muhataba ait olur; meğerki senette keşideci olarak gösterilen kimseye kendisine bırakılan çek defterini iyi saklamamış olması gibi bir kusurun isnadı mümkün olsun."

Yine, Banka Kartları ve Kredi Kartları Kanunu m. 15 uyarınca:

"Bu Kanunun 20. maddesi uyarınca harcama belgesi düzenlenmeksizin çeşitli iletişim araçları yoluyla veya sipariş formu vasıtasıyla yapılan mal ve hizmet alımlarındaki hukuka aykırı kullanımlardan kaynaklanan zararlardan kart hamili sorumlu tutulamaz".

Görüldüğü gibi, gerek çekle ödemeler, gerekse mesafeli sözleşmelerde kredi kartı verilerinin hukuka aykırı şekilde edinilmesi sonucu yapılan ödemeler açısından yasa koyucu malvarlığı zararının bankanın malvarlığında doğduğunu kabul etmiştir. Nitekim bu düzenlemeler İsviçre'de[13], Avrupa Birliği ülkelerinde ve ABD'de geçerli olan hukukî uygulamaya da paraleldir[14].

(12) *Berner Kommentar/Gautschi* (dn.7), Art. 398 N. 36c.

(13) İsviçre Federal Mahkemesi ilk defa 1986 yılında verdiği bir kararda (BGE 112 II 450) konuya bir riziko dağılımı sorunu olarak yaklaşmış ve daha önce sergilediği müşteri aleyhine tutumu terk etmiştir. Bu kararıyla mahkeme, aslen bankanın malvarlığına bir saldırı olduğunu ve bu zararı kural olarak bankanın taşıması gerektiğini kabul etmiştir. Nitekim son yirmi yıldır Mahkeme bu konudaki içtihadını değiştirmemiş ve en son 24 Nisan 2006 tarihinde (BGE 132 III 449) yayınlanan bir kararında teyit etmiştir.

(14) Kredi kartının hukuka aykırı kullanımı hakkında ayrıntılı bilgi için bkz. *Atamer*, Yeşim M.: Kredi Kartının Üçüncü Kişi Tarafından Hukuka Aykırı Şekilde Kullanılması Halinde Doğan Zararları Kim Taşıyacaktır?, Bilgi Çağında Hukukun Evrimi, Prof. Dr. Ünal Tekinalp'e Armağan, C. I, İstanbul 2003, s. 993-1031. Ayrıca bkz. 20 Mayıs 1997 tarihli Mesafeli Sözleşmelere İlişkin Olarak Tüketicinin Korunması Hakkında 97/7/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi (ATRG 1997 L 144/19), m. 8.

III. Mevduat hesabından üçüncü kişiler tarafından hukuka aykırı şekilde para çekilmesi nedeniyle bankanın malvarlığında doğan zararın müşteriye yansıtılması imkânı var mıdır?

Her ne kadar hukuka aykırı kullanım sonucunda ilk aşamada zarar bankanın malvarlığında doğuyorsa da, bankanın farklı kişilere karşı tazminat talepleri olabilir. Bunlardan ilki, kuşkusuz dolandırıcılık[15] fiilini işleyenlere karşı var olan haksız fiil temelli talebidir. Ancak bunun yanı sıra bankanın, müşterisine başvurması imkânı da olabilir. Burada talebin temelini, banka ve müşteri arasındaki sözleşme oluşturur. Banka, ya müşterinin çek defterini, imzasını, şifrelerini vs. gereği gibi muhafaza etmemesi nedeniyle sözleşmeden doğan özen yükümlülüğüne aykırı davrandığı gerekçesi ile ona karşı bir tazminat talebi sahibi olabilir; ya da müşterisi ile imzalamış olduğu sözleşmede yer alan genel işlem şartları ile rizikoyu baştan müşteriye aktarmış olabilir. Aşağıda bu iki hal üzerinde durulacaktır.

1. Müşterinin sözleşmeye aykırı davranışı nedeniyle bankanın bir tazminat talebinin var olması

a. Genel olarak sorunun ortaya konulması

Bankanın dolandırıcılık sonucu yapmış olduğu ödemeyi kendi malvarlığından gerçekleştirdiği kabul edildiğinde[16] müşterinin bu gelişmelerdeki rolü ancak, şifrelerinin öğrenilmemesi, çek defterinin kaybolmaması, bankaya yolladığı talimatların güvenilir şekilde bankaya ulaşması gibi konularda gerekli olan özeni gösterip göstermediği noktasında olabilir[17]. Zira, banka ile müşteri arasındaki sözleşme (hukuken nasıl nitelendirilirse nitelendirilirsin) müşteriye, bankanın zarara uğramasını engellemek üzere bir koruma yükümlülüğü yükler[18].

(15) Bu çalışmada "dolandırıcılık" kavramının kullanılması tercih edilmişse de zaman zaman ceza hukuku açısından bir hırsızlığın gerçekleşmiş olması da mümkündür. Olayın özelliklerine göre TCK m. 158, f. 1/f'nin, m. 142, f. 2/e'nin, m. 136'nın ve m. 243'ün uygulanması söz konusu olabilecektir. Bu açıdan çalışmada "dolandırıcılık" teknik anlamı ile kullanılmamıştır.

(16) Bu yönde *Reisoğlu* (dn. 3), s. 852; *Tandoğan* (dn. 9), s. 582; *Berner Kommentar/Gautschi* (dn. 7), Art. 398 N.36b; *Kilgus* (dn. 10), s. 140; *Hardegger* (dn. 10), s. 119; *Bucher*, Eugen: Wie lange noch Belastung des Kunden mit den Fälschungsrisiken im Bankenverkehr?, Recht 1997, s. 41, 42; *Guggenheim* (dn. 10), s. 249; BGE 111 II 263, 265; 112 II 450, 454; *Erfurth* (dn. 1), s. 2198, 2200; *Schleicher*, Michael: E-Commerce im Bankbereich, Berlin 2007, s. 217.

(17) *Bucher*, Eugen: Wer haftet wem? Zum Problem der Tragung des Risikos betrügerisch veranlasster Bankvergütung, recht 1984, s. 97, 103; *Hardegger* (dn. 10), s. 119.

(18) Koruma yükümlülükleri, bir kimsenin sözleşme ile kişi ve malvarlığını başka birisinin etki ve güven çevresine sokmasından kaynaklanır. Ayrıntılı bilgi için

Yukarıda yapılan benzetme devam ettirilecek olursa, hırsız gerçi bankanın "evine girmiştir", ama hırsızın bunu yapabilmesi için "anahtarı" ona müşteri sağlamış veya ihmali sonucu "pencereyi açık bırakmışsa" bankanın ona karşı bir tazminat talebi olacağı açıktır. Dolayısıyla yetkili olmayan üçüncü kişilerin, hesap ile ilgili bilgileri edinememeleri konusunda müşterinin gerekli özeni göstermemesi halinde sözleşmenin müspet ihlali söz konusu olur ve bankanın BK m. 96 uyarınca bir tazminat talebi doğar[19]. Bu durumda müşterinin bankaya yönelik, hesabındaki paraya ilişkin ifa talebine karşılık banka da kendi tazminat talebini ileri sürebilecektir[20]. Tarafların bu alacakları ise takas edilecektir.

Doğaldır ki müşteri sadece kusuru ile orantılı bir tazminat yükümlülüğü altında olabilir. Yani bankanın "evine" hırsız girmesi rizikosunu tümden müşteriye aktarması imkânı yoktur. Banka sadece, müşterinin kusuru oranında müşteriye karşı bir tazminat hakkı kazanır[21]. Ayrıca bu bağlamda dikkat edilmesi gereken diğer bir husus, bankanın kendi kusuruyla zararın doğumuna veya artmasına etki etmiş olup olmadığıdır. Yine hırsızlık örneği üzerinden düşünülecek olursa, banka "anahtarın" nasıl muhafaza edileceği konusunda müşteriyi gereği gibi aydınlatmamış ise, yani "kendi evini" gereği gibi korumak için üzerine düşen önlemleri almamış ise, ortaya çıkan zararın tümüyle müşterisi tarafından karşılanmasını isteyemez. Bu hallerde kusur oranları saptanacak ve ona göre zarar BK m. 44 uyarınca paylaştırılacaktır[22]. Bankanın ne ölçüde kusurlu olduğunun tespit edilmesi sadece bu noktada önem taşır, yani bankanın sorumluluğunun ihdası için değil, müşterinin de kusurlu olması halinde zararın nasıl paylaştırılacağının belirlenmesi için bu inceleme yapılır.

b. Müşterinin koruma yükümlülüğünün kapsamı

İnternet bankacılığının üçüncü kişiler tarafından kötüye kullanılması rizikosunu azaltmak amacıyla müşterinin ne tür önlemler alabileceğini tespit edebilmek için, bu tür kötüye kullanımların nasıl gerçekleştiği

bkz. *Serozan*, Rona: İfa, İfa Engelleri, Haksız Zenginleşme, İstanbul 2006, § 18 N. 5 vd. 2002 yılında Alman Medeni Kanununda yapılan reform sonrasında § 241'e ikinci fıkra olarak şu düzenleme eklenmiştir: "Borç ilişkisi içeriği itibariyle taraflardan her birini karşı tarafın hakları, malvarlığı ve menfaatlerini korumak yükümlülüğü altına sokabilir." Bu düzenleme ve koruma yükümlülüğü kavramı hakkında bkz. *MüKo/Roth*, § 241 N. 90 vd., in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 2 a, Schuldrecht, Allgemeiner Teil, §§ 241-432, 5. Auflage, München 2007.

(19) *Guggenheim* (dn. 10), s. 247.

(20) *Hardegger* (dn. 10), s. 119.

(21) *Wiesgickl* (dn. 11), s. 1039, 1049.

(22) *Schleicher* (dn. 16), s. 215.

konusunda bilgi sahibi olmak gerekir[23]. Dolayısıyla aşağıda öncelikle bu konuda -kuşkusuz teknik ayrıntılara girmeden- bazı veriler aktarılacaktır. Daha sonra bu tür dolandırıcılık teknikleri karşısında korunmanın ne ölçüde mümkün olduğu ve müşterilerin bu bağlamda üzerine düşenler tespit edilecektir.

aa. İnternet bankacılığında dolandırıcılık metotları[24]

- "*Pharming/DNS-spoofing*"[25]: Bilindiği gibi internette iletişim, İnternet-Protokolü (IP) aracılığıyla gerçekleştirilmektedir. Internet aracılığı ile iletişim kurabilmek için her bir kişi veya kurumun her biri 0 ila 255 arasında yer alan dört haneli bir IP adresine sahip olması gerekmektedir (örneğin İş Bankasının IP-adreslerinden biri 213.161.144.97'dir). Adeta telefon numaraları ile mukayese edilebilecek bu numaraları kimse aklında tutamayacağı için iletişime geçilecek ilgili numaraya bir isim (*domain-name*) verilmesi tercih edilmiştir. Örneğin "www.isbank.com.tr" bu türden bir isimdir. Ancak kullanıcıların bu isimleri yazması halinde, bunların temsil ettiği IP-numarasını ortaya çıkarmak için deşifre edilmesi ihtiyacı doğmaktadır. Bu işlem ya kişinin bilgisayarında kayıtlı olan bir dosya (*host-file*) ya da bağımsız olarak bu tür hizmet sunan *domain-name-service* (DNS – alan adı sistemi) üzerinden gerçekleştirilmektedir.

İnternet alanındaki saldırıların ilk türünde dolandırıcı ya doğrudan müşterinin bilgisayarındaki dosyada ya da DNS-server, yani alan adı sunucusundaki dosyada ilgili ismin ("www.isbank.com.tr") temsil ettiği numarayı değiştirmekte ve böylelikle müşterinin aynı ismi yazmasına rağmen başka bir numaraya bağlanmasına sebep olmaktadır. Bu tür bir

(23) İnternet bankacılığında dolandırıcılık sadece Türkiye'ye özgü bir sorun değildir. Hatta bu konuda artık özel web-sitelerinin var olması sorunun vahametini göstermektedir. Örn. bkz. www.antiphishing.org. Bu sitede yayınlanan bir rapora göre Ekim 2005 - Ekim 2006 döneminde internette yaşanan phishing olaylarının sayısı % 757 oranında artmıştır.

(24) Bu konuda ayrıntılı bilgi için bkz. *Borges*, Georg: Rechtsfragen des Phishing – Ein Überblick, Neue Juristische Wochenschrift (NJW) 2005, s. 3313 vd.; *Gajek*, Sebastian/*Schwenk*, Jörg/*Wegener*, Christoph: Identitaetsmissbrauch im Onlinebanking, Datenschutz und Datensicherheit (DuD) 2005, s. 639 vd.; *Karper*, Irene: Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofi?, DuD 2006, s. 215 vd.; *Kindl*, Michael /*Werner*, Dennis: Rechte und Pflichten im Umgang mit PIN und TAN, Computer und Recht (CR) 2006, s. 353 vd.; *Oppliger/Hauser/Frey*, Man in the Middle (MITM) Angriffe: Phishing in Echtzeit", Zeitschrift für Datenrecht und Informationssicherheit (DIGMA) 2006, s. 32-35; *Bohm/Brown/Gladman*: Electronic commerce: Who carries the risk of fraud? (http://www.fipr.org/WhoCarriesRiskOfFraud.htm) nr. 85 vd.

(25) Ayrıntılı bilgi için bkz. *Erfurth* (dn. 1), s. 2198, 2199-2200; *Gajek/Schwenk/Wegener* (dn. 24), s. 639, 641 vd.

müdahale genelde dolandırıcının daha önce müşterinin bilgisayarına bir mail yollamak suretiyle yerleştirdiği bir virüs veya truva atı (*trojan horse*)[26] sayesinde gerçekleşebilmektedir. Yani müşterinin aktif herhangi bir davranışı söz konusu değildir. Bu hallerde müşteri bankasının web sitesi adresini doğru yazmasına rağmen, otomatik olarak sahte bir web sitesine yönlendirilmekte ve bu adreste şifrelerini girmek suretiyle, verilerinin dolandırıcıların eline geçmesine olanak tanımaktadır.

- "*Phishing*"[27]: Milletlerarası literatürde *phishing* (*password fishing*) adı altında geçen bir diğer uygulama ise, internet kullanıcısına, kendi bankasından gelene tıpa tıp uyan bir e-posta yollanması ve bu e-postada, örneğin verilerin güncellenmesi gerekçesi ile, bütün güvenlik şifre ve numaralarının bildirilmesinin istenmesidir. Bu tür e-postalar genelde cuma akşam üzeri yollanmakta ve müşterinin hemen cevap vermemesi halinde hesabının hafta sonu üzeri bloke edileceği kendisine bildirilmektedir. Bu e-postada yer alan ve müşteriyi, bankanın ilgili web sitesine aktardığı düşünülen *hyperlink* ise onu aslında bankanın web-sitesinin bir taklidinin yer aldığı sayfaya götürmektedir. Yani aslında kendi bankasının web-adresini yazmış olmasına rağmen müşteri dolandırıcının web-sayfasına yönlendirilmektedir. Müşteri bunu yine fark etmeyip, "sisteme" girmek suretiyle bütün verilerini dolandırıcılara teslim etmektedir.

- "*Keylogger*": Kısmen phishing altında ele alınan bu yöntemde müşterinin bilgisayarına yerleştirilen bir truva atı sayesinde müşterinin bütün klavye hareketlerinin protokolü tutulmakta ve dolandırıcıya yollanmaktadır. Bu şekilde dolandırıcı, müşterinin şifrelerini girdiği anda bu bilgiyi kendi kayıtlarından görebilmektedir.

- "*Man-in-the-middle*": Bu tür saldırılar, ilk üçünden farklı olarak eş zamanlı gerçekleşmektedir. Yani banka ve müşteri iletişim halindeyken dolandırıcı araya girmektedir. Özellikle SSL (*secure sockets layer*) protokolü ile şifrelemenin gerçekleştirilmediği hallerde[28] bu riziko söz konusudur. Bu hallerde ya o anda verilen bilgiler doğrudan dolandırıcı tarafından edinilmekte ve daha sonra kullanılmakta ya da müşterinin verdiği bilgiye anında müdahale edilerek diğer tarafa bu manipüle

(26) Truva atları, örneğin bilgisayar oyunları gibi zararsız programların içinde yer alan, ancak bilgisayar kullanıcısının fark edemeyeceği şekilde arka planda aslında onun iradesi dışında işlemler gerçekleştiren zararlı programlardır. Örn. Bkz. *Erfurth* (dn.1), s. 2198, 2199.

(27) Bilgi için bkz. *Borges* (dn. 24), s. 3313 vd.

(28) Bu alanda da sahteciliğin söz konusu olduğu ve aslında şifreleme yapılmayan bir sitenin şifreleme yapılıyormuş gibi gösterilebileceği ve bu şekilde İnternet kullanıcısının dolandırılabileceği konusunda bkz. *Gajek/Schwenk/Wegener* (dn. 24), s. 639, 640.

edilmiş bilginin aktarılması sağlanmaktadır. Örneğin, bu şekilde bir havalenin doğrudan dolandırıcının hesabına yapılması temin edilmektedir.

bb. İnternet bankacılığında dolandırıcılığa karşı korunma yöntemleri ve bunların ne ölçüde etkili olduğu sorunu

İnternet bankacılığının % 100 bir güvenlik ile sunulması imkânı bugün için teknik açıdan mevcut değildir. Her elektronik güvenlik sisteminin bir yerde açığının bulunması mümkündür. Dolayısıyla bankaların ve diğer kişisel bilgi depolayan kurumların kendi sistemlerini güvenli kılmak için çok yüksek bir standart tutturmalarının gerekeceği açıktır. Zira bu sistemlere girilmesi halinde binlerce kişinin verilerine ulaşılması ve dolandırıcılık yapılması tehlikesi mevcuttur[29].

Nitekim bankaların bilgisayar sistemlerinin çok sıkı şekilde korunuyor olması nedeniyle dolandırıcılık olayları bugün genelde müşterilerin bilgisayarlarına yapılan saldırılar sonucunda yaşanmaktadır. Müşterilerin ise bu tür saldırılardan korunmak için yapabilecekleri ilk şey şifre, güvenlik kodu vs. gibi bilgilerin yetkisiz üçüncü kişilerin eline geçmemesi için bunları gereği gibi muhafaza etmeleridir. Özellikle şifrenin kolayca erişilebilir bir yere not edilmemesi, bunların bilgisayarda bir dosya içinde muhafaza edilmemesi, başka kişilere verilmemesi, bilinmeyen kişilerden gelen e-postaların ve ekli programların açılmaması gibi. Bunun yanı sıra, müşterilerin kişisel bilgisayarlarını daha güvenli kılacak olan bir uygulama, virüs programı ve *firewall* gibi sistemleri kurmak ve bunları güncellemektir. Bu şekilde kişisel bilgisayarlara internet aracılığıyla virüs, truva atı veya benzeri zarar verici programların bulaşması bir ölçüde engellenebilecektir. Ancak %100 bir koruma müşteri bilgisayarları açısından sağlanamaz, zira bu virüs programlarını her gün güncellemek imkânı olmayacağı için, yeni gelişen bir virüs veya truva atı ile bu programlara rağmen müşterilerin verilerini hukuka aykırı yollardan edinmek mümkün olabilecektir. Diğer yandan saldırının *man-in-the-middle* yöntemi ile gerçekleşmesi veya müşteri bilgisayarı dışında örneğin bir DNS sunucusuna karşı işlenmesi halinde müşterinin bilgisayarında her türlü güvenlik önlemi alınmış olsa bile saldırıyı engellemek söz konusu olamayacaktır.

Dolayısıyla müşterilerin şifrelerinin üçüncü kişilerin eline geçmemesi konusunda koruma önlemleri geliştirmek yine daha çok bankalara düşen bir görevdir. Bu konuda son yıllardaki gelişmelere bakılacak olursa aslında bankaların imkân dahilinde olan bir dizi koruma

(29) Mayıs 2006 itibariyle bir mağazanın kredi kartı yönetim sistemine yapılan korsan saldırı bu sistemin gereği gibi korunmamasının sonuçlarını açıkça ortaya koymuştur. Saldırı sonucu 9229 kişinin kredi kartı verileri kopyalanmış ve kötüye kullanılmıştır. Bu konuda bilgi için örn. bkz. (http://www.cnnturk.com/EKONOMI/GENEL/haber_detay.asp?PID=40&haber ID=186973)

önlemini ancak çok gecikmeli olarak devreye soktukları görülmektedir. Örneğin PIN numarasının düzenli aralıklarla değiştirilmesi zorunluluğu getirilmesi; yapılan işlemler hakkında cep telefonuna veya e-postaya uyarılar yollanması; müşterinin vermiş olduğu cep telefonu numarasının internet bankacılığı yoluyla değiştirilememesi; cep telefonu üzerinden sürekli yeni şifre üretme (şifrematik) uygulaması gibi uygulamalar ancak kötüye kullanımlar arttıktan sonra geliştirilmiştir. Ayrıca dünya bankacılık uygulamasındaki basit bazı diğer güvenlik önlemleri Türkiye'de hiç uygulanmamıştır. Örneğin Alman bankacılık uygulamasında yaygın bir yöntem, banka şubesinin bir liste halinde işlem numaralarını (*transaction number*/TAN) müşteriye vermesi ve müşteriden yapacağı her bir internet bankacılığı işlemi için hem PIN hem de bir seferlik kullanımı olan TAN bilgisini girmesini istemesidir. Bu hallerde üçüncü kişiler tarafından bir şekilde ilgili işlemde kullanılan PIN ve TAN numarasının öğrenilmesi bir tehlike doğurmayacaktır, zira aynı TAN numarası ikinci bir işlemde yeniden kullanılamayacaktır. Dolayısıyla ancak hem internet üzerinden müşterinin bilgilerinin "çalınması" hem de evine girerek TAN numaralarının çalınması halinde müşterinin hesaplarına ulaşmak mümkün olacaktır ki, bunun çok zor olduğu aşikârdır. Oysa Türkiye'de bankalar uzun süre, doğan zararın ne de olsa müşteriye aktarılabileceği inancı içinde kendi malvarlıklarını korumak için gerekli önlemleri geliştirmemiş ve gerekli uyarılarda da bulunmamıştır.

cc. Müşterilerden alınmaları beklenebilecek önlemler

Yukarıda ifade edildiği üzere[30] bankanın malvarlığında gerçekleşen azalmanın müşteriye yansıtılabilmesi, müşterinin bu dolandırıcılığın gerçekleştirilmesinde kusurlu olması halinde ve kusurlu olduğu oranda mümkündür. Yani müşterinin sözleşmeden doğan, karşı tarafın malvarlığını koruma yükümlülüğüne aykırı davranmak suretiyle sözleşmenin müspet ihlaline sebep olması halinde BK m. 96 uyarınca tazminat borcu doğacaktır. Acaba günümüz müşterisinin, bankanın malvarlığının zarara uğramaması için yukarıda aktarılmış olan dolandırıcılık yöntemlerine karşı korunmak amacıyla ne tür önlemler alması beklenebilir?

Bilgisayar kullanımının topluma yayılması ile beraber bugünün "ortalama" müşterisi, bilgisayara ilişkin teknik detaylardan anlayan bir müşteri olmaktan çıkmıştır. Özellikle "virüs/truva atı/firewall" gibi kavramlardan çok uzak olan bu müşteri, internet bankacılığından faydalanmasının içerdiği riskler hakkında, ayrıca uyarılmadıkça, genelde haberdar değildir[31]. Şifresini koruması gereği konusunda her müşterinin

(30) Bkz. yukarıda dn. 17'ye ilişkin metin.

(31) Almanya ve Avusturya açısından aynı yönde bir tespit için bkz. *Recknagel*, A. Einar: Vertrag und Haftung beim Internetbanking, München 2005, s. 225; *Krassnigg*,

bilgi sahibi olması gerektiğinden yola çıkılabilmekle beraber, teknolojik bazı bilgilere sahip olmak konusunda aynı değer yargısına varmak zordur.

Nitekim bu yüzden müşterilerin internet bankacılığının getirdiği tehlikeler konusunda banka tarafından özel olarak aydınlatılması gerektiği bugün genel anlamda kabul görmektedir[32]. Özellikle bankaların yeni dolandırıcılık tekniklerinden ilk haberdar olanlar olması, bu bilgiyi müşterileri ile paylaşmalarını gerektirir. Örneğin *phishing*, yani müşterilerin şifre ve bilgilerini vermelerini isteyen e-postalar hakkında, bu tür dolandırıcılıklar yaşandıktan sonra bilgilendirme gerçekleşmiştir. Bugün birçok bankanın web-sitesinde bu konuda uyarılar yer almaktadır.

Diğer yandan virüs programlarının kullanılması gereği hakkında da artık bir dizi bankanın web-sitesinde yer verdikleri uyarılar dikkat çekmektedir. Ancak bu uyarılar, bankaların internet bankacılığı sitesine girildiğinde ekranın göze batmayan bir köşesinde bulunan "güvenlik/güvenlik uyarıları" gibi bir ikon'un "tık"lanması halinde açılmaktadır. Yani buradaki bilgilerin edinilmesi için müşterinin aktif bir davranışına ihtiyaç vardır. Oysa müşteriler teknik açıdan bilgi sahibi olmadıkları için internet bankacılığının tehlikelerini tartamamakta ve bu uyarıları okumadan da işlem yapabilmektedir. Hele de bir virüs programının veya *firewall*'un, bilgisayara her zaman yüklü olan bir yazılım olarak düşünülmesi ve bu yüzden müşterilerin ayrıca bir adım atmaması çok muhtemeldir. Dolayısıyla bu tür uyarıların ideal olarak sözlü yapılması gerekir. Yurt dışındaki uygulamalara bakıldığında, banka müşterilerinin internet kullanımına geçebilmek için öncelikle müşteri temsilcileri ile görüşmeleri zorunluluğunun olduğu ve bu görüşmede her türlü teknik ayrıntı konusunda aydınlatıldıkları görülmektedir.

Gerekli bilgilendirmenin yapılmış olduğu hallerde bile, müşterilerin sürekli olarak virüs programlarını güncellemeleri veya daha ileri yeni programlar satın almaları ve bu şekilde yeni geliştirilen virüslere karşı da kendilerini koruma altına almalarını beklemek kanımca aşırıya gider[33]. Örneğin bir bankanın müşterilere ilişkin bilgilendirme notlarında yer alan, şu ifade aşırıya giden beklentiye güzel bir örnek teşkil eder: "*Bu nedenle anti-virüs programınızı belirli aralıklar ile en az haftada bir veya basında haber çıkarsa hemen güncellemeniz gerekmektedir.*" İnternet bankacılığına içkin olan bir riziko sonucu, bankanın malvarlığında meydana gelen bir zararın, müşterilere, abartılı güvenlik önlemleri alma yükümlülüklerinin getirilmesi suretiyle aktarılması mümkün değildir. Diğer yandan, bu programların ancak para karşılığında edinilebilecek ve güncellenebilecek olduğu gerekçesiyle de bunların müşteri bilgisayarında bulunmamasının koruma yükümlülüğüne aykırılık oluşturacağı görüşü sık sık reddedilmektedir[34]. Ara sonuç olarak, internet bankacılığı sistemine içkin bu kötüye kullanım rizikosunu müşterilerin engellemesi imkânı ancak sınırlı olarak mevcuttur.

Harald/*Stotter*, Martin: Rechtliche Entwicklungen im Internetbanking, Wirtschaftlich Rechtliche Blätter (WBL) 2004, s. 213, 217; *Erfurth* (dn.1), s. 2198, 2201.

(32) *Recknagel* (dn. 31), s. 220 vd.; *Hanau*, Max Ulrich: Handeln unter fremder Nummer, Berlin 2004, s. 70 vd.; *Krassnigg/Stotter*, (dn. 31) s. 213, 216; *Brückner* (dn. 11), s. 58-59; *Schönborn*, Konstantin Graf von: Die Bankhaftung bei der Überweisung im Internet, 132 vd.; *Erfurth* (dn. 1), s. 2198, 2201; *Schleicher* (dn. 16), s. 216.

(33) Aynı görüşte *Recknagel* (dn. 31), s. 226; *Krassnigg/Stotter* (dn. 31), s. 213, 217.

dd. Müşterilerin sözleşmeden doğan koruma yükümlülüklerine aykırı davrandıkları konusunda ispat yükü kimdedir?

Kanunda aksine hüküm bulunmadığı sürece ispat hukukunun genel kuralı Medeni Kanun m. 6 uyarınca taraflardan her birinin hakkını dayandırdığı olguları ispat etmesidir. Yani bankanın da, müşterisinin sözleşmeden doğan koruma yükümlülüğüne aykırı davrandığını ispat etmesi gerekir. Her ne kadar ilk aşamada BK m. 96 uyarınca ispat yükünün müşteride olduğu düşünülebilecek olursa da, bu düzenleme kusurun varlığına ilişkindir[35]. Oysa bankanın öncelikle sözleşmeye aykırı davranışın varlığını ortaya koyması gerekir. Bunun yanı sıra, sözleşmeye aykırı davranış nedeniyle bir zarar doğduğunu ve bu davranış ile zarar arasında nedensellik bağı bulunduğunu da banka ispatlamak durumundadır[36]. Bu ispatın gerçekleşmesi halinde müşteri ancak kusursuzluğunu ispatlayarak sorumluluktan kurtulabilecektir.

Sözleşmeden doğan asli ifa yükümlülüklerine aykırılık, örneğin ödememe, teslim etmeme çok kolay ispat edilebilirken, koruma yükümlülüklerine aykırı davranıldığının ispatı hiç de kolay değildir. Parola ve şifrenin, müşterinin bilgisi dahilinde üçüncü bir kişi tarafından kullanıldığı veya müşterinin bilgisayarında virüs programı veya firewall gibi güvenlik önlemlerinin alınmamış olması nedeniyle üçüncü bir kişi tarafından öğrenilebildiği konusunda doğrudan bir ispat genelde mümkün olmayacaktır. Dolayısıyla bu noktada üzerinde durulması gereken, dolaylı bir ispatın (emarelere dayanan ispatın) kabul edilip edilemeyeceğidir. Emarelere dayanan ispatta özel önem taşıyan bir konu

(34) *Recknagel* (dn. 31), s. 226; *Krassnigg/Stotter* (dn. 31), s. 213, 217.

(35) *BaslerKomm/Wiegand* (dn. 4), OR Art.97 N. 36; *BernerKomm/Weber*, Rolf H., OR Art 97 N. 317 in: Berner Kommentar zum Schweizerischen Privatrecht, Obligationenrecht, Bd. VI, 1. Abteilung, 5. Teilband, Die Folgen der Nichterfüllung, Bern 200; Alman hukukunda § 280 BGB'ye ilişkin olarak bkz. *Erfurth* (dn. 1), s. 2198, 2203; *MüKo/Ernst* (dn. 18), § 280 BGB, N. 146 vd.; *Palandt/Heinrichs*, Helmut: § 280 BGB, N. 34 vd., in: Palandt, Bürgerliches Gesetzbuch, 65. Auflage, München 2006.

(36) *Schleicher* (dn. 16), s. 245.

"ilk görünüş ispatıdır"[37]. Bu ispat türünde, bir olayın hayat tecrübelerine göre aksi şekilde gelişmesinin çok düşük bir olasılık teşkil ettiği hallerde, ilk göründüğü şekli esas alınır ve o biçimde var olduğu kabul edilir. Dolayısıyla hayat tecrübelerine aykırı olan akışı iddia eden taraf ispat yükü altında olur. Acaba doğru parola ve şifre ile işlem yapılmış olması, müşterinin reddetmesine rağmen, işlemin müşteri tarafından yapıldığı veya bu parola ve şifrenin, müşterinin koruma yükümlülüklerine aykırı davranışı nedeniyle üçüncü kişiler tarafından öğrenilmiş olduğu konusunda bir ilk görünüş ispatı olarak kabul edilmeli midir? Yani, kendisinin bu işlemi yapmadığı veya bu bilgileri başkasına vermediği veya bilgisayarının güvenli olduğu konusunda ispat yükünün müşteri üzerinde olduğu kabul edilmeli midir?

Konu yabancı literatürde tartışmalıdır[38]. Ancak internet ortamında teknolojik imkânlardan yararlanarak dolandırıcılık yapılması olasılığının artması ile birlikte; doğru şifre ve parola ile işlem yapılan hallerde, bunun müşteri tarafından veya kendisinin kusuru ile şifre ve parolayı öğrenen üçüncü bir kişi tarafından gerçekleştirildiği varsayımının hayatın olağan akışına uygun olduğu görüşü azınlıkta kalmıştır[39]. Kanımca da sadece sistemin yüzde yüze yakın güvenilir olması halinde, doğru şifre ve parola ile yapılan işlemlerin müşteriden neşet ettiği konusunda bir ilk görünüşün varlığı kabul edilmelidir[40]. Oysa bugün internet bankacılığı sistemi bu türden bir güvenlik arz etmemektedir ve bunun müsebbibi de müşteriler değildir.

(37) Bu konuda bilgi için bkz. *Yıldırım*, Kamil: Medeni Usul Hukukunda Delillerin Değerlendirilmesi, İstanbul 1990, s. 120 vd. ve özellikle s. 124 vd.; *Pekcanıtez*, Hakan/*Atalay*, Oğuz/*Özekes*, Muhammed: Medeni Usul Hukuku, Ankara 2006, s. 410 vd.

(38) Ayrıntılı bilgi için bkz. *Bruns*, Patrick: Beweislastverteilung bei mißbräuchlicher Nutzung elektronischer Zahlungssysteme, MMR 1999, 19, 21; *Borges* (dn. 24), s. 3313, 3316 vd.

(39) Bu hallerde bir ilk görünüş ispatının var olmadığı yönünde *Erfurth* (dn.1), s. 2198, 2205; *Kindl/Werner* (dn. 24), s. 353, 359; *Wiesgickl* (dn. 11), s. 1039, 1047; *Schleicher* (dn.16), s. 233-234. *Hanau*'a göre müşterinin, bilgisayarında virüs olduğunu ispat etmesi halinde ilk görünüş ispatı etkisini yitirir (dn. 32), s. 78. *Brückner* ise sadece bilgisayarda virüs olma ihtimalinin ispat edilmesini ilk görünüş ispatının etkisini yitirmesi için yeterli olacağı kanaatindedir. Yani ayrıca virüsün bilgisayarına kendi kusuru olmaksızın bulaştığını ispat etme yükümlülüğü olmaz (dn. 11), s. 119. Aynı yönde bir Alman alt derece mahkemesi kararı için bkz. AG München, 18.06.1998, CR 1998, s. 566, 567. Bankanın aydınlatma yükümlülüğünü yerine getirmemiş olduğu hallerde müşterinin sorumlu tutulamayacağı yönünde: *Krassnigg/Stotter* (dn. 31), s. 213, 219. Buna karşılık doğru şifre ile işlem yapılması halinde banka lehine bir ilk görünüş ispatının var olduğu kanaatinde *Kunst* (dn. 11), s. 23, 25.

(40) Bkz. *Schwarz*, Mathias (Hrsg.): Recht im Internet, Augsburg 2002, n. 6-4.3, s. 14-15.

2. Banka ile müşteri arasındaki sözleşme hükümleri uyarınca bankanın bir tazminat talebinin var olması

Uygulamada, banka ile müşteri arasında akdedilen sözleşmelere dahil edilen genel işlem şartları (GİŞ), dolandırıcılık risklerinden müşterilerin sorumlu olacağı yönünde düzenlemeler içermektedir. Banka, bir sahtekârlık nedeniyle kendi malvarlığından yanlışlıkla yaptığı bir ödemeyi müşterisine izafe etmenin hukukî dayanağını GİŞ yoluyla yaratmaktadır[41]. Amaç sorumluluğu sınırlandırmak değil, riziko dağılımını tespit etmektir[42]. Yani, söz konusu olan bankanın malvarlığına yönelik riski müşteriye aktarmaktır.

Türk hukukunda genel işlem şartlarını denetlemek için yasal bir düzenleme uzun yıllar eksik kalmıştır. Ancak buna rağmen Yargıtay, sözleşme taraflarından birinin tek yönlü olarak düzenlediği ve diğer tarafa pazarlık yapma imkânı olmaksızın dikte ettiği sözleşme koşullarını batıl saymıştır[43]. 2003 yılında Tüketicinin Korunması Hakkında Kanunda (TKHK) yapılan değişiklik ile gecikmeli de olsa tüketici sözleşmelerindeki haksız şartlara ilişkin özel bir düzenleme gelmiş ve açık bir denetim normu yaratılmıştır[44]. Bu hüküm uyarınca "satıcı veya sağlayıcının tüketiciyle müzakere etmeden, tek taraflı olarak sözleşmeye koyduğu, tarafların sözleşmeden doğan hak ve yükümlülüklerinde iyi niyet kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe

(41) *Bucher* (dn. 17), s. 97, 99; *Hardegger* (dn. 10), s. 122; *Kilgus* (dn. 10), s. 157.

(42) BGE 112 II 450.

(43) Örn. Bkz. 13. HD, 18.3.1996, 1734/2495, YKD 1996, s. 746, 750: "Tüketicinin korunmasının ortaya çıkardığı sorunlardan birisi de tüketicilerin genel işlem şartları yoluyla sömürülmesinin önlenmesidir. Ekonomik bakımdan güçsüz olanların korunması, Anayasamızda belirtilen "Sosyal Hukuk Devleti" ve "İktisadi ve Sosyal Hayatın Adalete Göre Düzenlenmesi", eş söyleyişle "Sosyal Adalet" ilkelerinin bir gereğidir. Sırası gelmişken hemen vurgulayalım ki, hakim, Medeni Yasanın 1. maddesinin kendisine tanıdığı yasa koyucu gibi hareket etme yetkisine dayanarak, özellikle hakların kullanılmasında ve borçların yerine getirilmesinde objektif iyiniyet kurallarına uymayı öngören MK m. 2/I; kişiliğin korunmasını düzenleyen MK m. 24; ahlaka aykırı sözleşmeleri yasaklayan BK m. 19/II gibi genel kurallar altında sözleşme özgürlüğüne tüketiciyi koruyucu sınırlamalar getirebilir. Gerçekte de mahkemeler; somut olayın kendine özgü verileri ve koşullarının gerçekleşmesi halinde ve yasal genel kurallar çerçevesinde; dikkati özel olarak çekilmeksizin sözleşmeye konan ve alışılmamış şartlarla, tüketiciyi bağlı tutmamalı ve hükümsüz saymalıdır. En önemlisi, yargı kararları ile tüketicinin bu yolda korunması hukuk devleti ve sosyal adaletin bir gereği kabul edilmelidir."

(44) Bu konuda ayrıntılı bilgi için bkz. *Atamer*, Yeşim: Genel İşlem Şartlarının Denetiminde Yeni Açılımlar: Tüketicinin Korunması Hakkında Kanun m. 6, Tüketici Sözleşmelerindeki Haksız Şartlar Hakkında Yönetmelik ve Borçlar Kanunu Taslağı m. 18a-f, Prof. Dr. Necip Kocayusufpaşaoğlu'na Armağan, Ankara 2004, s. 291-331.

neden olan sözleşme koşulları haksız şarttır." İnternet bankacılığı vasıtasıyla işlem yapılmasının TKHK'un kapsamında değerlendirilmesi imkânı olup olmadığı burada tartışılmayacaktır. Zira GİŞ denetiminin zaten Borçlar Kanununun genel hükümleri, özellikle BK m. 19 ve 20 uyarınca yapılması da mümkündür[45].

Bu sınırlar çerçevesinde acaba taraflar arasında akdedilen sözleşmede yer alan aşağıdaki tarzda bir genel işlem şartı nasıl değerlendirilmek gerekir?

"İşbu taahhütnameden doğan hakların, hesap, ürün/hizmetlerin kullanımının sadece tarafıma/mıza ve yetkilendirdiğim/iz kişilere ait olduğunu, bu hakkın, hesap, ürün ve hizmetlerin kullanımına ilişkin şifre, güvenlik kodu veya müşteri numarasını başkasına kullandırmayacağımı/zı ve devredemeyeceğimi/zi veya başkalarının eline geçmemesi için her türlü önlemi alacağımı/zı, aksi takdirde şifrem/iz ve güvenlik kodum/uz ile yapılan tüm işlemlerin sorumluluğunun tarafıma/ıza ait olacağını ve söz konusu işlemlerin tarafımdan/ımızdan yapılmadığı iddiasında bulunmayacağımı/zı kabul ve beyan ederiz."

Dolandırıcılık nedeniyle bankanın uğramış olduğu zararın her halükârda müşteri tarafından taşınacağına ilişkin bir genel işlem şartı gerek TKHK m. 6 gerekse BK m. 19/20 uyarınca batıl sayılırdı. Zira bu tür düzenlemeler dürüstlük kuralına aykırı şekilde taraflar arasında bir dengesizliğe yol açar[46]. Ancak somut olaydaki genel işlem şartı bu nitelikte değildir. Bu hüküm müşteri açısından bir davranış yükümlülüğü getirmekte (şifre vs.'yi korumak için her türlü önlemi almak) ve bu yükümlülüğe aykırı davranılması halinde sorumluluğun tümü itibariyle müşteriye ait olacağını öngörmektedir.

GİŞ ile müşteriye bir davranış yükümlülüğü getirilmesi kural olarak TKHK m. 6 ve BK m. 19/20'ye aykırı değildir. Ancak bunun için hem ilgili davranış yükümlülüğünün müşteri tarafından yerine getirilebilir nitelikte olması, hem de bu yükümlülüğe aykırı davranılması halinde ancak bu ihlalle orantılı bir zararı müşterinin taşıyacağının öngörülmüş olması gerekir. Yukarıda aktarılmış olduğu gibi, zarar aslen bankanın malvarlığında meydana geldiği için, bir GİŞ yoluyla bankanın bütün zararını, yasal sorumluluk dağılımına aykırı olarak müşteriye yüklemesi onun aleyhine ciddi bir dengesizlik oluşturacaktır. Müşteri kuşkusuz kusuru oranında zarara katlanmalıdır. Fakat tüm zararın ona

(45) Ayrıntılı bilgi için bkz. *Atamer*, Yeşim: Sözleşme Özgürlüğünün Sınırlandırılması Sorunu Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, 2. bası, İstanbul 2001, s. 200 vd. Nitekim Borçlar Kanunu Tasarısı da m. 20 vd.'da genel işlem şartlarının her türlü sözleşme açısından denetlenebilmesi için bir dizi yeni hüküm öngörmektedir.

(46) Alman hukuku için aynı yönde *Wiesgickl* (dn.11), s. 1039, 1050.

yüklenmesi sadece kasti bir hareket halinde, yani kendisinin bilerek şifreyi başkasına vermiş olması ve bu şekilde bankanın dolandırılmasına yardımcı olması halinde söz konusu olacaktır. Bu haller dışında, müşterinin kötüye kullanım rizikosunu önlemek için etkin bir adım atmasının ne kadar zor olduğu düşünülecek olursa bir ihmalin varlığını kabul konusunda çok dikkatli olmak gerekir. Kuşkusuz, ihmalin kabul edildiği hallerde de ancak bu ihmal oranında bir tazminat yükümlülüğü var olacaktır (BK m. 43). Dolayısıyla aktarılan türden GİŞ hükümleri, müşteri aleyhine sözleşmesel dengeyi aşırı surette bozduğu için BK m. 19/20 uyarınca batıl sayılmalıdır.

IV. Konu ile ilgili bazı Yargıtay kararlarının değerlendirilmesi

Yukarıdaki bilgiler ışığında Yargıtay'ın bugüne kadar konu ile ilgili olarak vermiş olduğu bazı kararlar değerlendirilecek olursa aşağıdaki sonuçlara varılmaktadır:

- **11. HD, 12.9.2003, E. 2003/8280, K. 2003/7705**: Davacı vekili, taraflar arasında imzalanan "*İnternet Bankacılığı Sözleşmesinde internet yoluyla havale yapma hizmeti verilmesi öngörülmediği halde müvekkili şirketin eski müdürü İsmail Emin Karcı'nın verilen şifreyi kullanarak şirket hesabından internet yoluyla virman talimatı vererek kendi hesabına toplam 511.787 Amerikan Doları aktardığını, davalı bankanın sözleşmede belirtilmeyen yöntemi kullandırması nedeniyle davacının uğradığı zarardan müştereken ve müteselsilen sorumlu bulunduğunu ileri sürerek, bu miktarın davalıdan tahsiline karar verilmesini talep etmiştir. Davalı vekili, sözleşmenin 3/2. maddesinde sonradan bankaca eklenecek internet hizmetlerinden de davacının yararlanacağının öngörüldüğünü, davacının da bu hizmetten yararlanarak havale işlemi yaptığını, sözleşmenin 4. maddesinde şifrenin özenle saklanması ve bu nedenle doğacak zararlardan davacının sorumlu olacağının kararlaştırıldığını belirterek, davanın reddini savunmuştur. Mahkemenin, davanın reddine dair verdiği kararın Dairemizce onanması üzerine davacı vekili, bu kez karar düzeltme isteminde bulunmuştur. Dosyadaki yazılara, mahkeme kararında belirtilip Yargıtay ilamında benimsenen gerektirici sebeplere göre, davacı vekilinin HUMK.nun 440. maddesinde sayılan hallerden hiçbirisini ihtiva etmeyen karar düzeltme isteğinin reddi gerekir.*"

Karar metnine yansıtılan bilgiler ışığında olay değerlendirildiğinde şu tespitlerde bulunmak mümkündür: **i.** Havale talimatı, olaydan anlaşıldığı üzere, yetkisi olmayan eski müdür tarafından gerçekleştirilmiştir. **ii.** Banka yetkisiz kişinin verdiği talimat üzerine gerçekleştirdiği ödemeyi kendi malvarlığından yapmıştır. **iii.** Ancak yetkisiz kişinin bu tür bir havale yapabilmesini engellemek için şirket üzerine düşeni yapmamıştır. **iv.** Dolayısıyla şirketin banka ile arasında mevcut mevduat hesabı sözleşmesinden doğan koruma yükümlülüğüne aykırılık söz konusudur. Muhtemelen eski müdürün temsil belgesinin geri

alınmamış olması veya temsil yetkisinin sona erdiği konusunda bankaya gerekli talimatların verilmemiş olması nedeniyle eski müdür internet şifresi almak ve havaleleri gerçekleştirmek imkânı bulmuştur (karş. BK m. 34, f. 3 ve m. 36, f. 2). v. Şirketin koruma yükümlülüklerine aykırılığı nedeniyle bankanın uğradığı zararı %100 oranında tazmin etmesi gerekir, meğerki bankaya izafe edilebilecek bir müterafık kusur olmamış olsun (örn. sözleşmede internet bankacılığının açıkçası yasaklanmış olması gibi). Bu senaryo çerçevesinde Yargıtay'ın verdiği karar doğrudur, ancak hukukî gerekçelendirme eksiktir.

- **11. HD, 28.2.2005, E. 2004/5101, K. 2005/1751**: Olayda davacı, davalı bankanın Aksaray Şubesi nezdinde bulunan iki hesabı üzerinden internet aracılığı ile işlem yapabilmek için şifre almıştır. İnternete girdiğinde hesaplarında para olmadığını gören davacı, yaptığı araştırma sonucunda, toplam 610 milyon liranın yetkisiz T tarafından bankanın Zincirlikuyu Şubesi'nden çekildiğini öğrenmiştir. Polis kayıtlarından, T'nin arkadaşı M'nin, davacının çalışma odasındaki ajandasından şifresini çaldığı anlaşılmıştır. Davalı bankanın 18 yaşını doldurmayan T'ye ödeme yapmakta kusurlu olduğu, basiretli davranmayan davalının ödeme yapmaması gerekirken, zarara neden olduğu ileri sürülerek, 610.000.000 liranın temerrüt faiziyle birlikte tahsili talep edilmiştir. "*Davalı vekili, davacının şifreyi çaldırmakla kusurlu olduğunu, havale alıcısı küçük'ün vekili ile gelmesi ya da velinin yazılı onayını getirmesi halinde ödemenin yapılması gerektiğinden, zarara banka eyleminin neden olduğunun söylenemeyeceğini savunarak, davanın reddini istemiştir. Mahkemece, dosya kapsamına, benimsenen bilirkişi raporuna göre, davacının şifreyi muhafazadaki özensizliği, davalının da reşit olmayan havale alıcısına ödeme yapması nedeniyle yarı yarıya kusurlu oldukları gerekçesiyle, davanın kısmen kabulüne karar verilmiştir.*" Kararı, davalı vekili temyiz etmiştir. Yargıtay kararı onamıştır.

Olaydan anlaşıldığı üzere: **i.** yetkisiz kişinin bankaya internet aracılığıyla verdiği talimat üzerine banka ödemede bulunmuştur. **ii.** Banka yetkisiz kişinin verdiği talimat üzerine gerçekleştirdiği ödemeyi kendi malvarlığından yapmıştır. **iii.** Davacı şifresini gereği gibi muhafaza etmemek suretiyle banka ile arasında mevcut mevduat hesabı sözleşmesinden doğan koruma yükümlülüğüne aykırı davranmıştır. Bu kusurlu davranışının zararın doğumunda etkisinin ne oranda olduğunu Dairenin takdir etmesi gerekir. 11. Hukuk Dairesinin, reşit olmayan kişiye ödemede bulunması nedeniyle bankanın "yarı yarıya kusurlu" olduğu tespiti ise, bankanın kusurunun müterafık kusur[47] olduğu, yani

(47) Kavram hakkında ayrıntı için bkz. *Oğuzman*, Kemal/*Öz*, Turgut: Borçlar Hukuku, Genel Hükümler, İstanbul 2005, 4. bası, s. 579 vd.; *Schwenzer*, Ingeborg: Schweizerisches Obligationenrecht, Allgemeiner Teil, 4 Aufl. Bern 2006, n. 16.04 vd.

zarar görenin, zararın doğumu veya artmasına ilişkin olarak kusurlu davranışının söz konusu olduğu tespitinin yapılmaması açısından eksiktir. Müşterinin kusurunun % 50 olarak tespit edilmesi halinde bankanın bu müterafık kusuru olsa olsa tazminat miktarının indirilmesinde etkili olabilirdi. Yani Dairenin takdirine göre müşterinin tazminat yükümlülüğü zararın % 30-40'ına indirilebilirdi. Oysa Daire, kusur oranlarını, adeta üçüncü bir kişinin malvarlığına zarar veren iki fail mevcutmuş gibi hesaplamıştır. Halbuki malvarlığı azalan bankadır, bu azalmada özensizliği ile etkili olan ise müşteridir. Müşteri ne oranda zarara sebep olmuşsa onu ödeyecektir. Banka da müterafık kusuru oranında bu tazminatın indirilmesine katlanacaktır.

- **19. HD, 31.5.2005, E. 2004/10991, K. 2005/6080**: "*Davacı vekili, müvekkilinin davalı bankada hesabı bulunduğunu, birikimlerini bu hesapta değerlendirdiğini, davalı banka görevlilerinin tavsiyesiyle B Tipli likit fon satın aldığını, bu işlemi şifre kullanarak internet kanalıyla yaptığını, müvekkilince daha sonra yapılan kontrolde hesabında para kalmadığının anlaşıldığını, banka görevlilerinin hesaptaki fonun internet kanalıyla satıldığını ve hesapta bulunan 7.400.000.000.-TL.nın bir başka kişinin hesabına havale edildiğini, bankanın kusursuz sorumlu olduğunu, hesapta bulunan paranın tahsili için yapılan takibe davalının haksız olarak itiraz ettiğini belirterek itirazın iptaline ve % 40 tazminata karar verilmesini talep ve dava etmiştir. Davalı vekili, müvekkilinin dava konusu olayda bir kusuru bulunmadığını, taraflar arasındaki sözleşme uyarınca davacıya ait şifrenin üçüncü kişiler tarafından kullanılması halinde sorumluluğun kendisine ait olduğunu bildirerek davanın reddi gerektiğini savunmuştur. Mahkemece, toplanan delillere ve bilirkişi raporuna göre dava konusu havale işlemlerinin* ***davacının internet bankacılık işlemlerini gerçekleştirmekte kullandığı şifrenin kullanılması suretiyle gerçekleştirildiği****, şifreyle gerçekleştirilen havale işlemlerinde aksine bir kayıt konulmadığından, dava konusu havale işlemlerinde bankanın ayrıca davacıdan teyit almasının gerekmediği, havale işleminde davalı bankanın herhangi bir kusuru bulunmadığı, davacının şifresini iyi koruyamaması nedeniyle kusurlu olduğu gerekçeleriyle davanın reddine karar verilmiş, hüküm davacı vekilince temyiz edilmiştir.*" Yargıtay 19. Hukuk Dairesi kararı onamıştır.

Bu karar, yukarıda aktarılan 11. Hukuk Dairesinin iki ve aşağıda aktarılacak 2006 tarihli diğer bir kararı ile mukayese edildiğinde, 19. Hukuk Dairesinin içtihadının farklı bir yönde gelişeceği izlenimi vermektedir. Daire, yetkisiz kişilerce, ancak doğru şifre kullanılarak yapılan işlemden doğan zararın tümü itibariyle müşteri tarafından taşınacağı görüşünü beyan etmiştir. Ancak Daire bu konuda herhangi bir hukukî gerekçe göstermemiştir. Yukarıda aktarılan bilgiler çerçevesinde kararda varılan sonuca katılmak mümkün değildir. Üçüncü kişi tarafından şifrenin hukuka aykırı yollarla edinilmesi suretiyle doğan zararlar

bankanın malvarlığında doğar. Dolayısıyla banka bu zararı ancak, müşterinin sözleşmeden doğan koruma yükümlülüklerine aykırı davranması halinde ona yansıtabilir. Olaya ilişkin verilerden, müşterinin bu tür bir davranışının olup olmadığı anlaşılamamaktadır. Dolayısıyla somut olayda müşterinin kusurunun derecesine ilişkin bir tespitte bulunmak mümkün değildir. Eğer müşterinin özen yükümlülüğüne aykırılığı ispat edilememişse bu durumda banka bütün malvarlığı zararını taşımak durumundadır.

- **11. HD, 24.11.2006, E. 2006/11943, K. 2006/12226:** "*Davacı vekili, müvekkilinin davalı banka nezdindeki hesabının O. A. adlı kişi tarafından internet şifresi ele geçirilip kullanılarak çekildiğini ileri sürerek (20.146.720.234.-) TL'nin davalıdan tahsilini talep ve dava etmiştir. Davalı vekili, davacının şifrenin başkalarınca ele geçirilmesinde kusurlu olduğunu savunarak davanın reddini istemiştir. Mahkemece, objektif özen yükümlülüğünü yerine getirmeyen davalı bankanın hafif kusurlardan dahi sorumlu olduğu, davacının şifresini koruma yükümlülüğüne uygun davranmadığı gerekçesiyle davanın kabulüne karar verilmiştir. Kararı davalı vekili temyiz etmiştir. Dairemizce yapılan inceleme sonucu, davacı hesaplarından 15 dakika içinde 16 ayrı işlemle para havalesi yapıldığı, bilgisayar korsanlığı yöntemiyle işlemler yapılmasını önleme yolunda ek güvenlik tedbiri almayan davalının kusurlu ve sorumlu olduğu gerekçesiyle yerel mahkeme kararı onanmış, davalı vekili bu kez karar düzeltme isteminde bulunmuştur. Yargıtay ilamında benimsenen gerektirici sebeplere göre davalı vekilinin HUMK'nın 440. maddesinde sayılan hallerden hiçbirini ihtiva etmeyen karar düzeltme isteğinin reddi gerekir.*" Dairenin 22.6.2006 tarihli temyiz safhasındaki kararında da şu tespitlerde bulunulmuştur: "*16.08.2004 tarihli uzman bilirkişiler kurulu raporunda yer alan saptamalardan, davalı bankanın iki ayrı şubesinde hesabı bulunan davacının taraflar arasındaki bireysel internet şubesi sözleşmesi uyarınca davalının internet şubesi nezdinde yaptığı işlemlerde kullandığı kullanıcı adı ve şifresinin bilgisayarına yerleşmiş casus programlarda başkasınca elde edilerek davacı hesaplarından (20.146.720.234) TL'nin çok kısa bir süre içerisinde (16) ayrı işlemle internet yolu ile davacının haberi olmadan davalı bankanın Konak Şubesi'ne aktarılmasında bu tür bilgisayar korsanlığı yöntemiyle işlemler yapılmasını önleme yolunda ek güvenlik tedbirleri almayan ve olaydan sonra bu yola tevessül eden davalının kusurlu ve sorumlu bulunduğunun, davacının sanal klavye kullanması halinde dahi bunun yapılan bilgisayar korsanlığını engellemeye teknik olarak yetmeyeceğinin anlaşılmasına, işlemi yapan kişi hakkındaki ceza soruşturması sonucunun hafif kusurundan dahi sorumlu olan davalı banka bakımından etkili görülmemesine göre, davalı vekilinin temyiz itirazlarının reddi gerekmiştir.*"

Aktarılan bu son kararda 11. Hukuk Dairesi her ne kadar haklı olarak, bankanın zararı taşıması gerektiği sonucuna varmışsa da hukukî gerekçeleri kanımca doğru değildir. Olaydan anlaşıldığı üzere: **i.** yetkisiz kişinin bankaya internet aracılığıyla verdiği talimat üzerine banka ödemede bulunmuştur. **ii.** Dolayısıyla banka yetkisiz kişinin verdiği talimat üzerine gerçekleştirdiği ödemeyi kendi malvarlığından yapmıştır. **iii.** Davacının şifresini gereği gibi muhafaza etmemek suretiyle banka ile arasında mevcut mevduat hesabı sözleşmesinden doğan koruma yükümlülüğüne aykırı davrandığı ispatlanamamıştır[48]. Bu durumda Dairenin, Bankanın kusuru konusunda ayrıntılı incelemeler yapmasına aslında hiç gerek kalmamıştır. Zira zarar zaten bankanın malvarlığında doğmuştur, banka bu zararı müşterisine yansıtamamaktadır, çünkü kendisinin koruma yükümlülüğüne aykırı bir davranışı ispatlanamamıştır. Bu durumda bankanın ayrıca müterafık kusurunun olup olmadığı tartışması gereksizdir. Dairenin, müşteri açısından müterafık kusurdan bahsetmesi ise doğru değildir. Müterafık kusur, zarar görenin zararın doğumuna veya artmasına ilişkin kusurudur. Oysa zarar gören bankadır, dolayısıyla sadece banka açısından bu tür bir değerlendirme önem taşıyabilir ve sadece zarar veren kişinin ödeyeceği tazminat miktarının belirlenmesi açısından BK m. 44 çerçevesinde dikkate alınır. Oysa olayda müşterinin tazminat ödemesi söz konusu değildir.

V. Sonuç

Engellenmesi güç bir rizikonun zararlı sonuçlarının kimin tarafından taşınması gerektiği konusunda hukukta karar verilirken dikkate alınacak olan farklı mülahazalar vardır. Bunlardan ilki, o rizikoyu kontrol etme olanağına daha çok kimin sahip olduğudur. Yani o rizikonun gerçekleşmesini en etkin ve en az maliyet ile önleme iktidarının (*cheapest cost avoider*) kimde olduğudur[49]. Olayımızdaki soruna bakıldığında, internet ortamında işlem yapılmasını daha güvenli kılmak için yeni teknolojiler üretme ve bunları uygulama konusunda ancak bankaların etkin olabileceği görülmektedir[50]. Müşteriler, aydınlatıldıkları oranda bazı tedbirleri alabilirse de, bunlar ancak sınırlı ölçüde bir güvenlik sağlayabilir. Nitekim internet bankacılığının gelişiminden bu yana, bankaların, sistemi daha güvenli kılmak için yaptıklarına[51] bakıldığında bu

(48) Bu husus, Yargıtay'ın temyiz safhasında onadığı Kadıköy Asliye 4. Ticaret Mahkemesi'nin kararından anlaşılmaktadır. Kararda şu ifade yer almaktadır: "*Mahkemece [...] davacının şifresini koruma yükümlülüğüne uygun davranmadığı ve müterafık kusurlu olduğu savunmasının kanıtlanmadığı gerekçesiyle davanın kabulüne karar verilmiştir.*"

(49) Bu konuda bkz. *Sanlı*, Kerem Cem: Haksız Fiil Hukukunun Ekonomik Analizi, Hukuk ve Ekonomi Öğretisi, İstanbul 2007, s. 435 vd.

(50) *Janisch/Schartner* (dn. 11), s. 162, 167.

(51) Her işlem için değişik bir şifre üreten şifrematik; havale limitleri; havale halinde cep telefonu mesajı veya e-posta ile anında bilgilendirme ve buna bağlı olarak

tür bir riziko dağılımının daha uygun olduğu da görülecektir. Bu tür teknolojileri geliştirme ve bu konuda yatırım yapma imkânı sadece bankalar açısından vardır. Müşteriler bu konuda her hangi bir adım atabilecek durumda değildir. Dolayısıyla zarar rizikosunu müşterinin taşıması gerektiğinin kabul edilmesi, bu zararın doğumunu engelleyecek teknolojilerin geliştirilmesini de sekteye uğratır[52]. Zira bankalar açısından, zararı müşterilerine yansıtabildikleri ölçüde, bu alana yatırım yapma konusundaki itici güç (*incentive*) ortadan kalkar. Müşteri ise, internet bankacılığının bu kadar rizikolu olması nedeniyle sistemi kullanmaktan vazgeçer. Bu sonuç ise ne ekonomik açıdan ne de taraflar açısından istenen bir sonuç olur.

Bir rizikonun kimin tarafından taşınacağı konusunda karar verilirken dikkate alınacak ikinci mülahaza, bu rizikoyu en iyi kimin sigorta ettirebileceğidir[53]. Avusturya Federal Mahkemesinin 2002 yılında verdiği bir kararında ifade ettiği gibi[54], zararın banka müşterisi tarafından taşınması kabul edildiğinde, bu onun ekonomik çöküşü anlamına gelecekken, banka tarafından taşınması halinde zararın sigortalanması mümkün olacak ve bu şekilde zarar topluma yayılacaktır. Zira banka, sigorta primlerini müşterilerinden işlem ücreti olarak tahsil edebilecektir. Oysa müşterilerin kendilerini bu tür bir rizikoya karşı sigortalama imkânları yoktur. Piyasada bu türden bir sigorta sunulmamaktadır. Sunulsa bile bunun maliyeti müşteri açısından çok daha fazla olacaktır, çünkü onun prim ödemelerini sistemdeki diğer aktörlere yansıtması imkânı yoktur. Dolayısıyla ekonomik açıdan doğru karar, sisteme içkin (yani engellenemez veya yüksek maliyet ile engellenebilir) rizikoyu sigortalama imkânı olan tarafa zararı taşıtmak ve bunun maliyetini (yani sigorta primlerini) sisteme katılan herkese yaymaktır. Bu şekilde zarar da topluma yayılacaktır. Dolayısıyla internet bankacılığından faydalanan müşterilerden ek ödeme istenmesi kanımca hukuk politikası açısından doğru bir tercihtir. Madem ki sisteme içkin bir zarar potansiyeli var, ama kimse bu sistemden vaz geçmek istemiyor, o zaman aktörlerin hepsi bir ölçüde maliyete katlanmalıdır. Banka zarar potansiyelini sigortalayabilir, müşteri ise bu sistemi kullanmak için daha fazla para ödeyebilir.

---

cep telefonu ve e-posta adreslerinin İnternet yoluyla değiştirilememesi gibi. Yakında ancak elektronik imza ile işlem yapılabilecek olması (*homebanking*), yeni tür İnternet browser'ların çok daha büyük bir güvenlik sağlayacak olması da bu konuda teknolojik gelişmelerin ne kadar büyük bir önem taşıdığını göstermektedir. Bu konuda bkz. *Gajek/Schwenk/Wegener* (dn. 24), s. 639, 642.

(52) *Bohm/Brown/Gladman* (dn. 24), Nr.132.

(53) *Gössmann*, Wolfgang/*Weber*, Beatrix, Recht des Zahlungsverkehrs, 4. bası, 2004, s. 305; *Guggenheim* (dn.10), s. 249; *Behrens*, Peter: Die ökonomischen Grundlagen des Rechts, Tübingen 1986, s. 159.

(54) OGH 19.11.2002, ÖBA 2003, 141.

Aşağıda, mahkemelerin, internette yaşanan bu tür saldırılar sonucu doğan zararı kimin taşıyacağı konusunda izleyebileceği hukukî mantık kurgusu özet olarak verilmiştir.

1. Banka ve müşterisi arasındaki sözleşmelere usulsüz tevdi, karz ve vekalet sözleşmesi hükümleri kıyasen uygulanır.

2. Bu hükümler uyarınca bankaya tevdi edilen paranın kaybolması veya çalınması rizikosunu banka taşır.

3. Bankanın ancak, müşterinin zararın doğumunu engellemek konusunda bir koruma yükümlülüğüne aykırı davrandığını ispat edilebildiği ölçüde, sözleşmenin müspet ihlali hükümleri (BK m. 96) uyarınca müşteriden bir tazminat talebi olabilir.

4. Müşterinin ödemesi gereken tazminatın kapsamı belirlenirken BK m. 44 uyarınca bankanın (zarar gören olarak) zararın doğumuna veya artmasına etki edip etmediği dikkate alınır. Eğer banka, sistemi gereği gibi güvenli kılmamış, müşterilerini koruma önlemleri hakkında gereği gibi aydınlatmamış ise müterafık kusurlu sayılır ve tazminat miktarından indirim yapılır.

5. Bankanın, zararı tümü itibariyle müşteriye yükleyen genel işlem şartları, müşteri aleyhine sözleşmesel dengeyi aşırı surette bozduğu için BK m.19/20 veya tüketici işlemlerinde, Tüketicinin Korunması Hakkında Kanun m. 6 uyarınca batıl sayılır. Bu hallerde de bankanın ancak kusuru oranında müşteriye başvurması imkânı olacaktır.